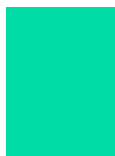
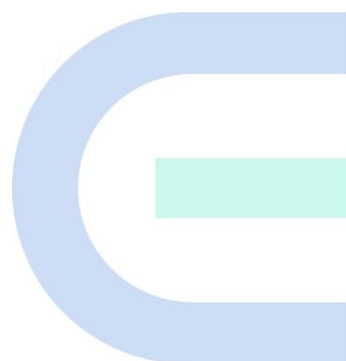


# RG-WALL 1600-Z-S Series Cloud-Managed Firewall

## Cookbook



## Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

Any reproduction, excerpt, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, is prohibited without the prior written consent of Ruijie Networks.

Trademarks including  ,  ,  are owned by Ruijie Networks.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

## 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 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](mailto:service_rj@ruijienetworks.com)

## Conventions

### 1. GUI Symbols

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

### 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

Preface .....	1
1 Product Overview .....	1
1.1 Overview .....	1
1.2 Product Characteristics.....	1
1.3 Hardware Description .....	2
1.3.1 RG-WALL 1600-Z3200-S Panels.....	3
1.4 Specifications.....	6
1.4.1 RG-WALL 1600-Z3200-S Specifications .....	6
2 Device Management .....	8
2.1 Logging In to the Device .....	8
2.1.1 Logging In to the Device from the Web .....	8
2.1.2 Logging In to the Device from the Console .....	14
2.1.3 Logging In to the Device Using SSH .....	20
2.2 Modifying the Web Login Configuration .....	22
2.3 Account Permission Settings.....	25
2.3.1 Administrator Permission Overview .....	25
2.3.2 Enabling Default Accounts.....	25
2.3.3 Creating an Administrator .....	27
2.3.4 Changing the Password.....	32
2.4 Configuration Backup and Restoration.....	35
2.4.1 Exporting the Configuration .....	35
2.4.2 Importing the Configuration .....	36
2.5 Defaults Restoration .....	37

2.5.1 Web-based One-Click Restoration .....	37
2.5.2 Restoration by Pressing the Reset Button.....	38
2.6 Password Restoration.....	39
2.7 SNMP Management .....	42
2.7.1 Overview .....	42
2.7.2 Configuring SNMP .....	43
3 License Activation.....	48
3.1 Authorization Service Overview.....	48
3.2 Secure Cloud Platform.....	49
3.2.1 Overview .....	49
3.2.2 Secure Cloud Platform Operations.....	50
3.2.3 License Activation Methods .....	70
3.3 Precautions for License Activation .....	73
4 Signature Library Upgrade .....	74
4.1 Configuring Automatic Upgrade .....	74
4.2 Local Manual Upgrade.....	75
4.3 Online Automatic Upgrade.....	77
5 Version Upgrade.....	79
5.1 Overview .....	79
5.2 Upgrade Operations .....	80
5.2.1 Offline Upgrade .....	80
5.2.2 Online Upgrade.....	81
5.2.3 Version Rollback .....	82
6 Configuration Examples for Typical Scenarios .....	84

6.1 Integrated Deployment on Ruijie Cloud.....	84
6.1.1 Firewall Deployment (Routing Mode) .....	84
6.1.2 NBR Deployment (Transparent Mode) .....	90
6.1.3 Deployment Using Ruijie Cloud App (Routing Mode).....	96
6.1.4 Deployment Using Ruijie Cloud App (Transparent Mode).....	105
6.2 Transparent Mode.....	114
6.2.1 Preparations.....	114
6.2.2 Deployment in Transparent Mode (Quick Deployment) .....	115
6.2.3 Out-of-Band Management in Transparent Mode (Custom Deployment) .....	120
6.2.4 Multi-bridge Deployment Mode.....	126
6.2.5 Precautions for Deploying Transparent Bridge Mode .....	133
6.2.6 Configuring a Bridge Interface .....	134
6.3 Routing Mode.....	138
6.3.1 Preparations.....	138
6.3.2 Single-Line Onboarding (Quick Deployment).....	139
6.3.3 Single-Line Onboarding (Custom Deployment).....	148
6.4 Off-Path Mode.....	173
6.4.1 Preparations.....	173
6.4.2 Deployment in Off-Path Mode (Quick Deployment) .....	174
6.4.3 Configuring an Off-Path Interface (Custom Deployment) .....	179
6.4.4 Precautions for Deploying Off-Path Mode .....	182
7 Common Operations .....	183
7.1 NAT Policy .....	183
7.1.1 NAT Technology .....	183

7.1.2 Configuring Destination Address Translation (One-to-One Port Mapping) .....	186
7.1.3 Configuring Bidirectional Address Translation (Allowing Intranet PCs to Access the Map Server by Using a Public Network Address).....	196
7.1.4 Importing NAT Policies in a Batch .....	201
7.2 Security Defense.....	203
7.2.1 Principle and Application Scenario .....	203
7.2.2 DoS/DDoS Attack Defense .....	208
7.2.3 Intrusion Prevention .....	216
7.2.4 Virus Protection.....	219
7.2.5 ARP Attack Defense.....	222
7.2.6 Local Defense .....	226
7.2.7 Threat Intelligence .....	231
7.2.8 URL Filtering .....	240
7.3 Configuring SSL Proxy Policies.....	245
7.3.1 Overview .....	245
7.3.2 Configuring an SSL Proxy Template .....	246
7.3.3 Importing Certificate.....	247
7.3.4 Configuring an SSL Proxy Policy.....	252
7.3.5 Allowlist .....	255
7.4 Port Scan .....	257
7.5 Traffic Learning.....	263
7.6 Security Policy .....	267
7.6.1 Overview .....	267
7.6.2 Configuring Security Policy (Using Wizard).....	271
7.6.3 Configuring Security Policy (Manual) .....	280

7.6.4 Adjusting Policy Order.....	284
7.6.5 Optimizing Policy .....	285
7.6.6 Policy Lifecycle Management .....	287
7.6.7 Simulation Run.....	288
7.6.8 Importing Security Policies in a Batch .....	291
7.6.9 Enabling Basic Protocol Packet Control .....	293
7.7 DHCP Management.....	295
7.7.1 Overview .....	301
7.7.2 Configuring a DHCP Server.....	302
7.7.3 Address Management List .....	307
7.8 Blocklist and Allowlist.....	308
7.8.1 Overview .....	308
7.8.2 Precautions .....	308
7.8.3 Creating an IPv4 Allowlist .....	309
7.8.4 Creating an IPv6 Allowlist .....	311
7.8.5 Creating an IPv4 Blocklist.....	312
7.8.6 Creating an IPv6 Blocklist.....	314
7.8.7 Creating a Temporary IPv4 Blocklist.....	316
7.8.8 Creating a Temporary IPv6 Blocklist.....	317
7.9 Security Rule Base Management .....	319
7.10 Connecting to Ruijie Cloud .....	320
7.10.1 Overview .....	320
7.10.2 Connecting to Ruijie Cloud .....	320
7.10.3 Operations on Ruijie Cloud.....	322

7.11 DNS Server Configuration .....	328
7.12 Intelligent Routing .....	329
7.13 Address Library Routing (ISP-based Routing) .....	333
7.13.1 Overview .....	333
7.13.2 Configuring an ISP Address Library .....	333
7.13.3 Configuring ISP Routing .....	339
7.13.4 Viewing the Routing Table of Address Library .....	342
7.14 Aggregate Interface .....	343
7.15 Link Detection .....	348
7.16 SSL VPN .....	350
7.16.1 Overview .....	350
7.16.2 (Optional) Import Local Certificate .....	351
7.16.3 Creating an SSL VPN Gateway .....	353
7.16.4 Hardware Signature Management .....	364
7.16.5 Operation Monitoring .....	366
7.17 VRRP .....	367
7.17.1 Overview .....	409
7.17.2 Working Process .....	410
7.17.3 Configuring a VRRP Group .....	411
7.17.4 Viewing VRRP Logs .....	414
7.18 User Authentication .....	错误!未定义书签。
7.18.1 Overview .....	错误!未定义书签。
7.18.2 User Management .....	错误!未定义书签。
7.18.3 Authentication Domain Management .....	错误!未定义书签。

7.18.4 Authentication Settings .....	错误!未定义书签。
7.18.5 Authentication Server.....	错误!未定义书签。
8 Routine Maintenance .....	439
8.1 Checking Indicators on the Hardware Device Panel.....	439
8.2 Checking Basic Configurations.....	441
8.3 Log Monitoring .....	443
8.3.1 Querying System Logs.....	443
8.3.2 Querying Security Logs.....	444
8.3.3 Querying Session Logs.....	446
8.3.4 Querying Operation Logs.....	447
8.3.5 Configuring the Syslog Server .....	448
8.4 Traffic Monitoring .....	449
8.4.1 Querying Interface Traffic Monitoring .....	449
8.4.2 Querying Source IP Traffic Statistics .....	450
8.4.3 Querying App Traffic Statistics.....	452
8.5 Session Monitoring .....	453
8.5.1 Overview .....	453
8.5.2 Real-Time Session Information .....	453
8.5.3 Session Statistics Collection.....	455
8.6 Intelligence Overview.....	456
9 Advanced Features .....	459
9.1 ALG.....	459
9.1.1 Overview .....	459
9.1.2 Configuring ALG.....	459

10 FAQs.....	461
10.1 Product Knowledge.....	461
10.1.1 What Is the Hardware Architecture of the RG-WALL 1600-Z-S Series Firewall? ...	461
10.1.2 What Are the Restrictions of Port MGMT? .....	461
10.2 Firewall Deployment .....	461
10.2.1 What Firewall Deployment Modes Are Supported?.....	461
10.2.2 Can GE Optical Port and 10GE Optical Port Form a Bridge?.....	464
10.3 Typical Feature Configuration .....	464
10.3.1 How Is Source NAT Implemented?.....	464
10.3.2 Does the Firewall Support Link Detection? .....	464
10.3.3 Does the Z-S Series Firewall Block TCP Sessions in the Secondary Traversal Scenario?.....	465
10.3.4 Does the Firewall Support Port Aggregation? .....	465
10.4 Login Management .....	465
10.4.1 What Can I Do If I Fail to Log In to the Web Page? .....	465
10.4.2 What Can I Do If I Fail to Log In to the System Through SSH? .....	465
10.5 O&M and Monitoring.....	466
10.5.1 How Do I View the CPU, Memory, and Hard Disk Information of the Firewall?.....	466
10.5.2 How Do I View the Interface Traffic of the Firewall?.....	466
11 Troubleshooting.....	468
11.1 Security Policy .....	468
11.1.1 Principle.....	468
11.1.2 Configuration Points of Security Policies .....	468
11.2 Data Packet Processing .....	469
11.3 Diagnostic Center .....	471



11.4 Packet Obtaining.....	474
11.5 Device Self-Test.....	476
11.6 One-Click Fault Information Collection.....	478
11.7 Data Flow Diagnosis.....	479
11.7.1 Packet Statistics Collection.....	479
11.7.2 Flow Status.....	483
11.7.3 Packet Tracing.....	485
12 Running Status Check After Product Implementation .....	489
12.1 Checking the Software Version .....	489
12.2 Checking the Management Mode.....	490
12.3 Checking Firewall Policies .....	493
12.4 Checking the Operation Status.....	494
12.5 Checking the System Status.....	494
12.6 Checking the Log Status.....	495
12.7 Checking the Network Connectivity.....	497
12.8 Checking the Service Use Status .....	498

# 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.

**Hardware-based attack defense**

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

**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.)



**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

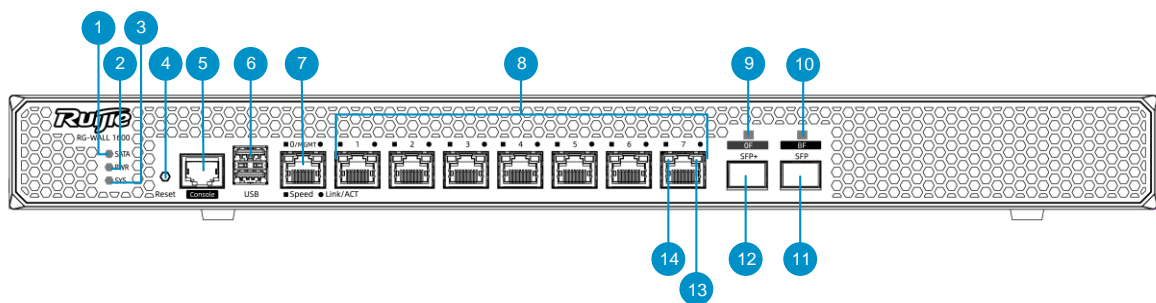


Table 1-1 Components on the Front Panel

No.	Component	Description
1	SATA hard disk indicator	<ul style="list-style-type: none"> <li>• Steady green: A hard disk is connected.</li> <li>• Blinking green: Data is being read or written.</li> </ul>

No.	Component	Description
2	PWR indicator	<ul style="list-style-type: none"> <li>● Steady green: The power supply is normal.</li> <li>● Off: The power supply is cut off or fails.</li> </ul>
3	SYS indicator	<ul style="list-style-type: none"> <li>● Blinking green: The device is powered on and being initialized.</li> <li>● Steady green: Initialization is complete.</li> <li>● Steady red: An alarm is generated.</li> </ul>
4	Reset button	<ul style="list-style-type: none"> <li>● Restarting the device: Press the button for less than 3 seconds.</li> <li>● Restoring factory settings: Press the button for more than 5 seconds.</li> </ul> <p>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 <b>System &gt; One-Click Collection</b>, and download the information.</p>
5	Console port	<p>It is used to connect to the console for device maintenance and diagnosis.</p> <p>Note: The console port is used only in special scenarios. For details, contact technical support personnel.</p>
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	<ul style="list-style-type: none"> <li>● Steady green: The port is connected.</li> <li>● Blinking green: The port is receiving or sending data.</li> <li>● Off: The optical port is incorrectly connected.</li> </ul>

No.	Component	Description
10	Optical port 8F indicator	<ul style="list-style-type: none"> <li>● Steady green: The port is connected.</li> <li>● Blinking green: The port is receiving or sending data.</li> <li>● Off: The optical port is incorrectly connected.</li> </ul>
11	Optical port 8F	Gigabit optical port. For details about optical modules that support this port, see <a href="#">Table 1-3</a> .
12	Optical port 0F	10 Gigabit optical port. For details about optical modules that support this port, see <a href="#">Table 1-3</a> .
13	Link/ACT status indicators (round) of electrical ports 0 to 7	<ul style="list-style-type: none"> <li>● Steady green: The port is connected.</li> <li>● Blinking green: The port is receiving or sending data.</li> <li>● Off: The port is incorrectly connected.</li> </ul>
14	Speed indicators (square) of electrical ports 0 to 7	<ul style="list-style-type: none"> <li>● Steady orange: Gbit/s port speed</li> <li>● Off: 100/10 Mbit/s port speed</li> </ul>

## 2. Rear Panel

Figure 1-2Rear Panel

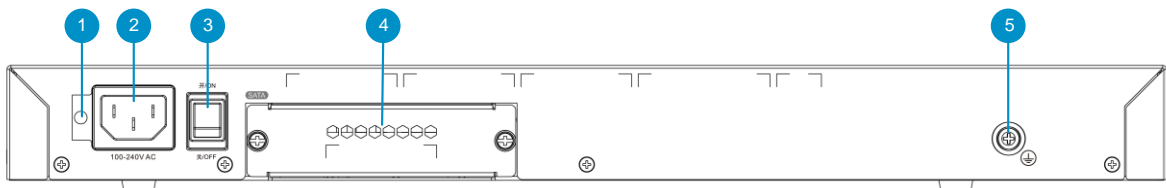


Table 1-2 Components on the Rear Panel

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.

No.	Component	Description
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

<b>Model</b>	RG-WALL 1600-Z3200-S
<b>Storage</b>	DDR4 SDRAM: 4 GB
	Boot ROM: 8 MB
	eMMC: 8 GB
	SATA hard disk: 1 TB
<b>Port</b>	<p>The firewall supports eight Gigabit electrical ports and two optical ports.</p> <ul style="list-style-type: none"> <li>● 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.</li> <li>● Gigabit optical port: supports 1000BASE-SX/LX/ZX mini GBIC and GE-SFP-LX20/LH40-BIDI optical modules.</li> <li>● 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.</li> </ul>
	<p>MGMT port</p> <p>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</p>

	and crossover cables.
	Console port: 1
	USB port: two USB 2.0 ports
<b>Bypass</b>	Not supported
<b>Expansion Slot for Hard Disk</b>	(Optional) One 1 TB hard disk can be configured.
<b>Expansion Card</b>	Not supported
<b>Hot Swapping</b>	Hard disk: not supported
<b>Port Standards</b>	Ethernet port: 10Base-T/100Base-TX/1000Base-TX, 1000BASE-SX/LX/ZX, and 10GBASE-SR/LR/ZR
	Console port: RS-232
<b>Dimensions (H x W x D)</b>	43.6 mm x 440 mm x 200 mm (1.72 in. x 17.32 in. x 7.87 in.; without rubber pads)
<b>Power Supply</b>	100–240 V AC, 50–60 Hz; 0.65 A
<b>Max. Power Consumption</b>	Less than 25 W
<b>Temperature</b>	0°C to 45°C (32°F to 113°F)
<b>Humidity</b>	10% to 90% RH (non-condensing)



## 2 Device Management

### 2.1 Logging In to the Device

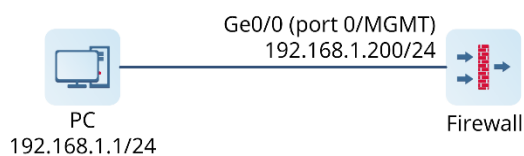
#### 2.1.1 Logging In to the Device from the Web

##### 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)

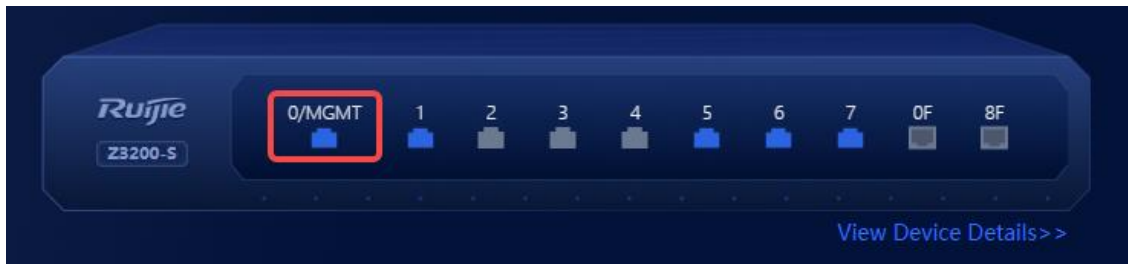
##### **Note**

- If the address of port 0/MGMT on the firewall is modified but you forget the address, you can access the Command Line Interface (CLI) to view the current configuration. For details, see [0](#)

[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.

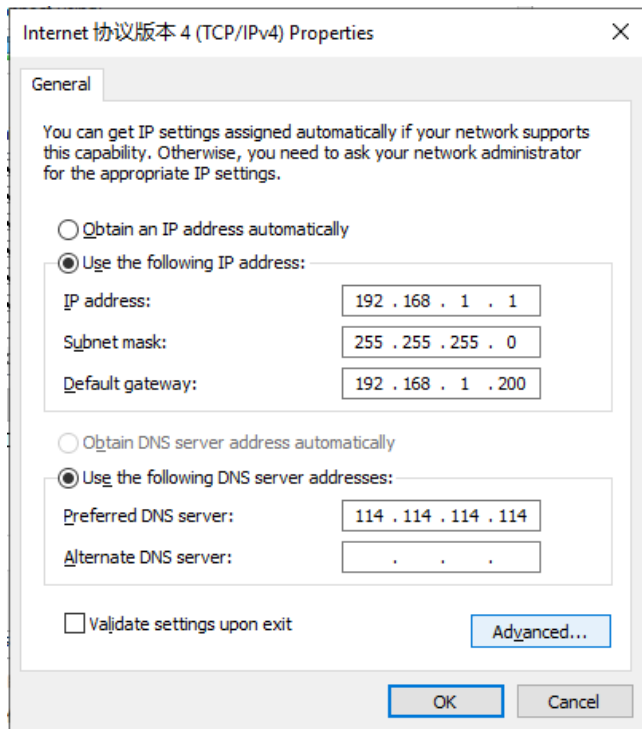
### Configuration Points

- (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.



(2) Log in to the web management page.

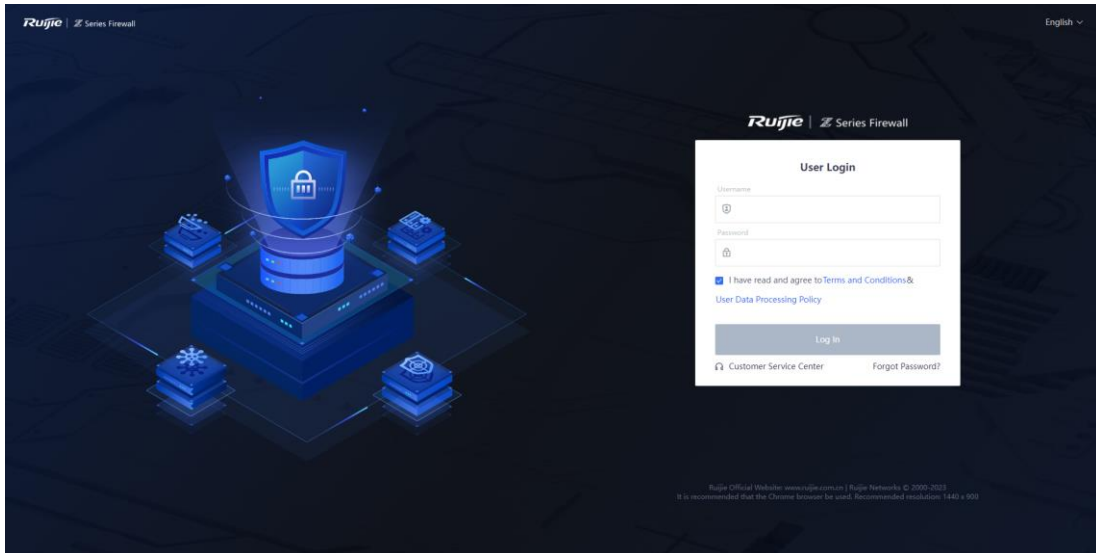
---

**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.

---

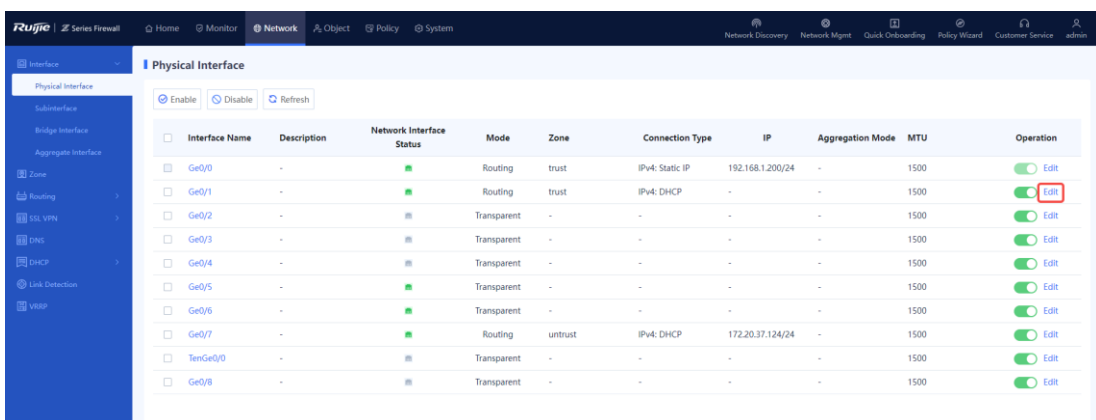
- a Open a browser on the management PC.
- b Enter **https://192.168.1.200** in the address bar and press **Enter**.  
The login page is displayed.
- c Enter the username (**admin**), password (default: **firewall**), and verification code. Read the statement, select **I have read and agree to Terms and Condition & User Data Processing Policy**, and click **Log In**.



(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**.



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

c Configure attributes of Ge0/1.

< Back
**Edit Physical Interface**

---

**Basic Info**

Interface Name

Description

Connection Status  Enable  Disable

Mode  Routing Mode  Transparent Mode  Off-Path Mode

\* Zone  [+ Add Security Zone](#)

Interface Type  WAN Interface  LAN Interface

---

**Address**

IP Type  IPv4  IPv6

Connection Type  Static Address  DHCP  PPPoE

\* IP/Mask

\* Next-Hop Address

Default Route

---

**Line Bandwidth**

Uplink

Downlink

---

**Access Management**

Permit  HTTPS  PING  SSH

---

**Advanced**

ISP Address Library

ⓘ MTU

MAC  [Restore Default MAC](#)

Link Detection

Item	Description	Remarks
IP/Mask	IP address of the physical interface.	[Example] 192.168.0.200/24
Access Management	Whether the interface supports HTTPS, ping, and SSH. <ul style="list-style-type: none"> <li>● <b>HTTPS:</b> Allows users to access the</li> </ul>	The configuration takes effect when local defense is enabled on the device.

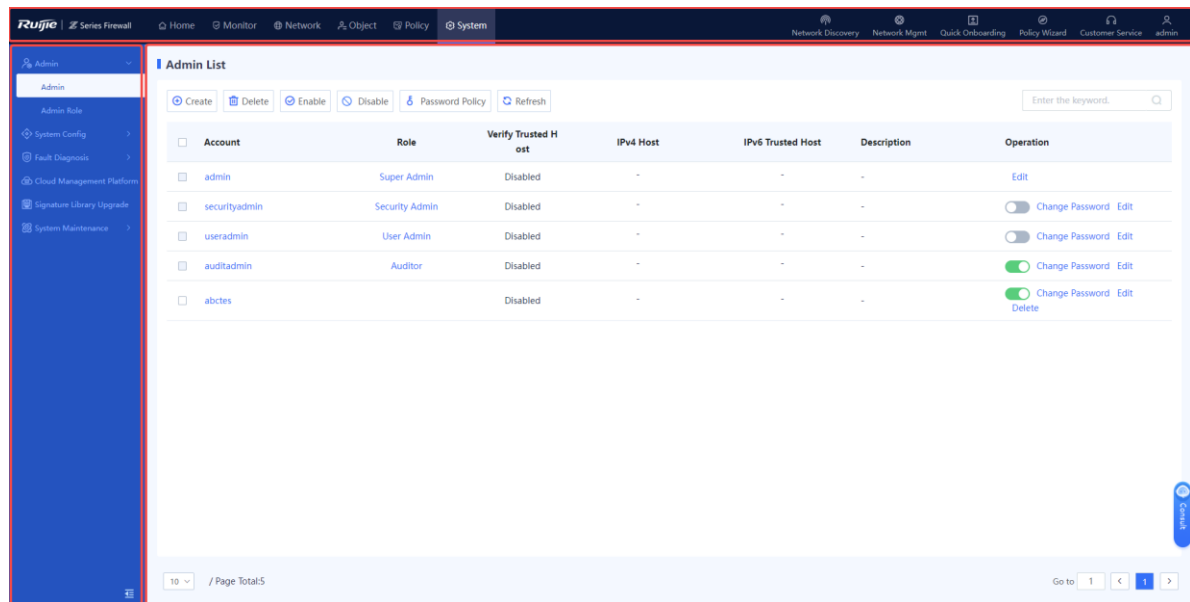
Item	Description	Remarks
	<p>device using <code>https://Interface IP address</code>, such as <code>https://192.168.0.200</code>.</p> <ul style="list-style-type: none"> <li>● <b>PING:</b> Allows users to ping the interface address. If this option is not selected, ping fails even if there is a reachable route.</li> <li>● <b>SSH:</b> 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 <code>ssh 192.168.0.200</code>.</li> </ul>	<p>[Example] Select <b>HTTPS</b>.</p>

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**



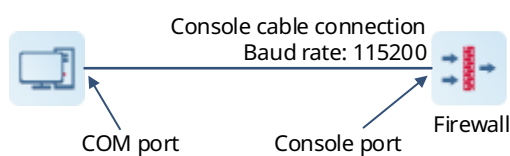
Area	Description
Mark and panel area	<ul style="list-style-type: none"> <li>● This area displays the company logo, device name, and function panel.</li> <li>● This area supports new network discovery, network-wide management, quick onboarding, policy configuration wizard, and customer service, helping users quickly complete deployment operations.</li> <li>● This area displays the current login user and allows you to change the password and log out.</li> </ul>
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 2-2COM port****Figure 2-3USB-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**.

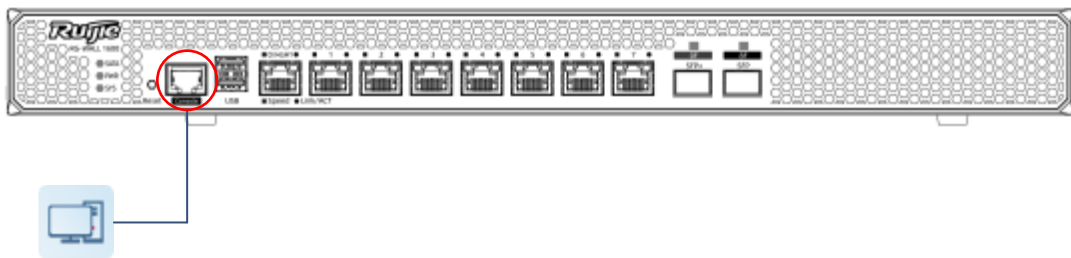
**Configuration Points**

- (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.

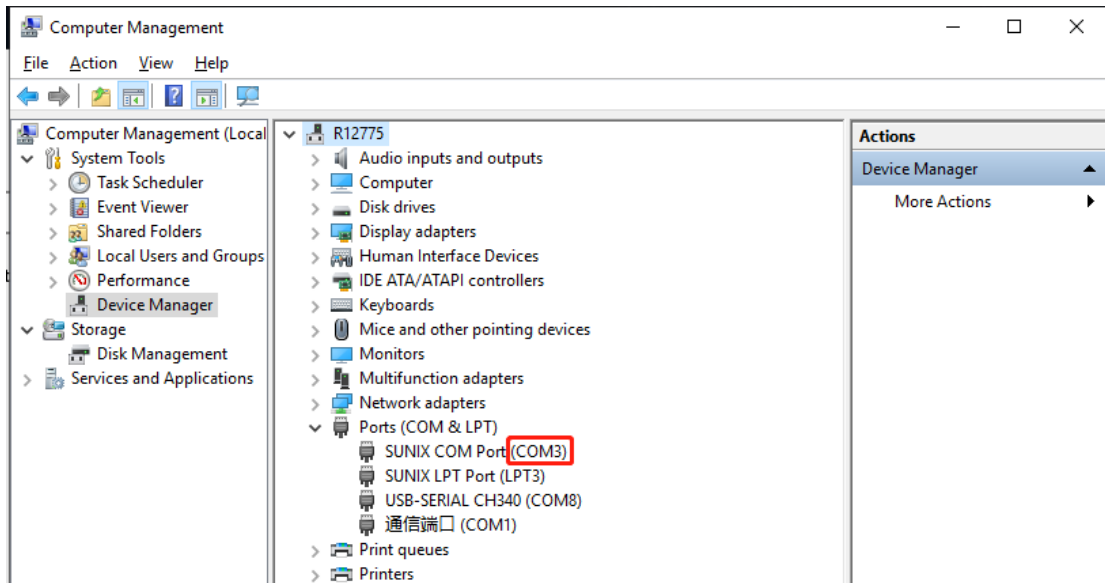
---


**Note**

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

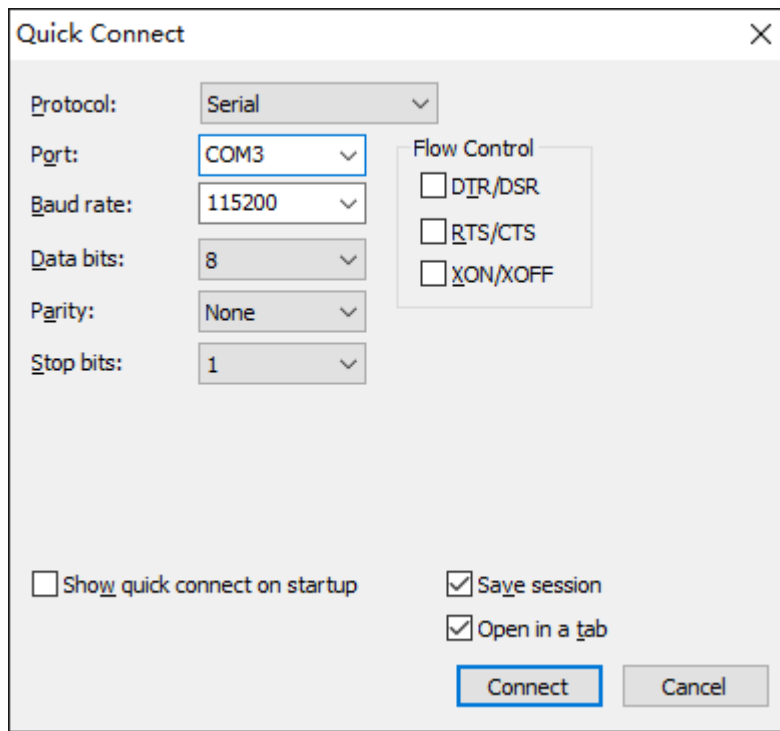
---

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



### 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:
```

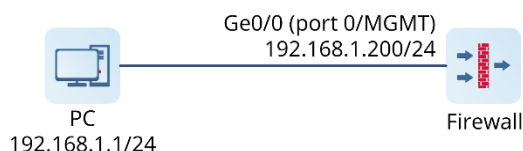


## 2.1.3 Logging In to the Device Using SSH

### 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.

**Edit Physical Interface**

**Basic Info**

Interface Name:

Description:

Connection Status:  Enable  Disable

Mode:  Routing Mode  Transparent Mode  Off-Path Mode

\* Zone:  [Add Security Zone](#)

Interface Type:  WAN Interface  LAN Interface

**Address**

IP Type:  IPv4  IPv6

Connection Type:  Static Address  DHCP  PPPoE

\* IP/Mask:

**Line Bandwidth**

Uplink:

Downlink:

**Access Management**

Permit  HTTPS  PING  SSH

**Advanced**

MTU:

MAC:

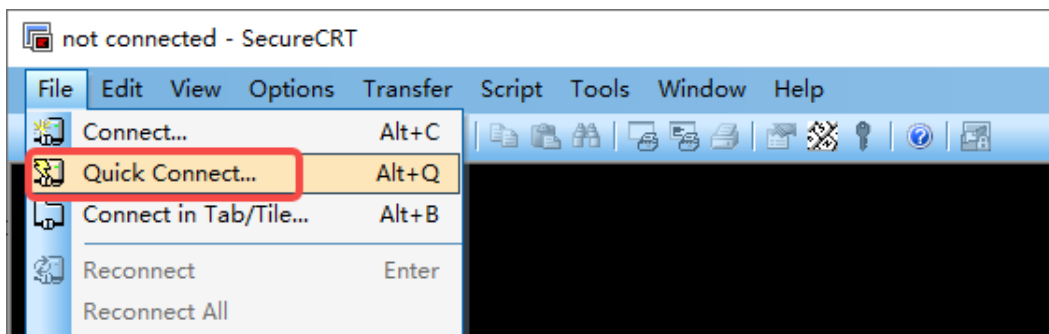
- b In the **Access Management** area, select **SSH** (ping function disabled on the interface by default) and click **Save**.

(2) Manage the device using SSH.

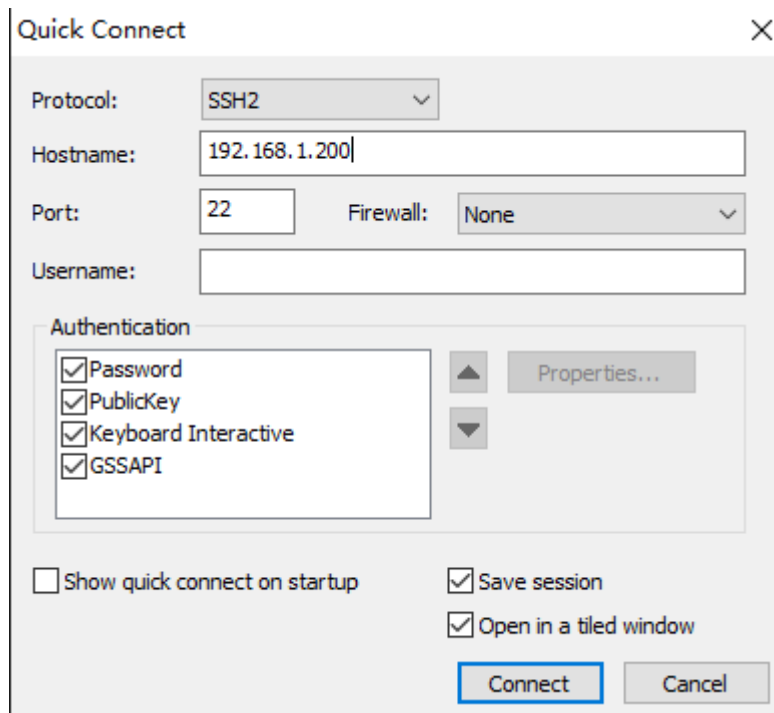
Create an SSH connection using the terminal simulation software (such as SecureCRT), and enter the username and password (for login to the web management page) to manage the device.

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 dialog box configuration:

- Protocol: SSH2
- Hostname: 192.168.1.200
- Port: 22
- Firewall: None
- Username: (empty)
- Authentication: Password, PublicKey, Keyboard Interactive, GSSAPI (all checked)
- Save session: checked
- Open in a tiled window: checked
- Show quick connect on startup: unchecked

- 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.

The screenshot displays the Ruijie Series Firewall management interface. The top navigation bar includes 'Home', 'Monitor', 'Network', 'Object', 'Policy', and 'System'. The 'System' menu is expanded, showing options like 'Network Discovery', 'Network Mgmt', 'Quick Onboarding', 'Policy Wizard', 'Customer Service', and 'admin'. On the left, a sidebar menu lists 'Admin', 'System Config', 'System Time', 'SNMP', 'Service Parameters', 'Authorization Management', 'Fault Diagnosis', 'Cloud Management Platform', 'Signature Library Upgrade', and 'System Maintenance'. The main content area is titled 'Advanced Settings' and contains the following configuration fields:

- 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

At the bottom of the configuration area, there are two buttons: 'Save' and '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 <a href="#">6.1 Integrated Deployment on Ruijie Cloud</a> .	[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.	<ul style="list-style-type: none"> <li>● Enter an integer in the range of 0 to 1440, in minutes.</li> <li>● The default value is 30 minutes.</li> </ul> [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.	<ul style="list-style-type: none"> <li>● Enter an integer in the range of 0 to 10.</li> <li>● The default value is 6.</li> </ul> [Example] 3
Lockout Period	Period of time within which the automatically locked user is not allowed to log in to the web management page.	<ul style="list-style-type: none"> <li>● Enter an integer in the range of 0 to 30, in minutes.</li> <li>● The default value is 3.</li> </ul> [Example] 30
Verification Code	Whether a verification code is required for login to the web management page.	By default, the value is <b>Enable</b> . [Example] <b>Enable</b>

(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 <b>Admin</b> menus under <b>System</b> Read-write permissions on other menus	securityadmin
Auditor	Read permission on <b>Home</b> menus Read permission on <b>Monitor</b> menus No permissions on other menus	auditadmin
User Admin	Read permission on <b>Home</b> menus Read-write permissions on <b>Admin</b> menus under <b>System</b> 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.

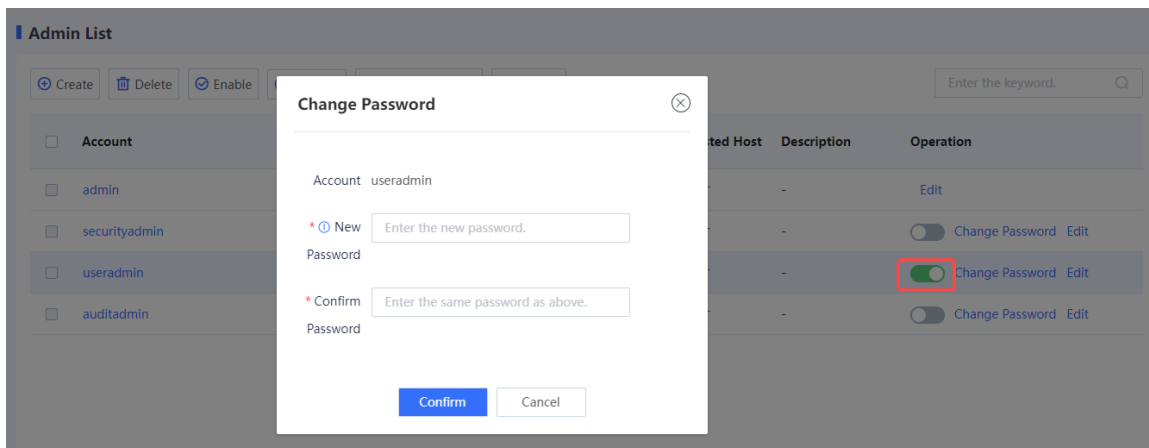
**Procedure**

- (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.



- (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

\* Enabled State  Enable  Disable

\* Role

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

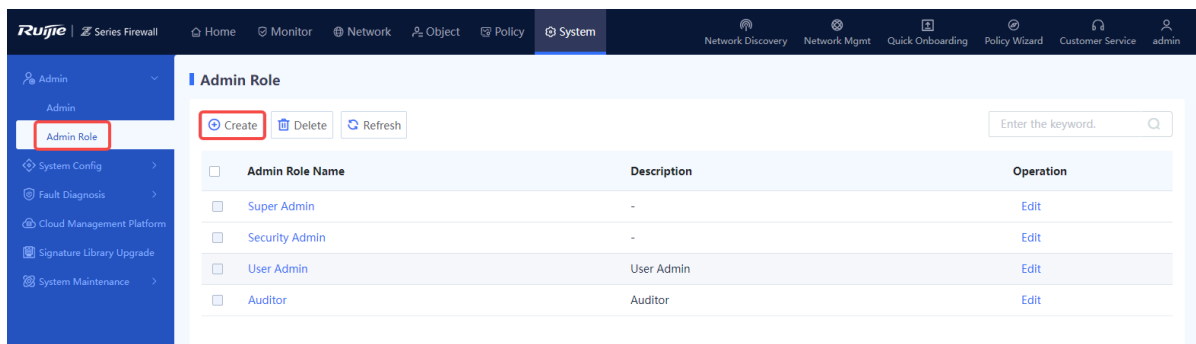
### 1. Creating an Administrator Role

#### 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**.



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

< Back
**Add Admin Role**

**Basic Info**

\* Admin Role Name

Description

**Permission Settings**

Permission	<input checked="" type="radio"/> Read-Write	<input type="radio"/> Read-Only	<input type="radio"/> None
> Monitor	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> Network	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> Object	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> Policy	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> System	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> Quick Onboarding	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> Policy Wizard	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Save

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
<b>Permission Settings</b>		
Permission	Web page functions that can be operated by the new administrator role.	[Example] Monitor
Permission Settings	Different modules have different permissions, including: <b>Read-Write:</b> View, add, delete, and edit permissions <b>Read-Only:</b> View permission only <b>None:</b> No permission at all	[Example] Read-Only

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

## 2. Creating an Administrator Account

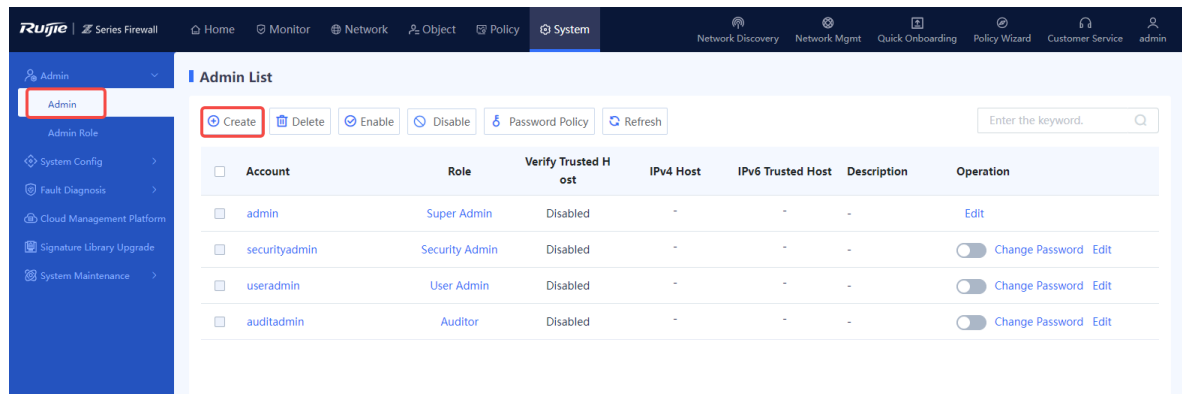
### Application Scenario

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**.



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

< Back

### Add Admin Account

**Basic Info**

\* Account

\* Enabled State  Enable  Disable

\* Role

Description

---

**Advanced**

\*

\*

---

**Configure Trusted Host**

Restrict Trusted Host Login

[Delete](#)

[+ Add IPv4 Trusted Host](#)

[Delete](#)

[+ Add IPv6 Trusted Host](#)

Item	Description	Remarks
<b>Basic Info</b>		
Account	Username of the created administrator.	<ul style="list-style-type: none"> <li>The username can contain letters, digits, and underscores (_), and must start with a letter.</li> <li>The value cannot be the same as an existing administrator username.</li> </ul> <p>[Example] Admin_security</p>

Item	Description	Remarks
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
<b>Advanced</b>		
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
<b>Configure Trusted Host</b>		
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 Host 1	Enter the IPv4 address of a trusted host.	[Example] 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

\* Maximum Password  Day

Age

- (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.

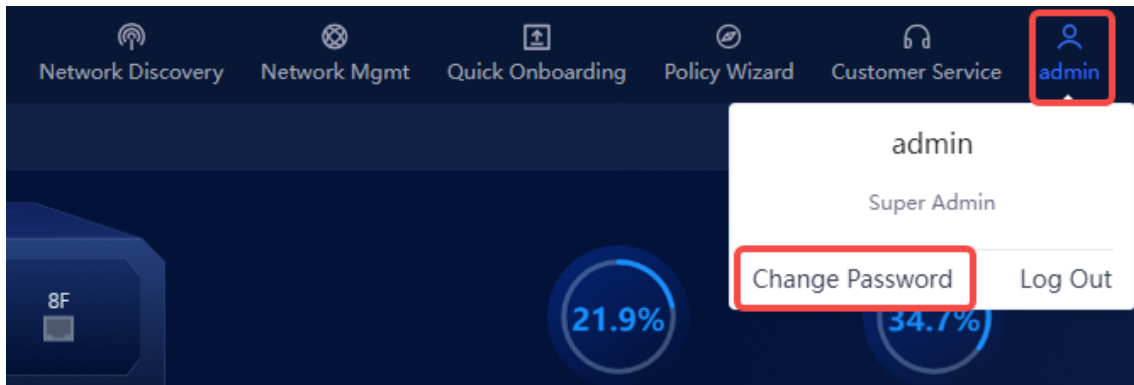
## 2. Changing the Default User Password of the Super Admin

### 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.

**Change Password** ⊗

---

\* Old Password

\* 🔒 New Password

\* 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.	<p>The new password must meet the following requirements:</p> <ul style="list-style-type: none"> <li>● Contain 8 to 15 characters.</li> <li>● 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.</li> <li>● Cannot be the same as the username or the username in reverse order.</li> </ul>
Confirm Password	Password after change that is entered again.	The value of <b>Confirm Password</b> must be the same as that of <b>New Password</b> .

(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

\* ⓘ New Password

\* Confirm Password

(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

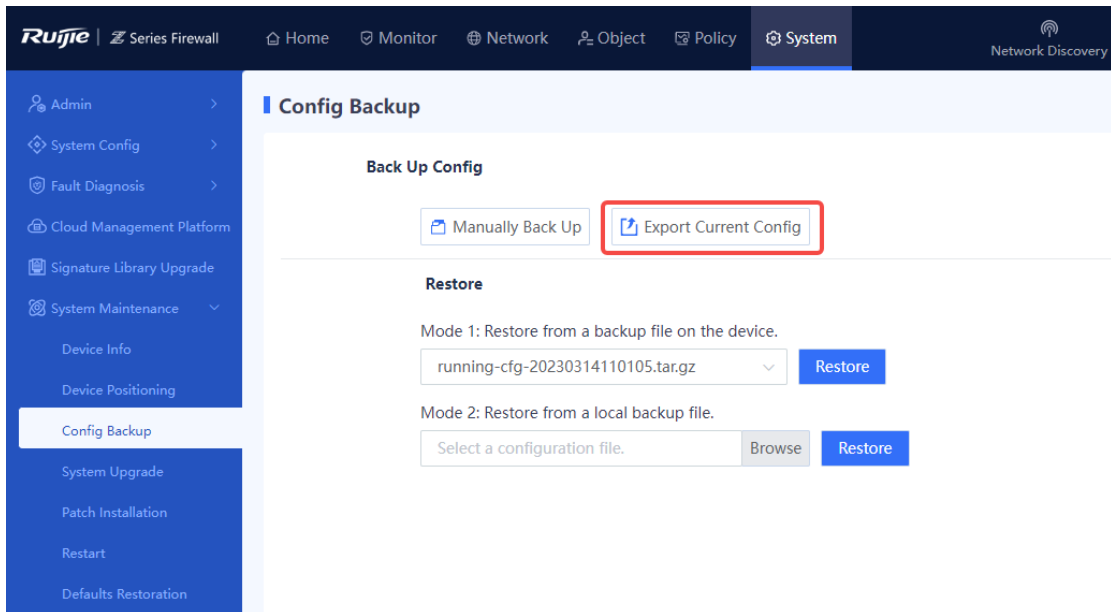
### 2.4.1 Exporting the Configuration

#### Application Scenario

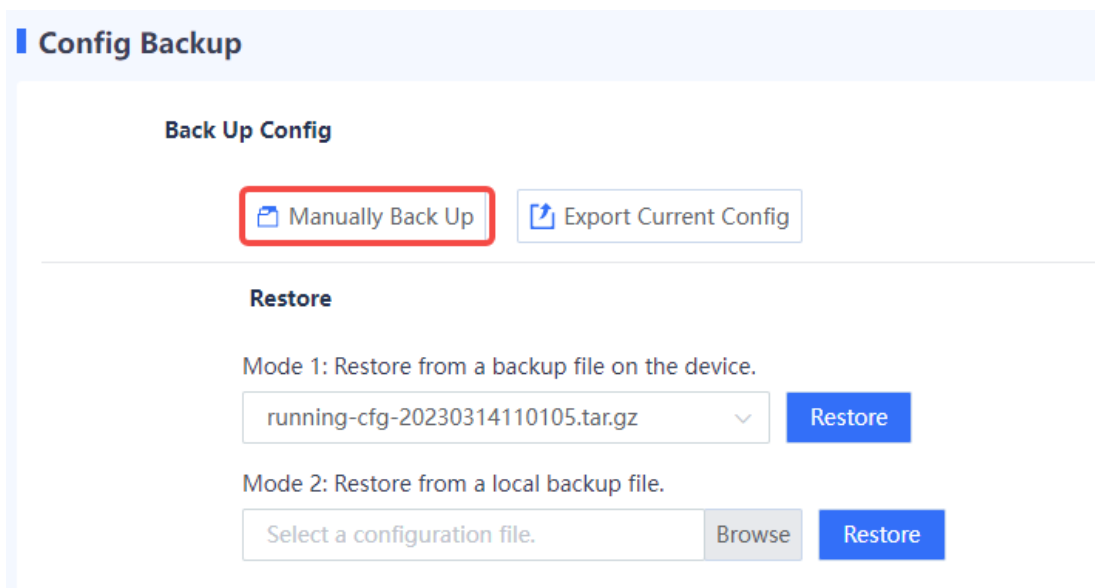
An administrator can use the configuration backup function to manually back up the current configuration or export the current system configuration file to facilitate subsequent restoration or batch configuration.

#### 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.



## 2.4.2 Importing the Configuration

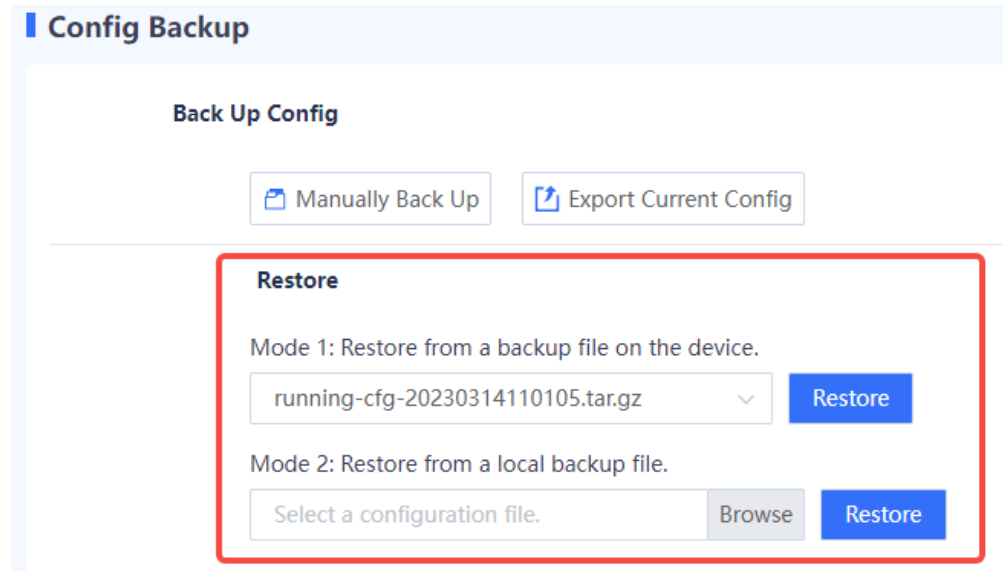
### Application Scenario

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.



- (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.

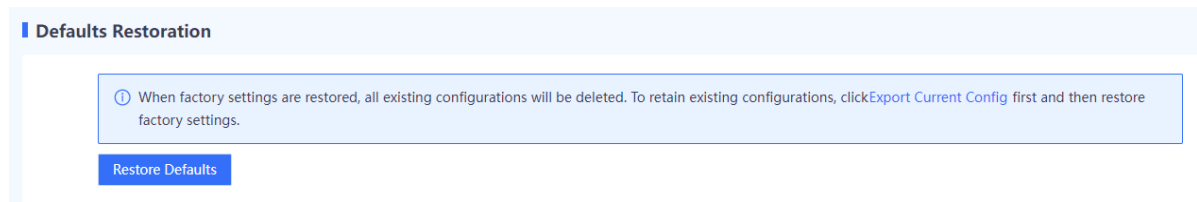
### 2.5.1 Web-based One-Click Restoration

**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**.



### 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

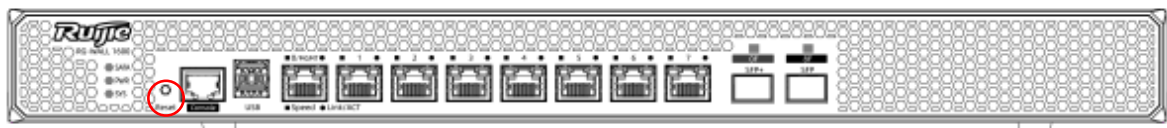
### Application Scenario

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.

---

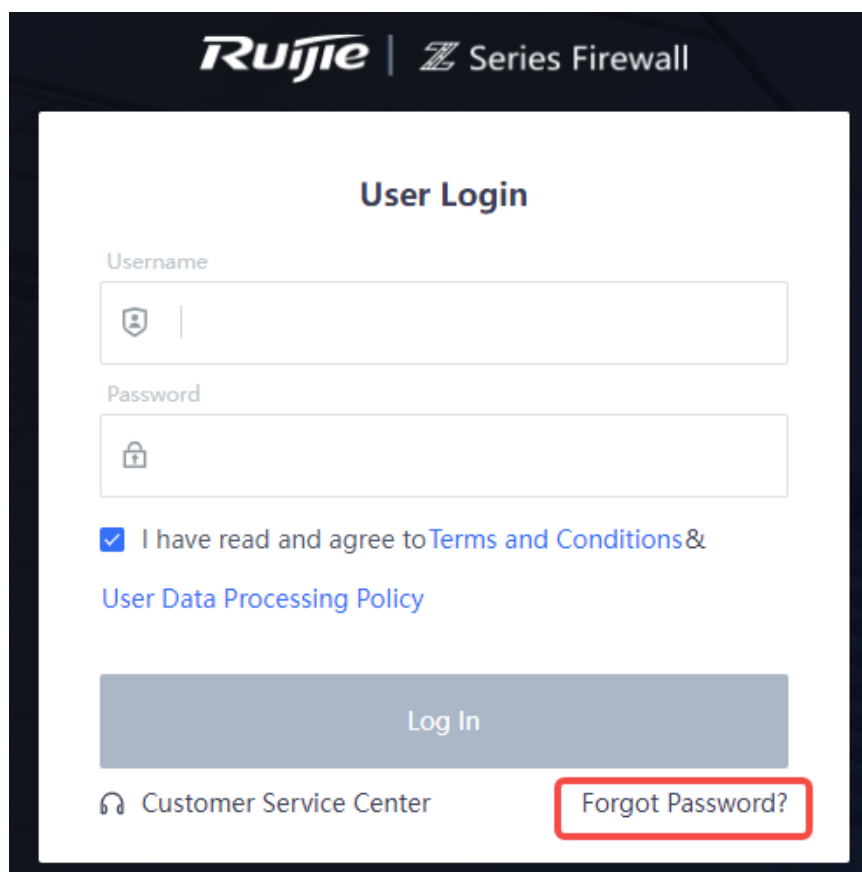
## 2.6 Password Restoration

### 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.



The screenshot shows the 'User Login' interface for the Ruijie Z Series Firewall. At the top, the Ruijie logo and 'Z Series Firewall' are displayed. The main heading is 'User Login'. Below this, there are two input fields: 'Username' with a user icon and 'Password' with a lock icon. A checkbox is checked, indicating agreement to the 'Terms and Conditions & User Data Processing Policy'. A 'Log In' button is positioned below the fields. At the bottom, there is a 'Customer Service Center' link and a 'Forgot Password?' link, which is highlighted with a red rectangular border.

- (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



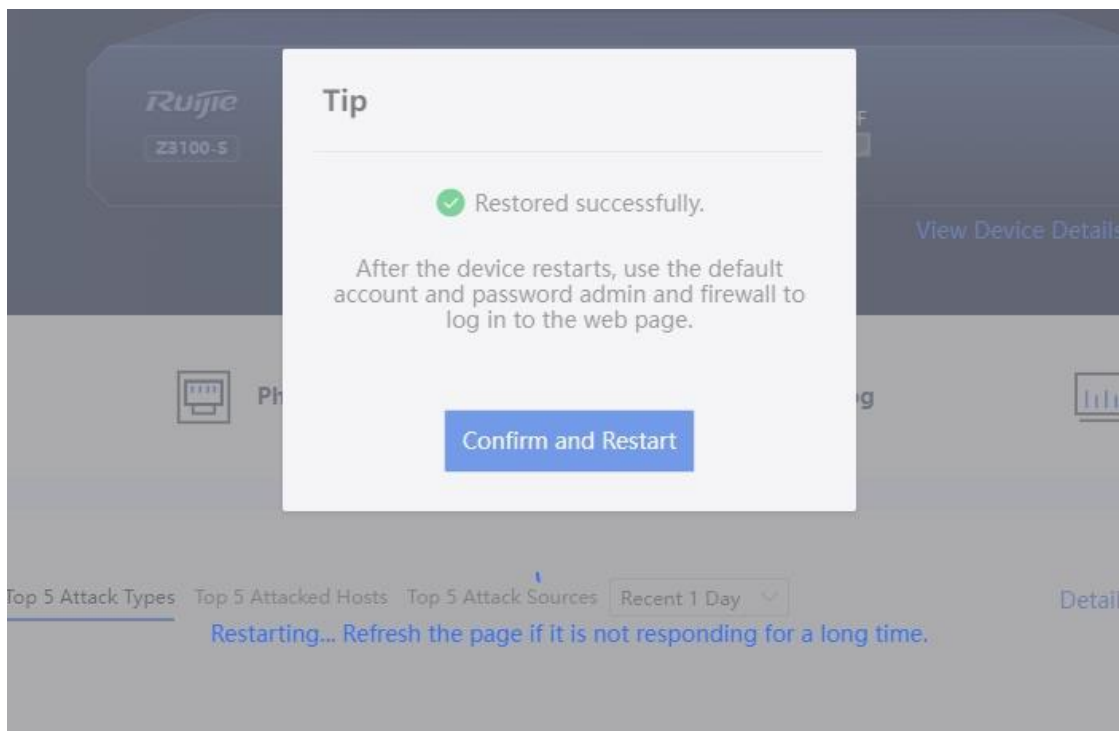
Restoring... Refresh the page if it is not responding for a long time.

### Tip

✔ Restored successfully.

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

Confirm and Restart



✔ Restart succeeded.

Restart succeeded. Please log in again.  
Refresh the page and try again later if the server does not respond.

Got It

- 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

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

## 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.

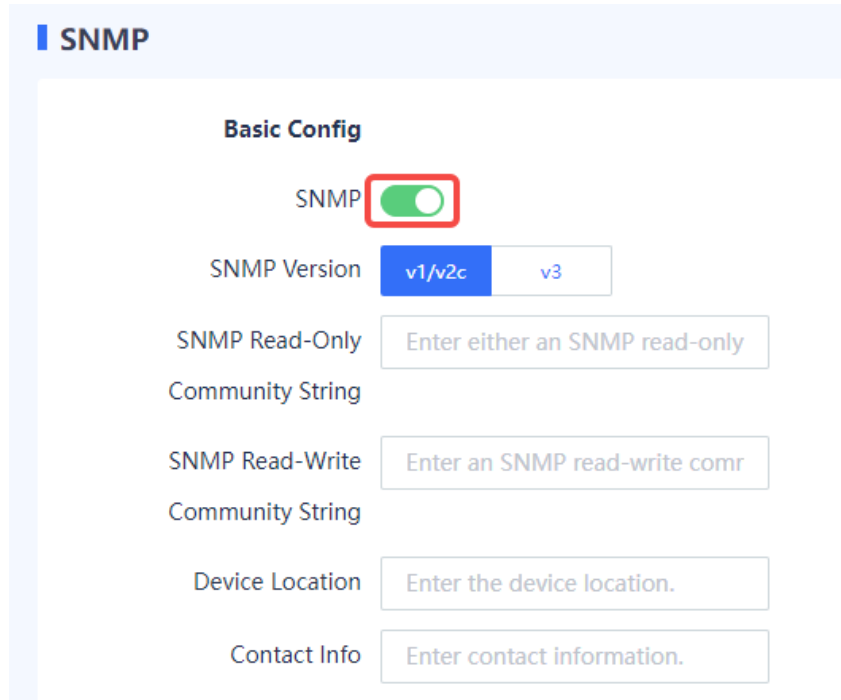
## 2.7.2 Configuring SNMP

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

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

The screenshot shows the Ruijie Series Firewall configuration interface for SNMP. The left sidebar contains navigation options like Admin, System Config, and various service parameters. The main content area is titled 'SNMP' and is divided into 'Basic Config' and 'Trap Receiver' sections. In the 'Basic Config' section, the 'SNMP' toggle is currently turned off. The 'SNMP Version' is set to 'v1/v2c'. There are input fields for 'SNMP Read-Only Community String', 'SNMP Read-Write Community String', 'Device Location', and 'Contact Info'. The 'Trap Receiver' section shows a configuration for 'Trap Receiver1' with fields for IP address, Port (162), Type (TRAP2), and Security Username. A 'Save' button is visible at the bottom of the configuration area.

(2) Enable **SNMP**.



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

Item	Description	Remarks
SNMP Version	Version number of SNMP. The options are <b>v1/v2c</b> and <b>v3</b> .	The selected version must match that of the NMS server.  [Example]  v3
SNMP Version: v1/v2c		
SNMP Read-Only Community String	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.	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
SNMP Read-Write	Community name used for authentication between the	The value must be the same as the read-write community name on the

Item	Description	Remarks
Community String	<p>managed device and NMS server.</p> <p>If the NMS user uses a read-write community name for authentication, the user possesses the read-write permission on device configuration.</p>	<p>NMS. Otherwise, access from the NMS to the device may fail.</p> <p>Characters such as `~!#%^&amp;*+ \{;:'"/&lt;&gt;? and spaces are not allowed.</p> <p>[Example]</p> <p>private</p>
SNMP Version: v3		
Security Username	Username used by the NMS user to access the managed device.	<p>The value must be the same as that on the NMS.</p> <p>Characters such as `~!#%^&amp;*+ \{;:'"/&lt;&gt;? and spaces are not allowed.</p> <p>[Example]</p> <p>user1</p>
Authentication Algorithm	Authentication algorithm used to verify the user identity. MD5 and SHA algorithms are supported.	<p>The value must be the same as that on the NMS.</p> <p>[Example]</p> <p>MD5</p>
Authentication Key	Password used to verify whether the NMS user is valid.	<p>The value must be the same as the authentication password configured on the NMS.</p> <p>[Example]</p> <p>authkey</p>
Encryption Algorithm	Encryption algorithm used to encrypt the transmitted data. AES and DES algorithms are supported.	<p>The value must be the same as that on the NMS.</p> <p>[Example]</p> <p>AES</p>
Encryption Key	Password used to encrypt the	The value must be the same as the encryption password configured on

Item	Description	Remarks
	transmitted data.	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 get in touch with the device-related personnel.	-
Trap Receiver Click <b>Create</b> 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 <b>TRAP</b> , <b>TRAP2</b> , and <b>INFORM</b> .	The type is <b>TRAP2</b> 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)	<ul style="list-style-type: none"> <li>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.</li> <li>Each license provides the upgrade service of the IPS signature library of one year.</li> </ul>
			App identification (app/URL)	<ul style="list-style-type: none"> <li>This license upgrades the app identification signature library to identify Internet applications and limit and control the Internet application access of users.</li> <li>Each license provides the</li> </ul>

Category	Industry Attribute	Effective Time	License Type	Description
				upgrade service of the app identification signature library of one year.
			Antivirus (AV)	<ul style="list-style-type: none"> <li>● 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.</li> <li>● Each license provides the upgrade service of the AV signature library of one year.</li> </ul>
			Threat Intelligence (TI)	<ul style="list-style-type: none"> <li>● 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.</li> <li>● Each license provides the upgrade service of the TI signature library of one year.</li> </ul>

## 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

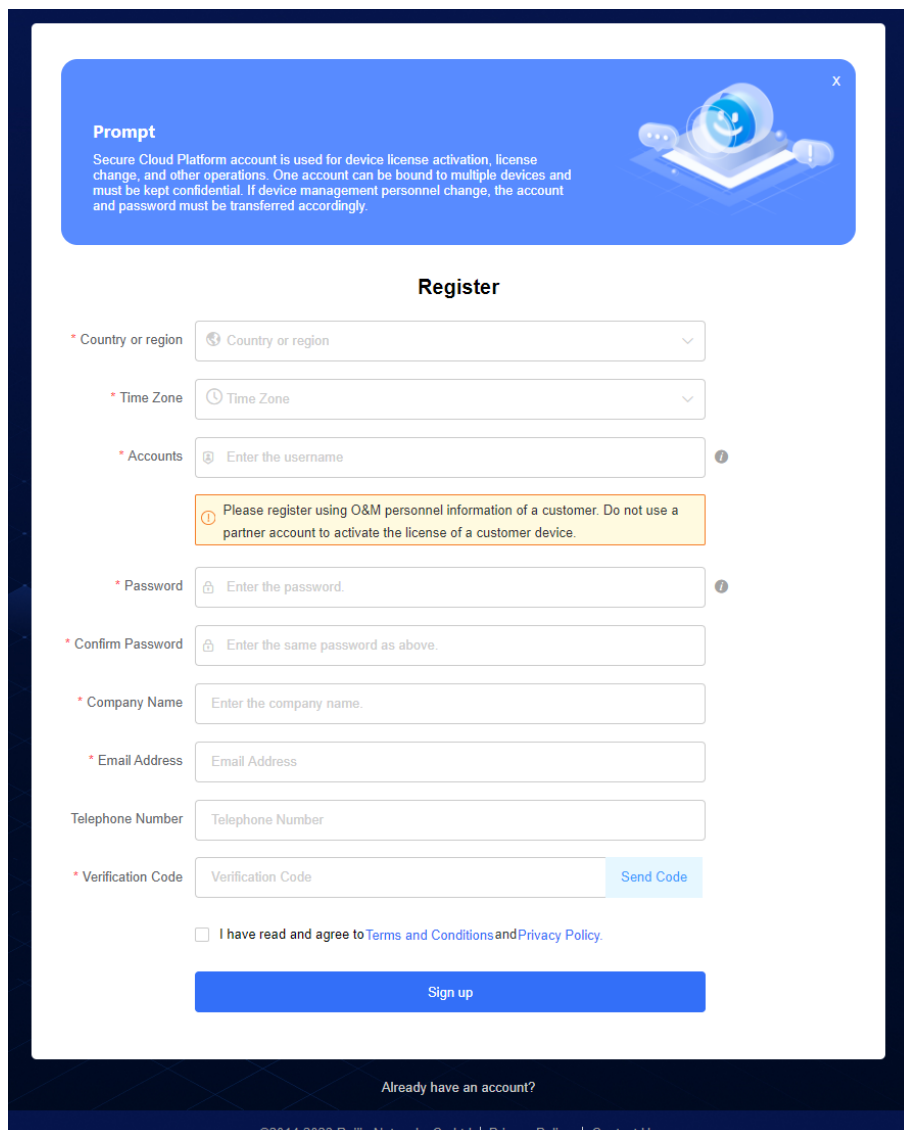
### 1. User Registration and Login

(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

\* Time Zone

\* Accounts  ⓘ

ⓘ 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  ⓘ

\* Confirm Password

\* Company Name

\* Email Address

Telephone Number

\* Verification Code

I have read and agree to [Terms and Conditions](#) and [Privacy Policy](#).

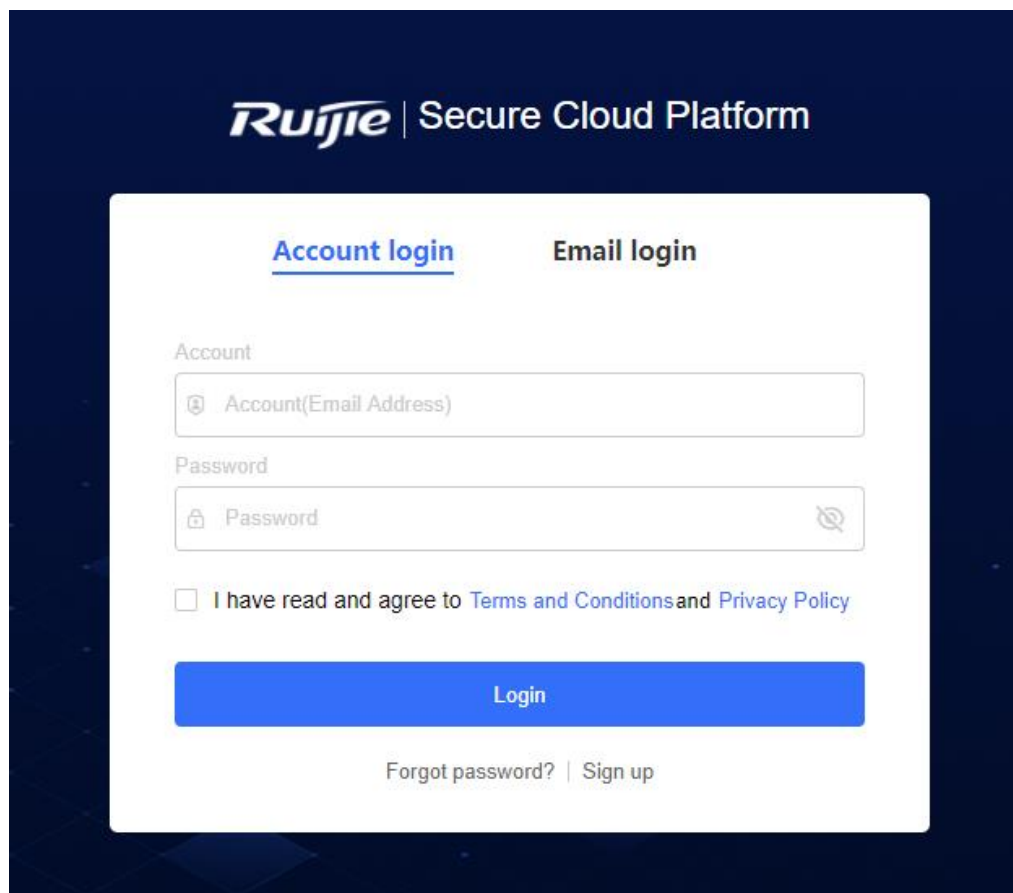
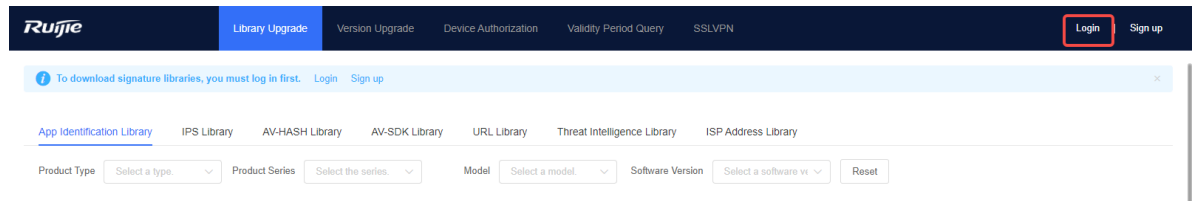
[Already have an account?](#)

©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.

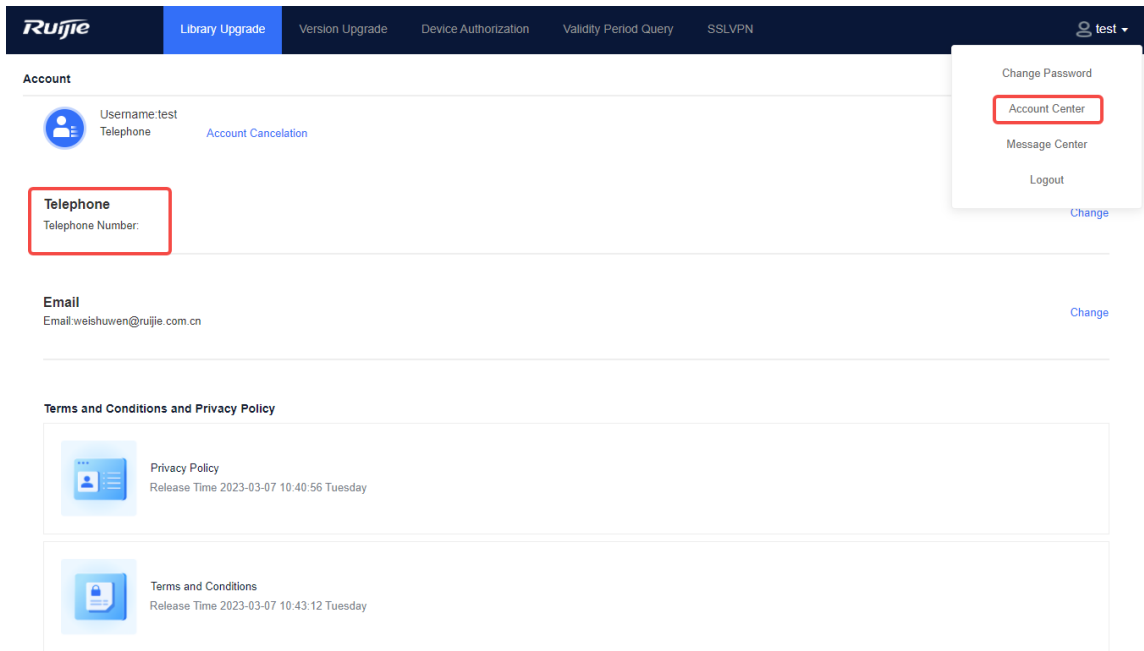
If the login page is not displayed, click **Login** in the upper right corner of the home page.



(3) Modify personal information.

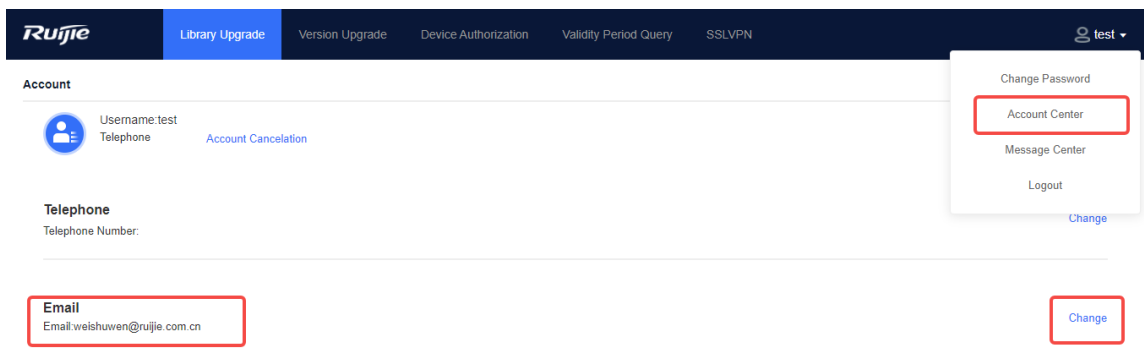
a Modify the mobile number.

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.



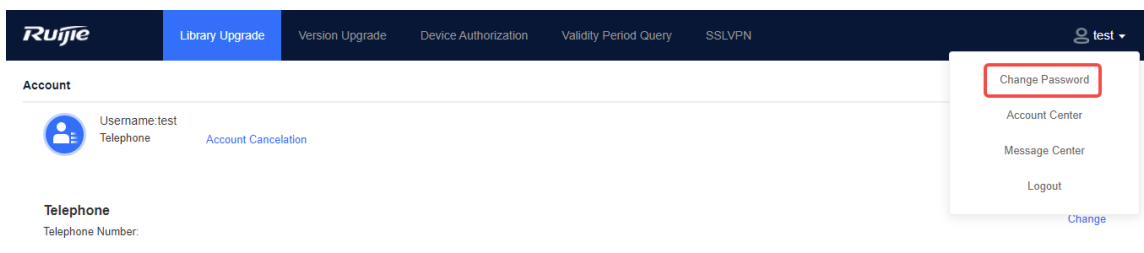
b Modify the email address.

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.



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.



## 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

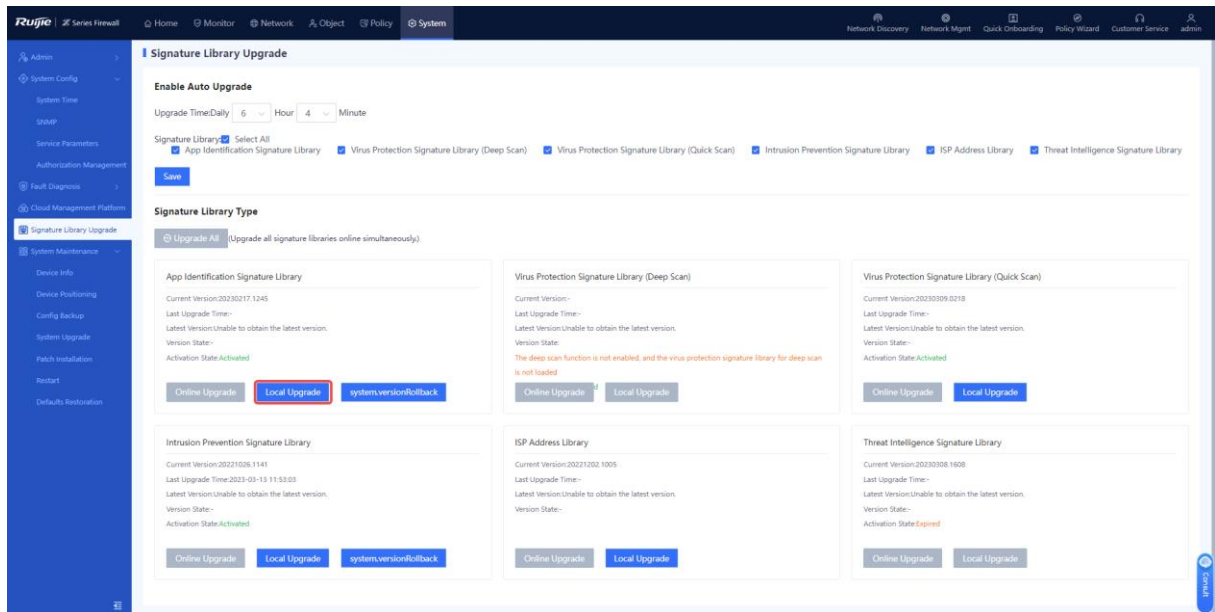
(1) Download a version file for the app identification signature library.

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

The screenshot shows the Ruijie Secure Cloud Platform interface. The top navigation bar includes 'Library Upgrade', 'Version Upgrade', 'Device Authorization', 'Validity Period Query', and 'SSLVPN'. The 'Library Upgrade' menu is highlighted in red. Below it, the 'App Identification Library' sub-menu is also highlighted. The interface includes filters for Product Type, Product Series, Model, and Software Version, along with a 'Reset' button. A table lists available signature library versions with columns for No., File Name, Version Number, Version Description, Model, Software Version, Release Date, File Size (MB), MD5, and Operation. The 'Download' button for the first entry is highlighted in red.

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	27e2a4b58f08...	<a href="#">Download</a>
2	app_signature_...	20230302	lyf-app-full.202...	Z5100-test	NGFW_NTOS ...	2022-12-31	358.46	dad9a1eafe1b...	<a href="#">Download</a>
3	app_signature_...	20230303	lyf-app-full.202...	Z5100-test	NGFW_NTOS ...	2022-12-31	358.46	dad9a1eafe1b...	<a href="#">Download</a>
4	app_signature_...	20220807.1404	lyf-app-full.202...		Universal	2022-12-01	0.77	651ad40cd19a...	<a href="#">Download</a>
5	app_signature_...	20220810.1104	lyf-app-full.202...		Universal	2022-08-10	0.42	3633948d57de...	<a href="#">Download</a>
6	app_signature_...	20220711.1629	hjqtest-app: 2...		Universal	2022-07-11	0.40	1c5c6cee7240...	<a href="#">Download</a>

(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).



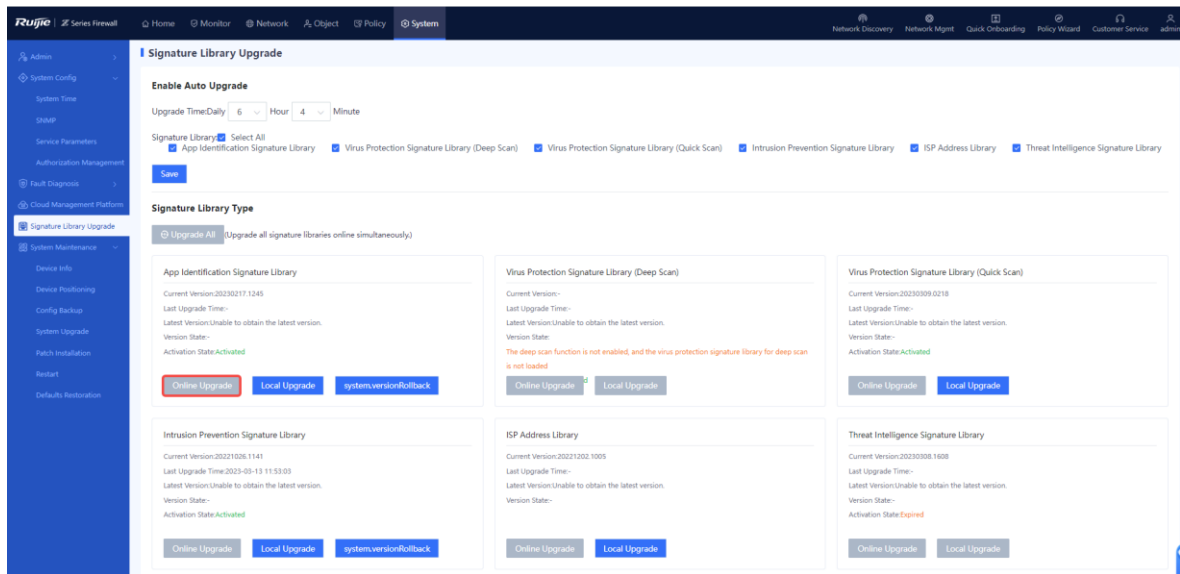
- Online upgrade

**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.

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...	<b>New version</b> ↓ 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 <b>Original version</b>
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.



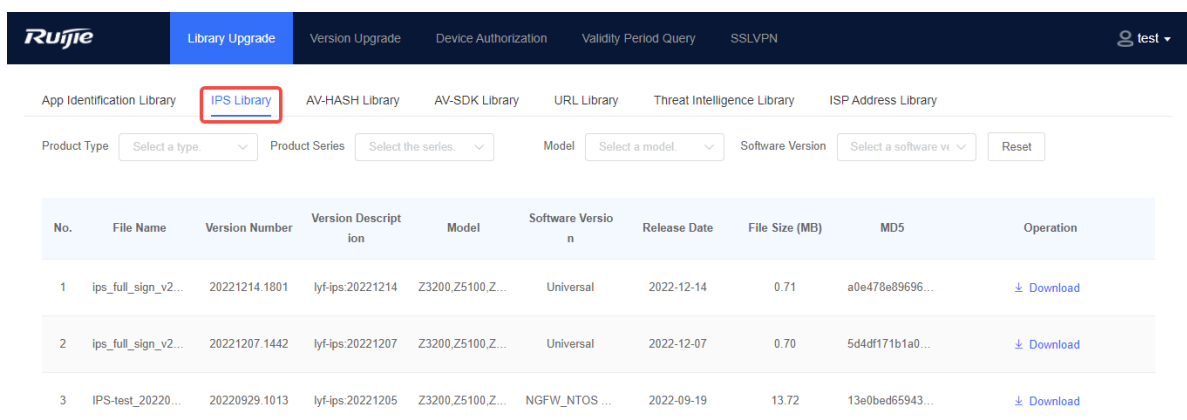
### 3. IPS Signature Library Upgrade

#### Prerequisites

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

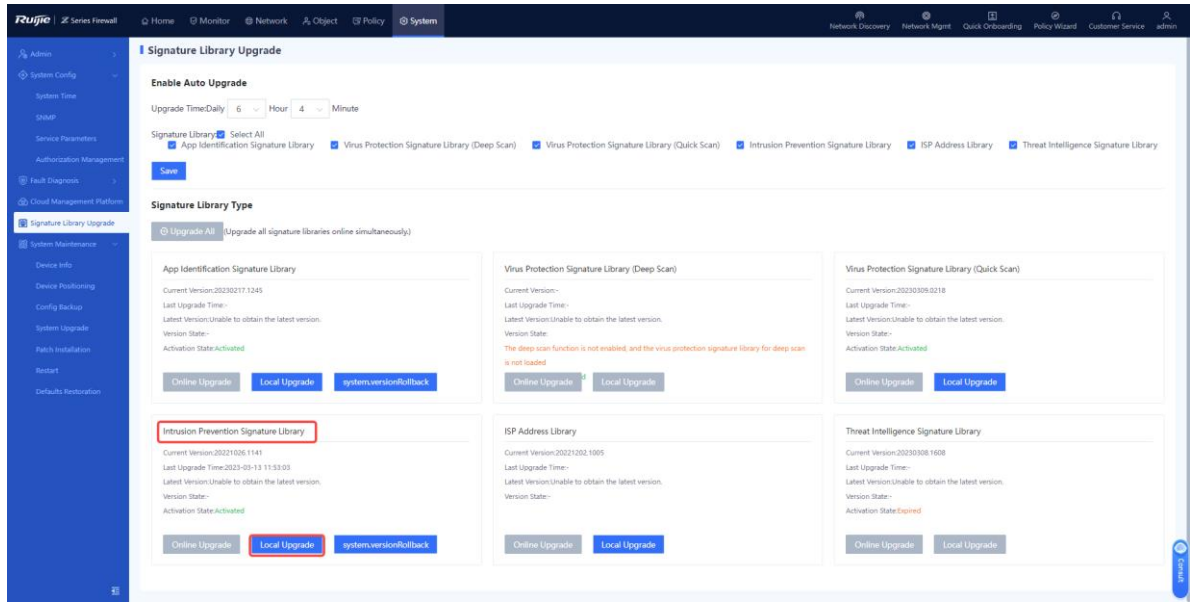
#### Procedure

- 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.





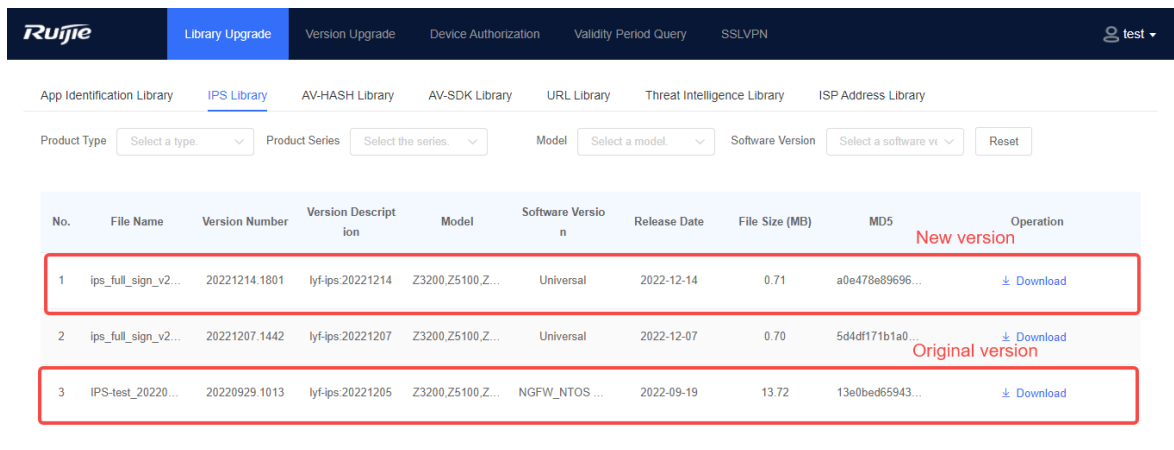
(2) After the version file is downloaded, choose **System > Signature Library Upgrade** on the firewall to upgrade the IPS signature library in offline mode (local upgrade).



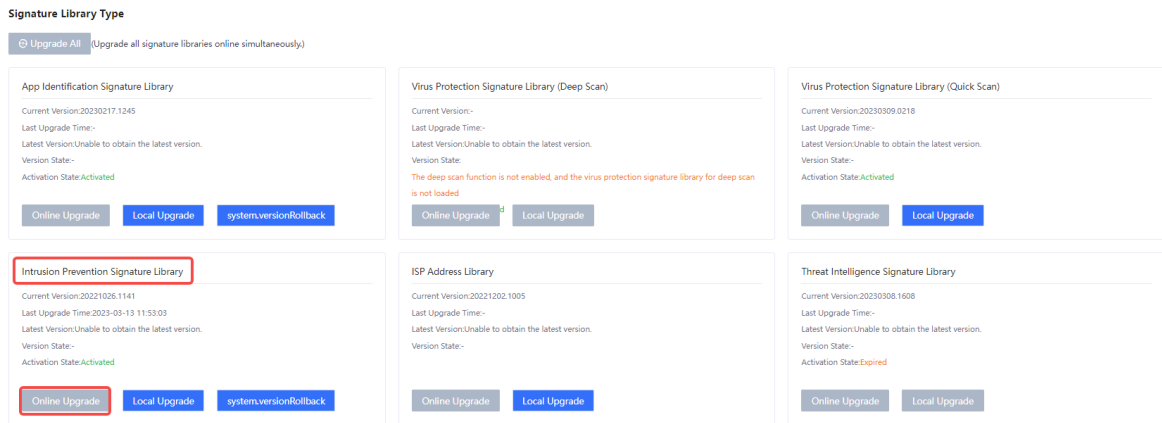
- Online upgrade

**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.



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



### 4. Virus Protection (Quick Scan) Signature Library Upgrade

#### Prerequisites

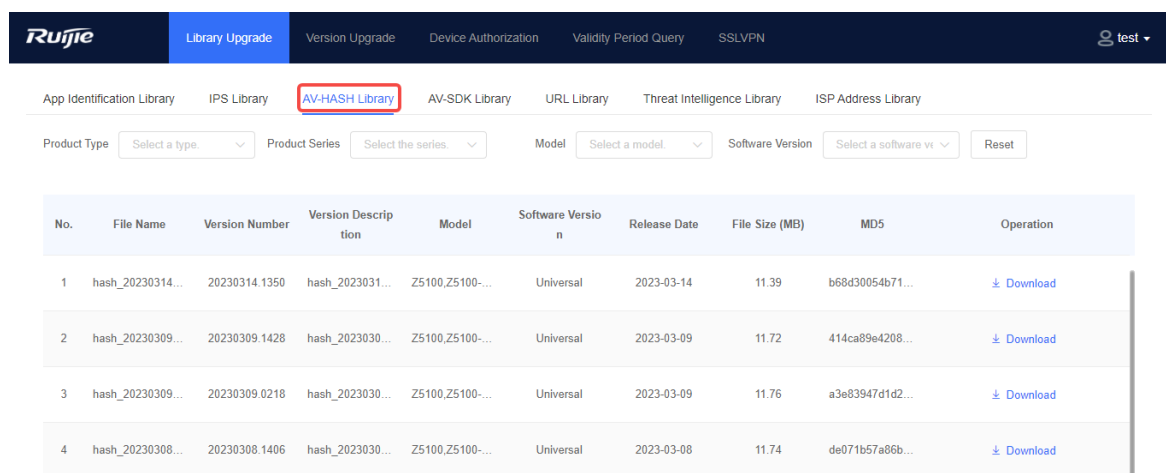
The Antivirus (AV) license has been activated for the firewall and the license is within the validity period.

#### Procedure

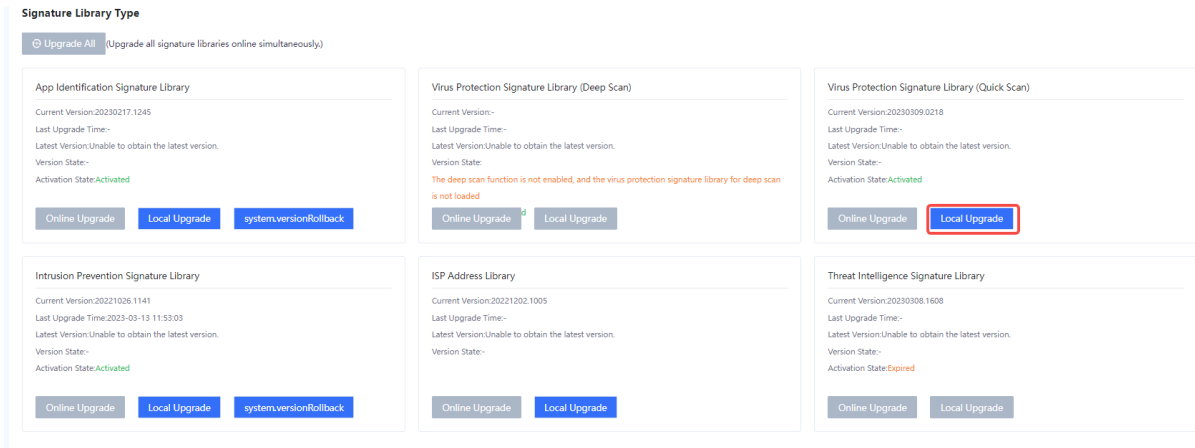
- Offline upgrade

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

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



(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.

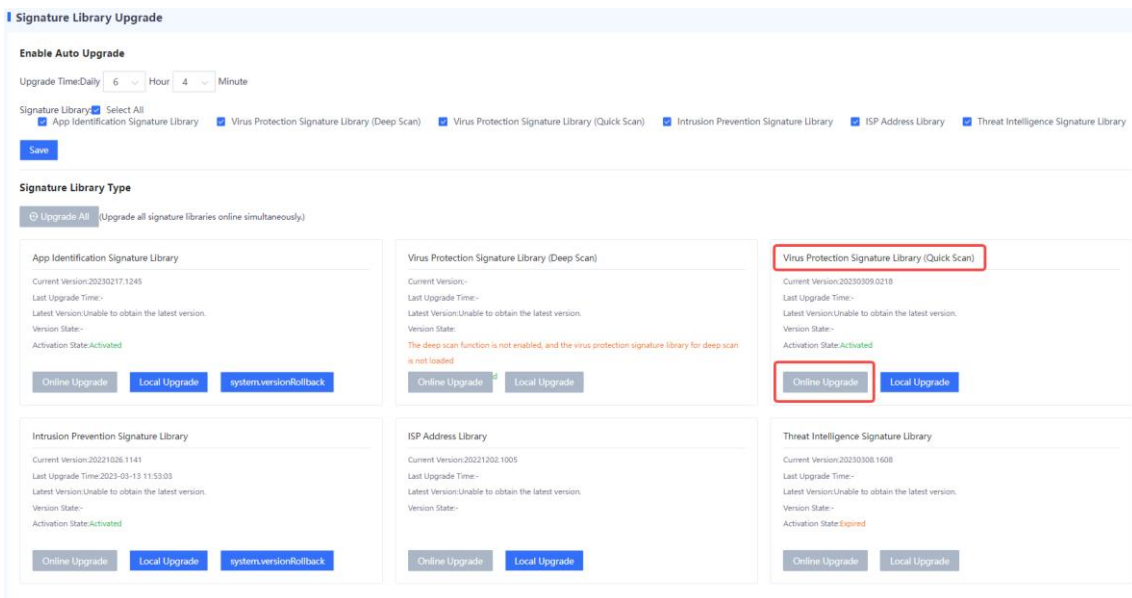


- Online upgrade

**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.



## 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.

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

The screenshot shows the 'Library Upgrade' section of the Ruijie Secure Cloud Platform. The 'AV-SDK Library' is selected. Below the navigation bar, there are filters for Product Type, Product Series, Model, and Software Version. A table lists four available versions of the AV-SDK library, each with a 'Download' button in the 'Operation' column.

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.

The screenshot shows the 'Signature Library Type' upgrade interface. It features a 'Signature Library Type' header and a 'Upgrade All' button. Below, there are six panels for different signature libraries: App Identification, Virus Protection (Deep Scan), Virus Protection (Quick Scan), Intrusion Prevention, ISP Address, and Threat Intelligence. The 'Virus Protection Signature Library (Deep Scan)' panel has a red box around its 'Local Upgrade' button. The 'Virus Protection Signature Library (Quick Scan)' panel shows an 'Expired' activation 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 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

[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](#)

## 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.

The screenshot shows the Ruijie management interface with the 'Library Upgrade' menu selected. The 'ISP Address Library' sub-menu is active. Below the navigation tabs, there are filters for Product Type, Product Series, Model, and Software Version, along with a 'Reset' button. A table lists available versions for download.

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...	<a href="#">Download</a>
2	isp_20221030.1...	20221030.1000	isp_20221030....	Z5100,Z5100-...	Universal	2022-10-30	0.01	0ABAF66F14A...	<a href="#">Download</a>

- (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 (Upgrade all signature libraries online simultaneously.)

<p><b>App Identification Signature Library</b></p> <p>Current Version:20230217.1245                  Last Upgrade Time:-                  Latest Version:Unable to obtain the latest version.                  Version State:-                  Activation State:Activated</p> <p>Online Upgrade Local Upgrade system.versionRollback</p>	<p><b>Virus Protection Signature Library (Deep Scan)</b></p> <p>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</p> <p>Online Upgrade Local Upgrade</p>
<p><b>Intrusion Prevention Signature Library</b></p> <p>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</p> <p>Online Upgrade Local Upgrade system.versionRollback</p>	<p><b>ISP Address Library</b></p> <p>Current Version:20221202.1005                  Last Upgrade Time:-                  Latest Version:Unable to obtain the latest version.                  Version State:-</p> <p>Online Upgrade Local Upgrade</p>

- 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.

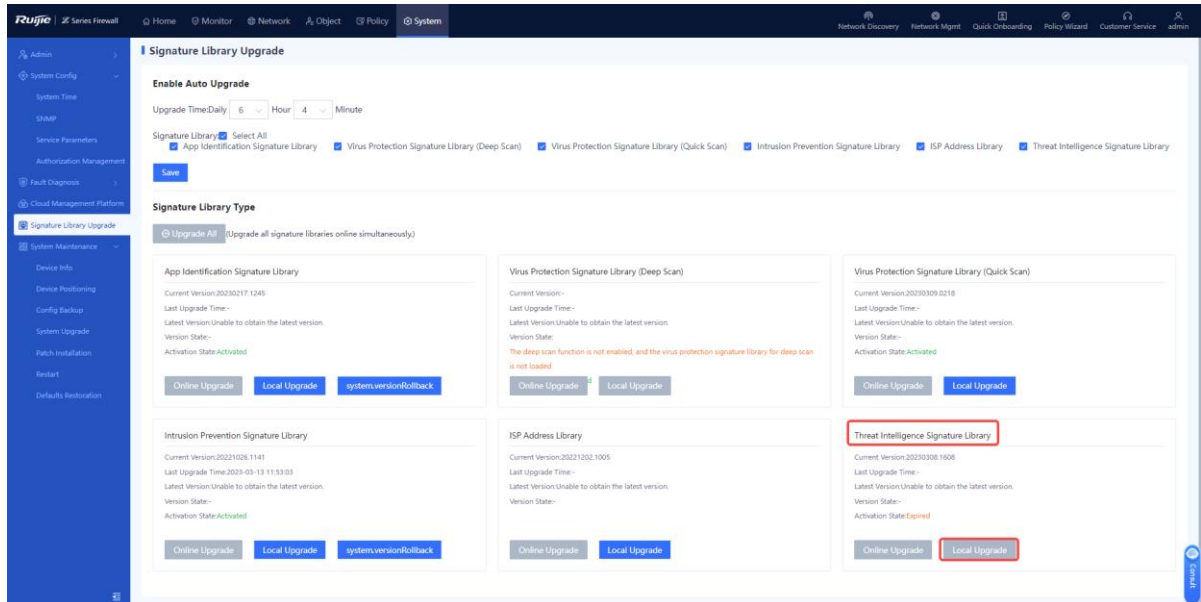
### Procedure

- 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.

The screenshot shows the Ruijie management interface. The top navigation bar includes 'Library Upgrade', 'Version Upgrade', 'Device Authorization', 'Validity Period Query', and 'SSLVPN'. Under 'Library Upgrade', the 'Threat Intelligence Library' tab is selected and highlighted with a red box. Below the tabs, there are filters for 'Product Type', 'Product Series', 'Model', and 'Software Version', along with a 'Reset' button. A table lists three available upgrade files for the Threat Intelligence Library.

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...	<a href="#">Download</a>
2	ti_20230307.16...	20230307.1604	ti_20230307.1...	Z5100,Z5100-...	Universal	2023-03-07	14.42	d901b8b2af50...	<a href="#">Download</a>
3	ti_20230306.16...	20230306.1602	ti_20230306.1...	Z5100,Z5100-...	Universal	2023-03-06	14.53	c35f98822b87...	<a href="#">Download</a>

- (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.



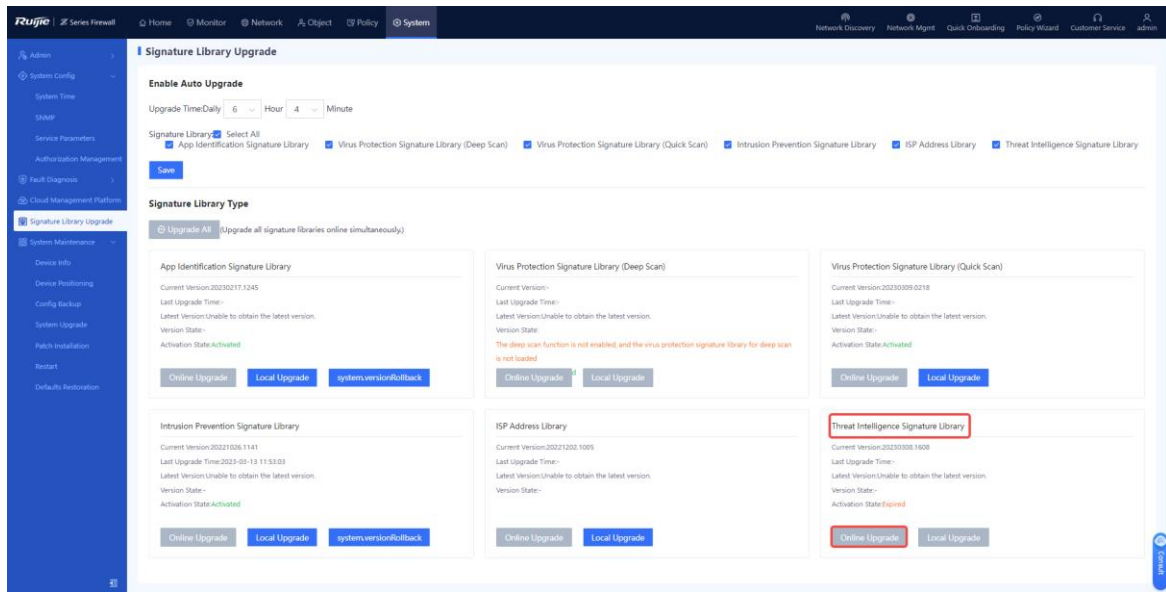
- Online upgrade

### **i** 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.



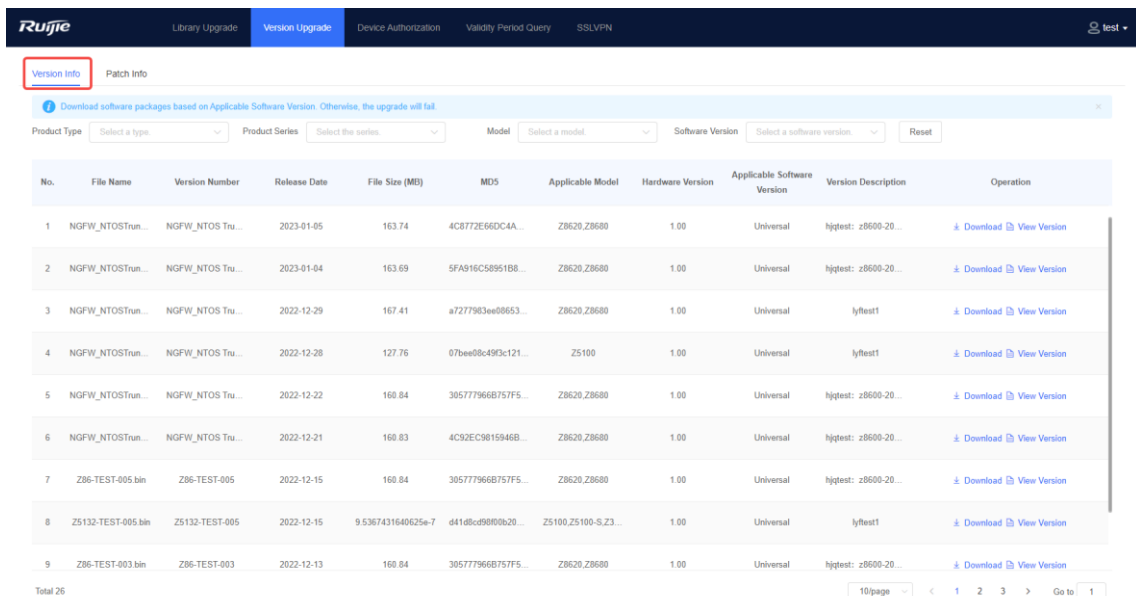


## 8. System Upgrade

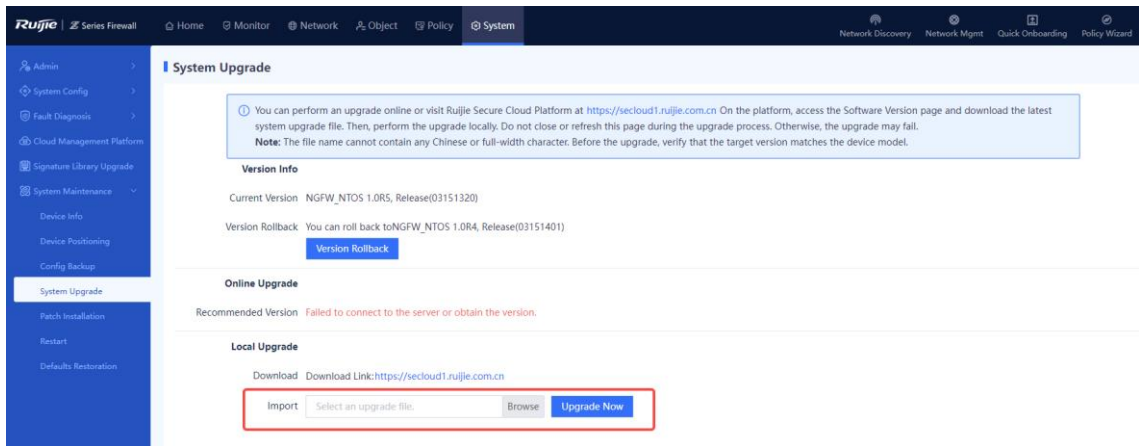
- Offline upgrade

(1) Download a device version.

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



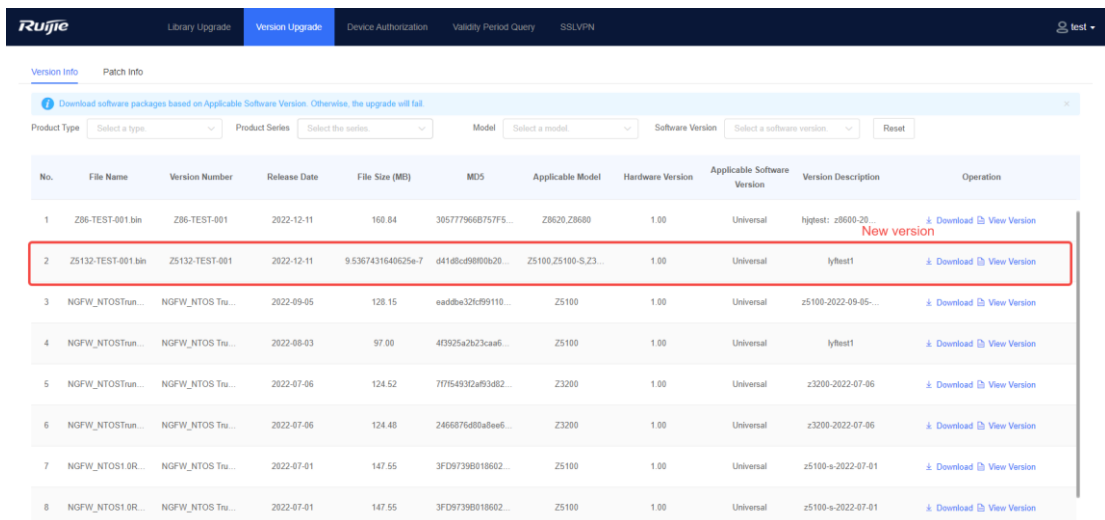
- (2) After the version upgrade file is downloaded, choose **System > System Maintenance > System Upgrade** on the firewall, upload the upgrade file, and perform offline upgrade (local upgrade) of the device system version.



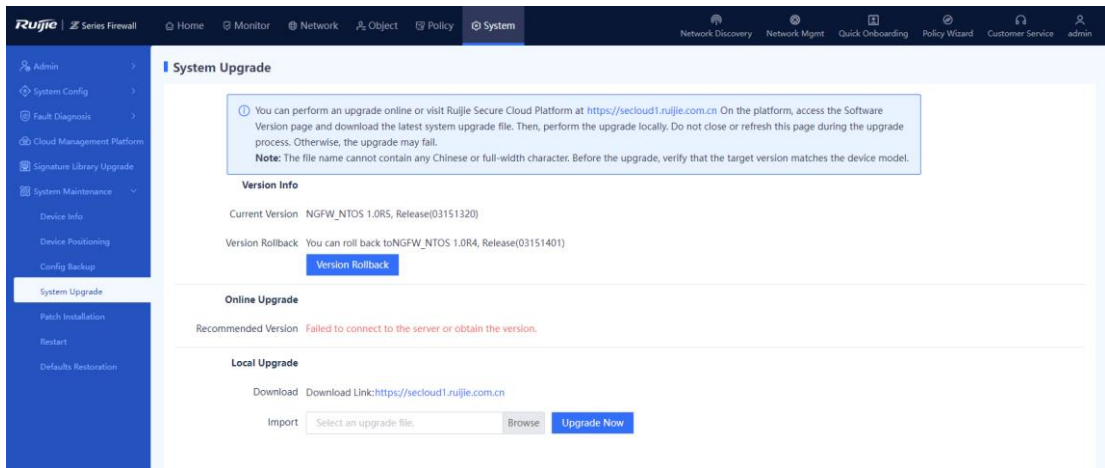
- Online upgrade

**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.



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



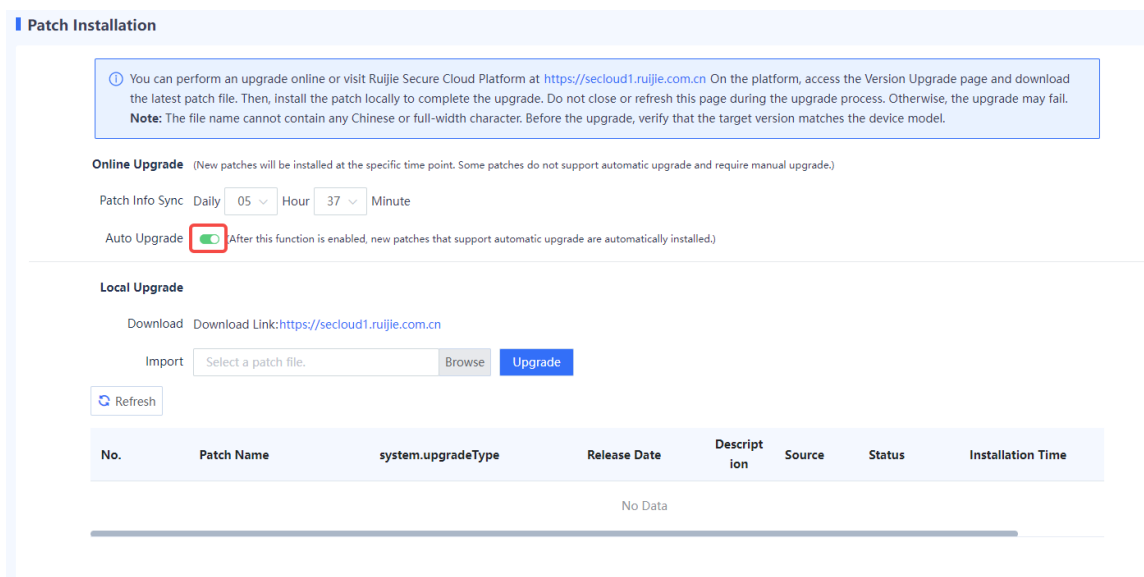
## 9. Patch Installation

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.

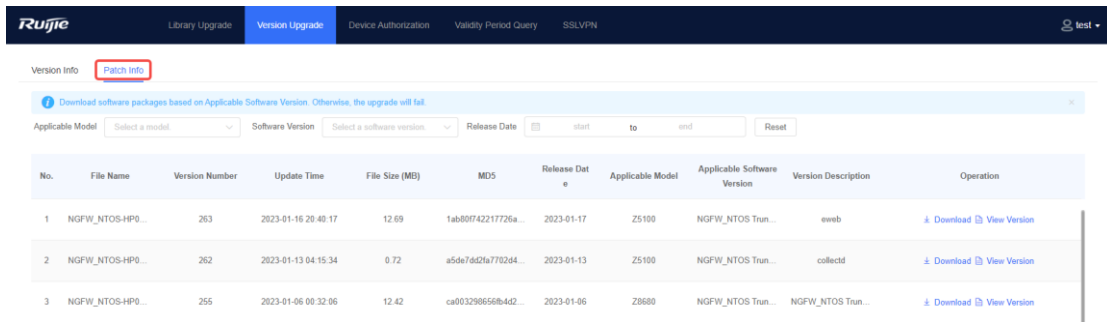
### Caution

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

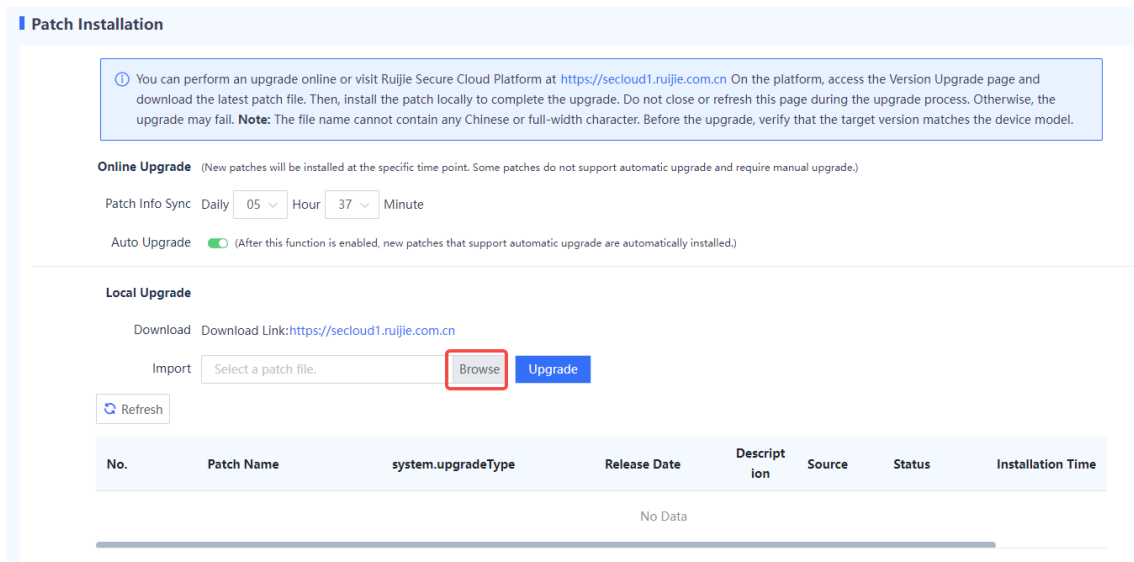


- Offline patch installation

- 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.



- 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.



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

### **i** Note

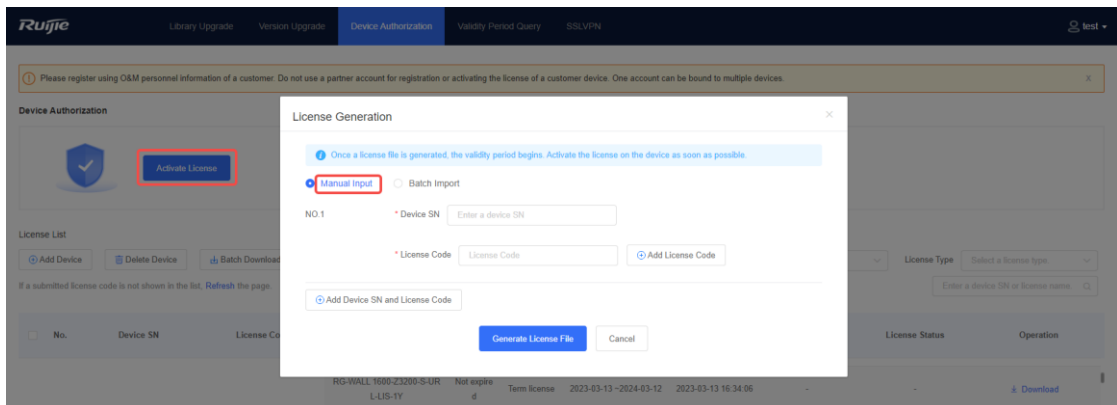
Device restart is not required after successful hot patch installation, but is required for successful cold patch installation. You need to select whether to restart the device based on actual needs.

## 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:

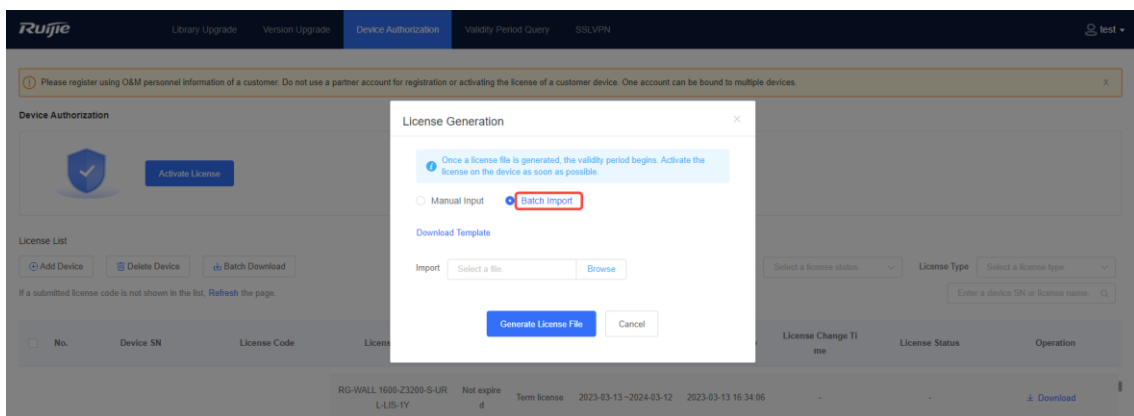
- Manually add the device SN and license code.

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



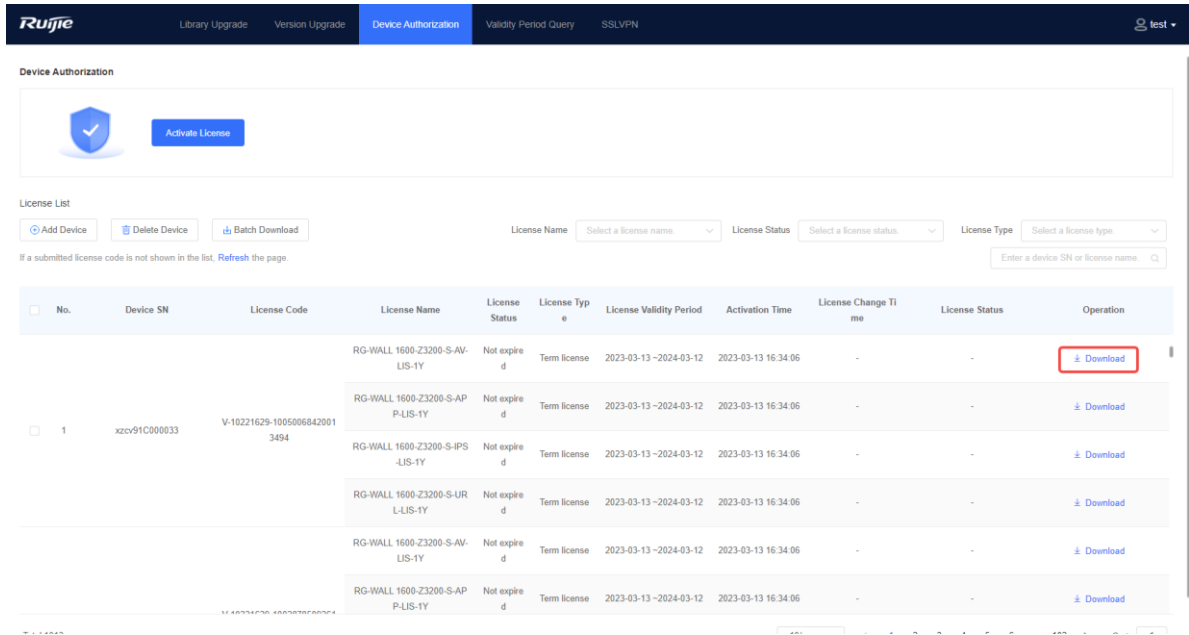
- Batch import device SNs and license codes.

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**.

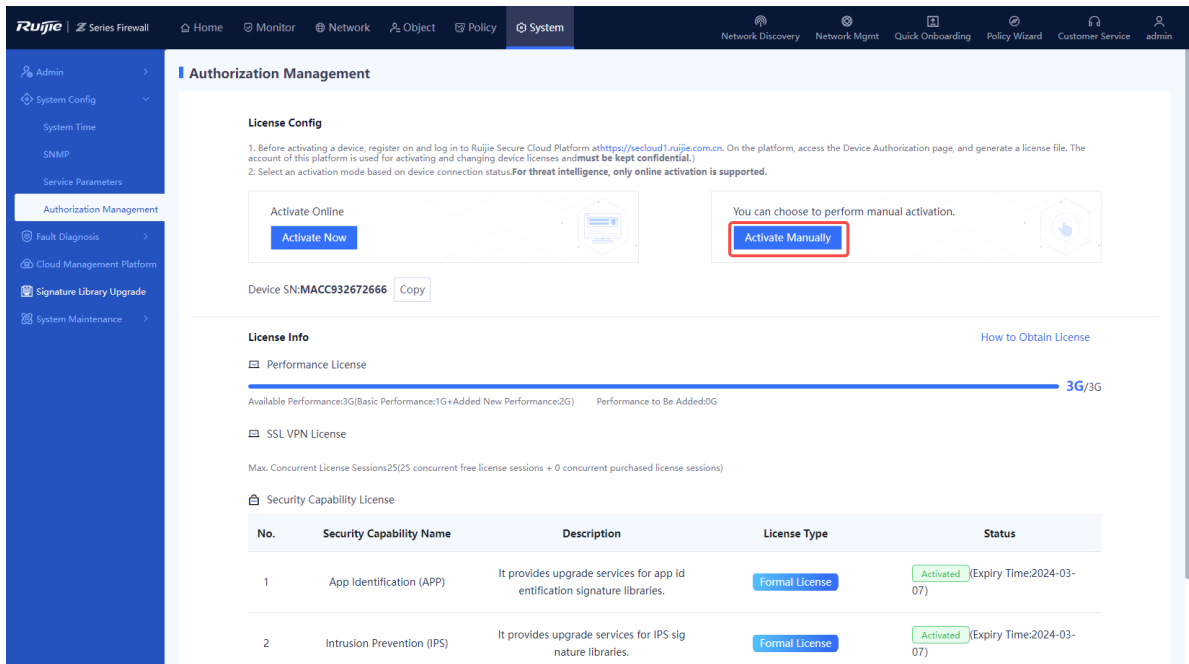


- **Offline activation**

- (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.

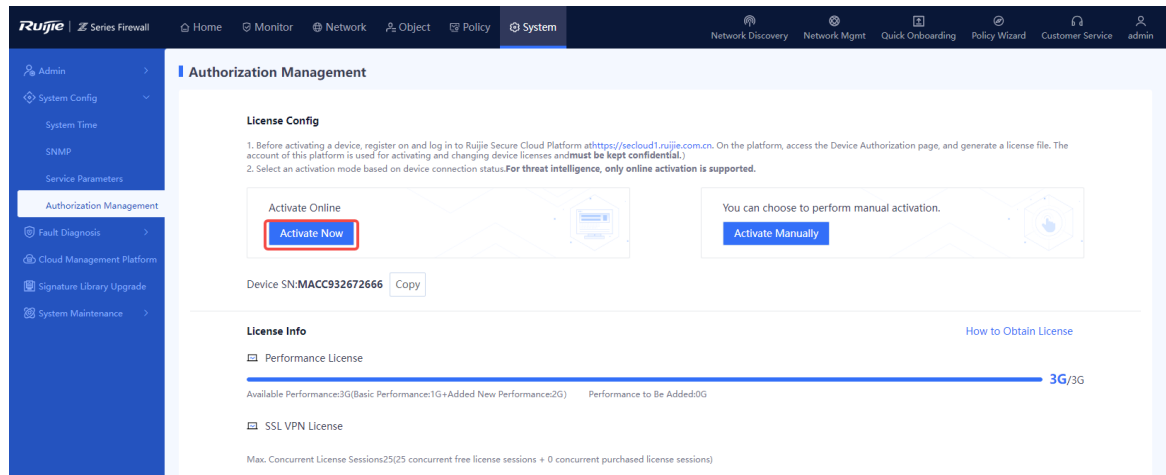


- (2) On the firewall, choose **System > System Config > Authorization Management** and click **Activate Manually** to upload the license file for offline license activation. For details, see [3.2.3 2. Manual Activation](#).



- 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](#).



### 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.

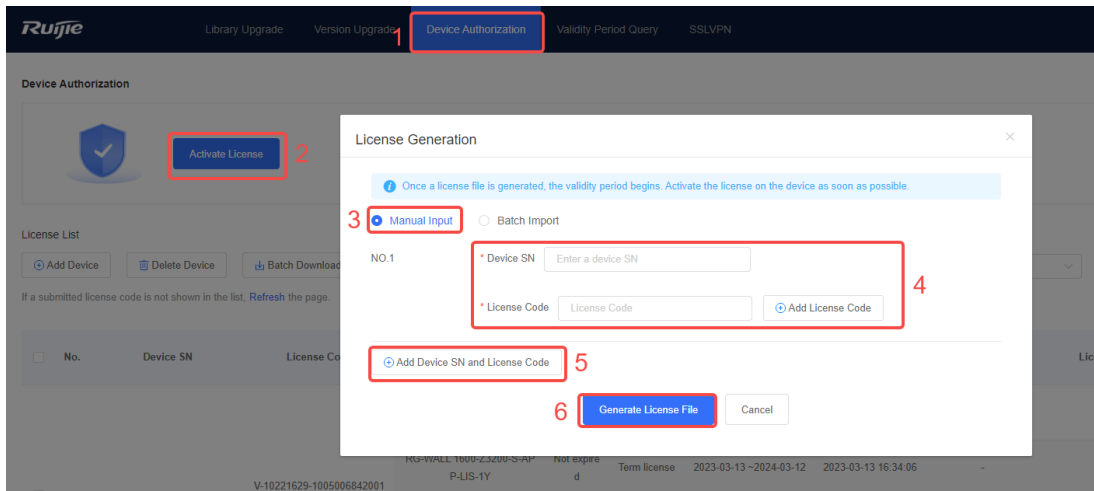
#### 1. Automatic Activation

##### Application Scenario

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

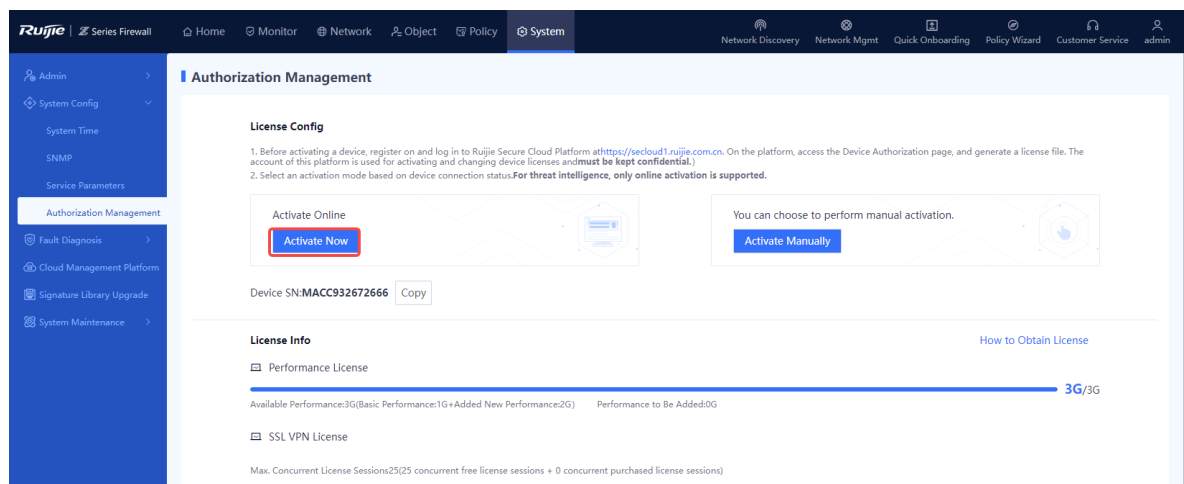
##### Prerequisites

- 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.



### Procedure

- (1) Choose **System > System Config > Authorization Management**.
- (2) Click **Activate Now**.



### 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

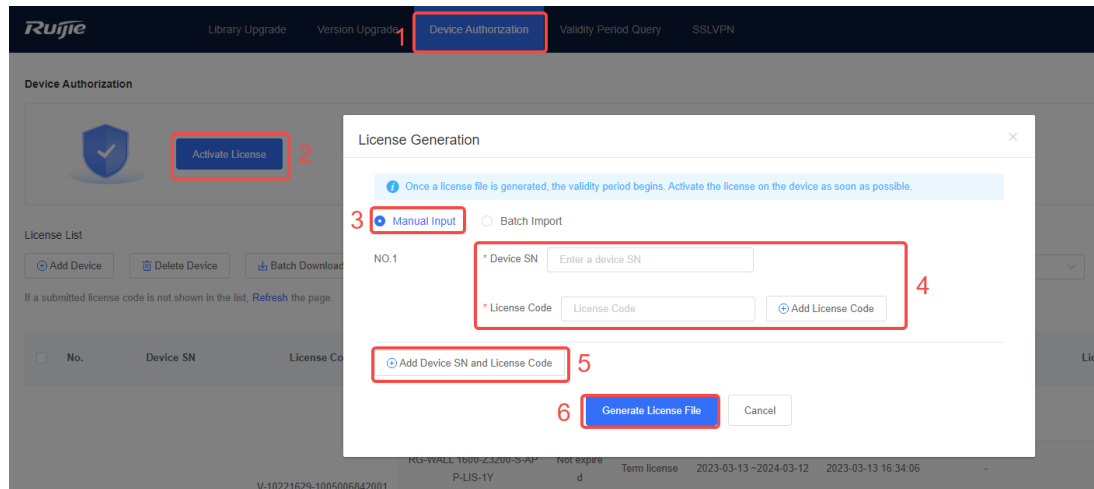
### Application Scenario

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.



**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]

**2. Export License File**

Visit Ruijie Secure Cloud Platform at <https://secloud1.ruijie.com.cn> On 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

- (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.

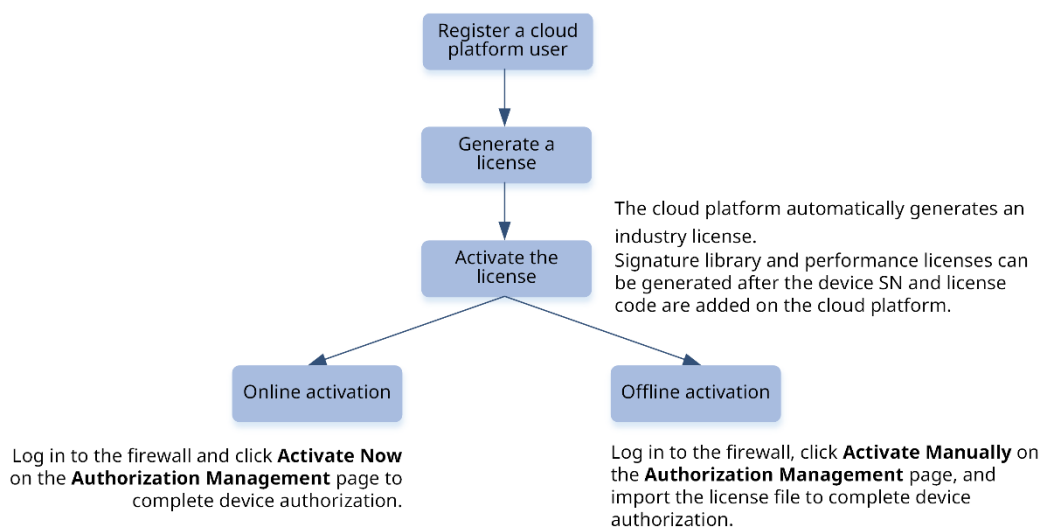
#### Follow-up Procedure

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.)



- 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.

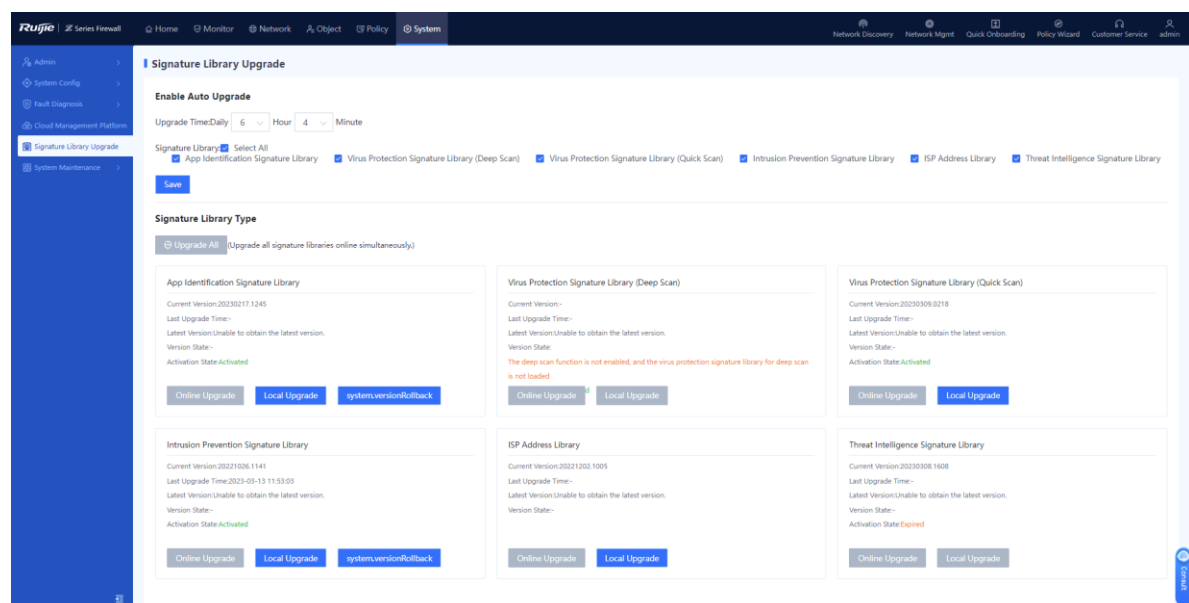
## 4.1 Configuring Automatic Upgrade

### 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**.



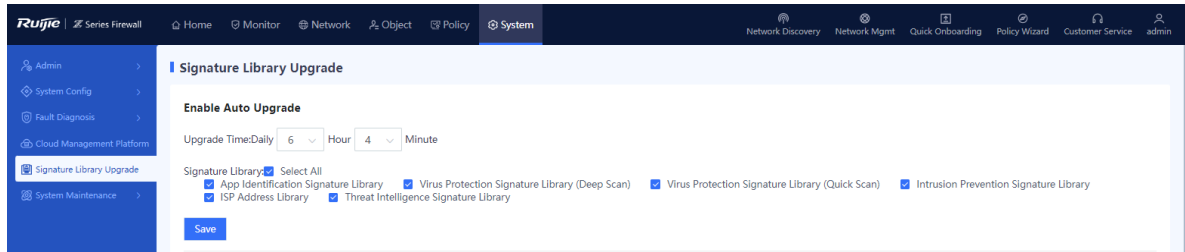
The system displays information about the current signature libraries:

- **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.



- 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**.

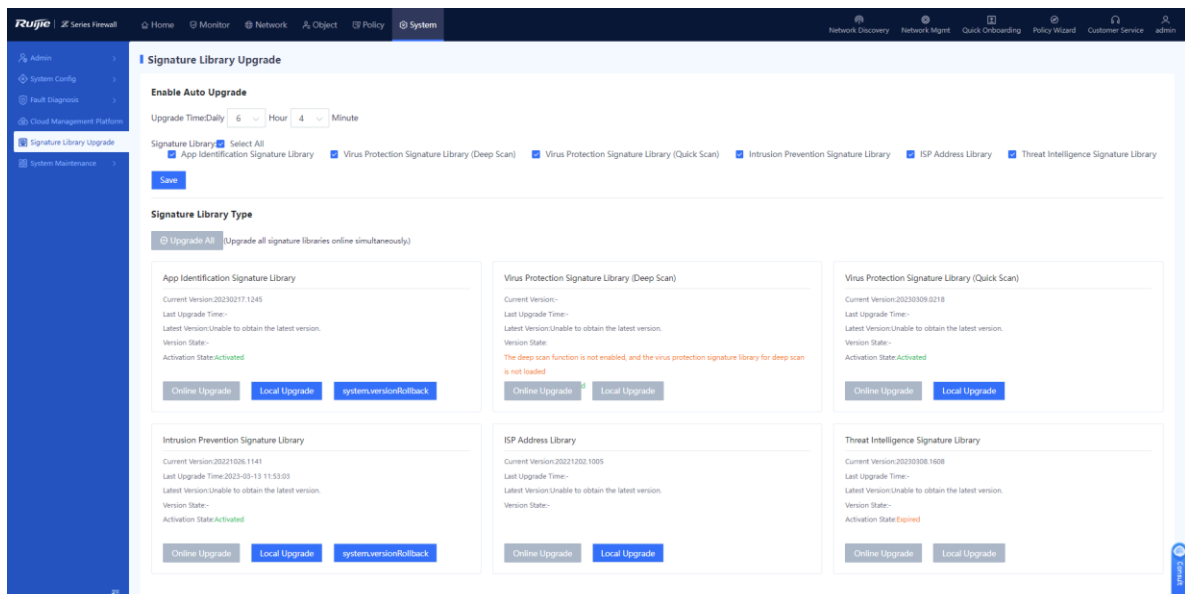
## 4.2 Local Manual Upgrade

### 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**.



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 signature libraries online simultaneously)

<p><b>App Identification Signature Library</b></p> <p>Current Version:20230217.1245                  Last Upgrade Time:-                  Latest Version:Unable to obtain the latest version.                  Version State:-                  Activation State:Activated</p> <p><input type="button" value="Online Upgrade"/> <input type="button" value="Local Upgrade"/> <input type="button" value="system.versionRollback"/></p>	<p><b>Virus Protection Signature Library (Deep Scan)</b></p> <p>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</p> <p><input type="button" value="Online Upgrade"/> <input type="button" value="Local Upgrade"/></p>
<p><b>Intrusion Prevention Signature Library</b></p> <p>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</p> <p><input type="button" value="Online Upgrade"/> <input type="button" value="Local Upgrade"/> <input type="button" value="system.versionRollback"/></p>	<p><b>ISP Address Library</b></p> <p>Current Version:20221202.1005                  Last Upgrade Time:-                  Latest Version:Unable to obtain the latest version.                  Version State:-</p> <p><input type="button" value="Online Upgrade"/> <input type="button" value="Local Upgrade"/></p>

- 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** ⊗

i 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

Import

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

- d Click **Upgrade Now**.

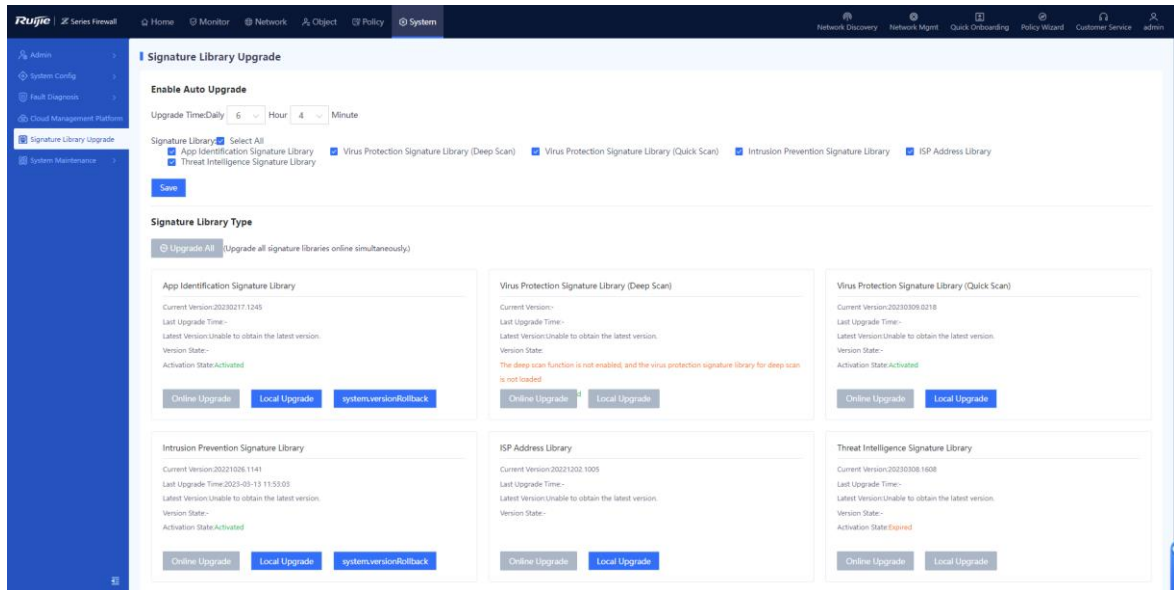
### 4.3 Online Automatic Upgrade

#### 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

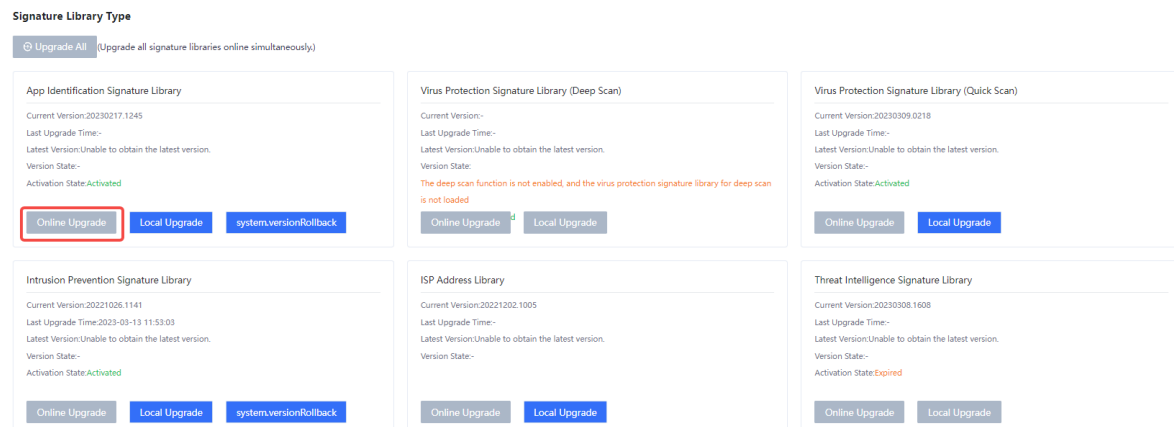
- (1) Choose **System > Signature Library Upgrade**.



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**.



---

 **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.

---

<b>File Name</b>	<b>NGFW_NTOS1.0R2P1_Z5100-S_install.bin</b>
<b>File Description</b>	System upgrade installation package, universal version
<b>File Size</b>	158,404,288 bytes
<b>Applicable Product</b>	RG-WALL-1600-Z5100-S
<b>MD5 Value</b>	415f9d28e04604418e1120ee68964618



<b>Software Version</b>	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.

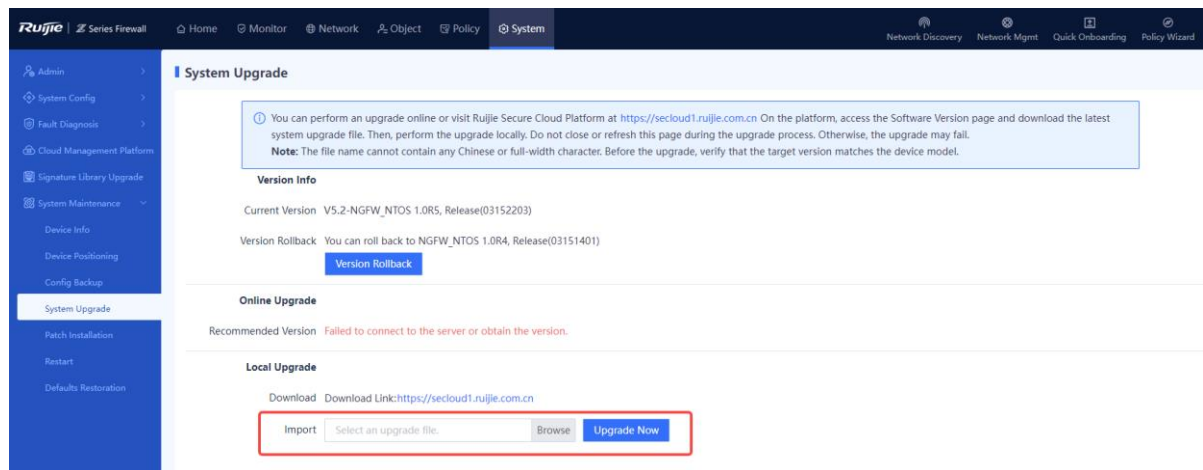
#### Prerequisites

An upgrade file is obtained in advance.

#### Procedure

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

The **System Upgrade** page is displayed.



- (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.

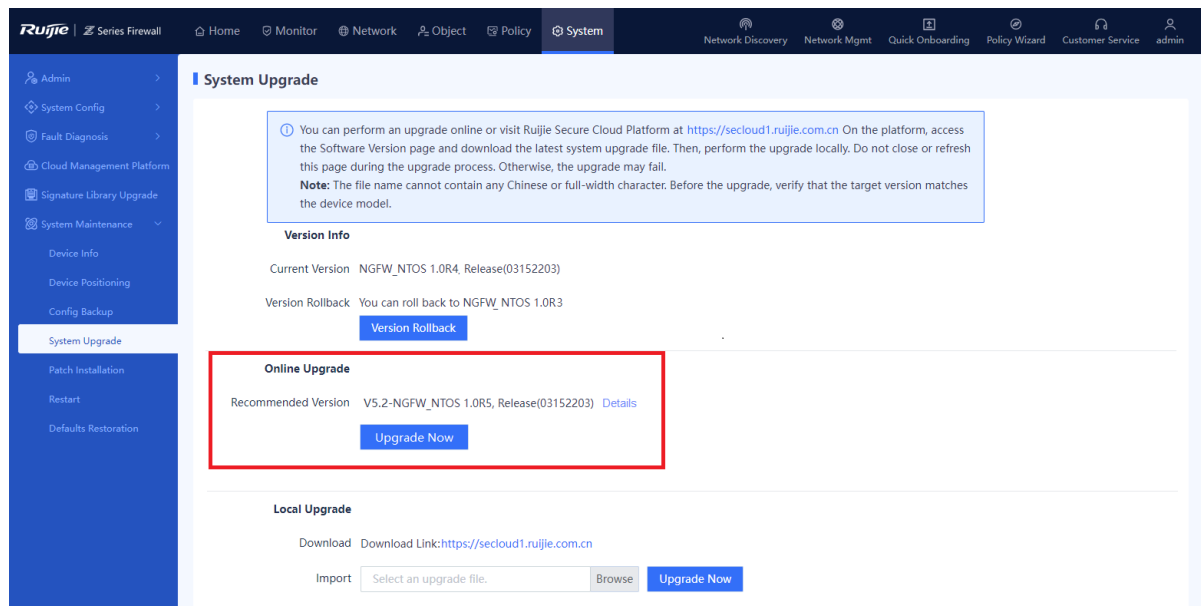
## 5.2.2 Online Upgrade

### 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**.



(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**

① 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)  
**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  **Browse** **Upgrade Now**

- (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**

① 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 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)  
**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  **Browse** **Upgrade Now**

**Version Rollback** dialog box: Do you want to perform version rollback now?  
**OK** **Cancel**

# 6 Configuration Examples for Typical Scenarios

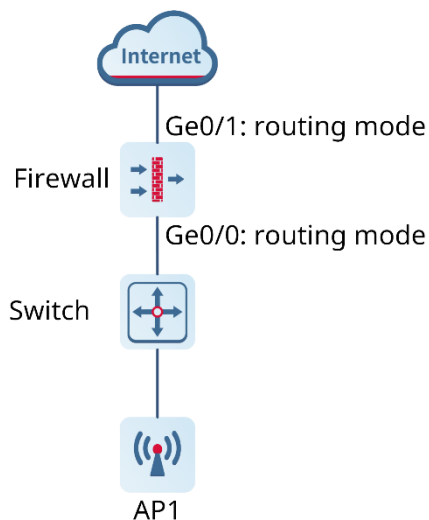
## 6.1 Integrated Deployment on Ruijie Cloud

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)

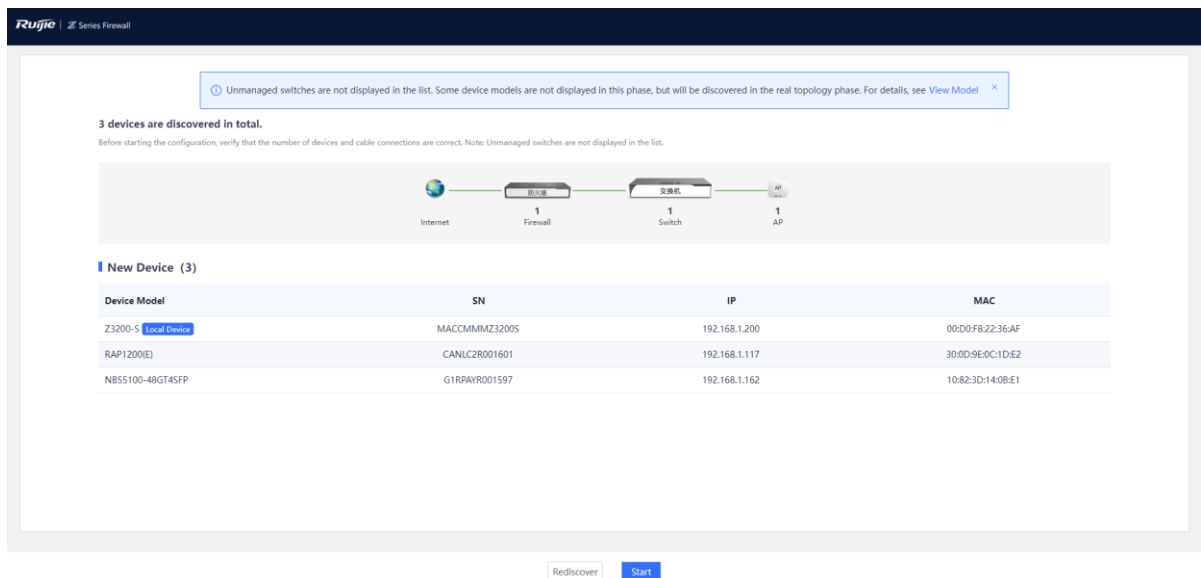
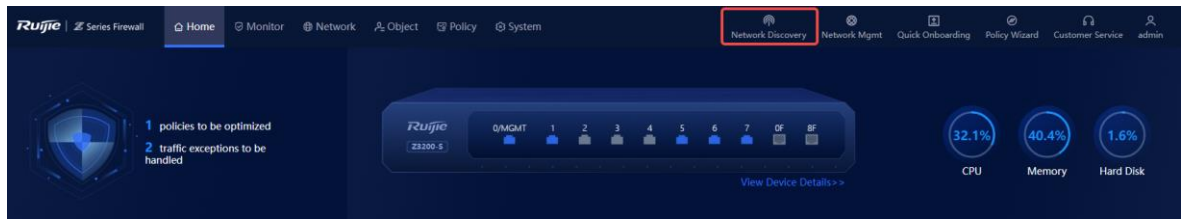
#### 1. Application Scenario

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

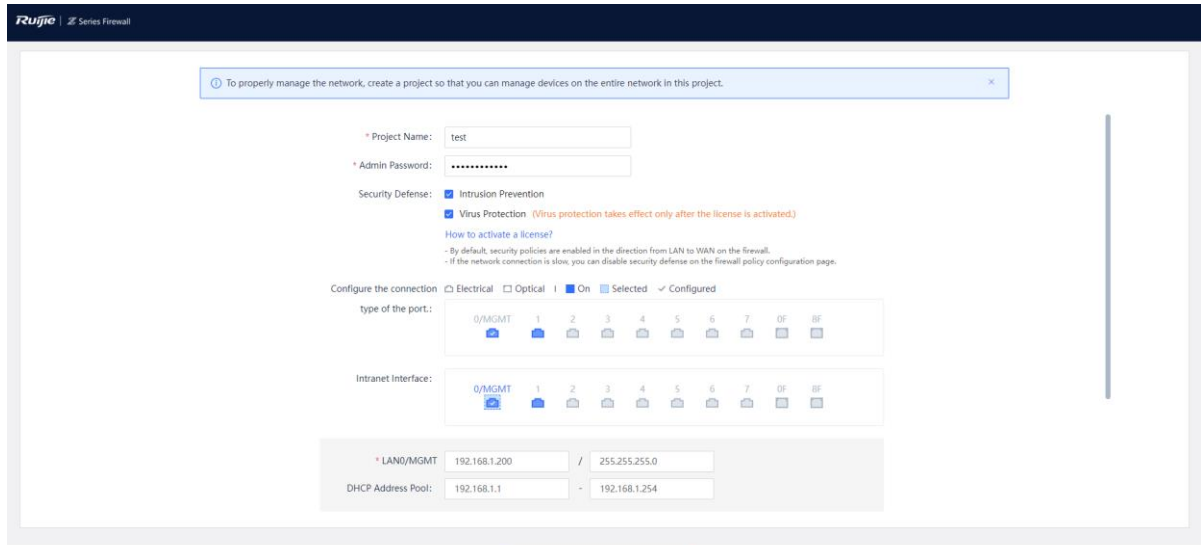
- (1) Click **Network Discovery**. The current networking information is displayed.



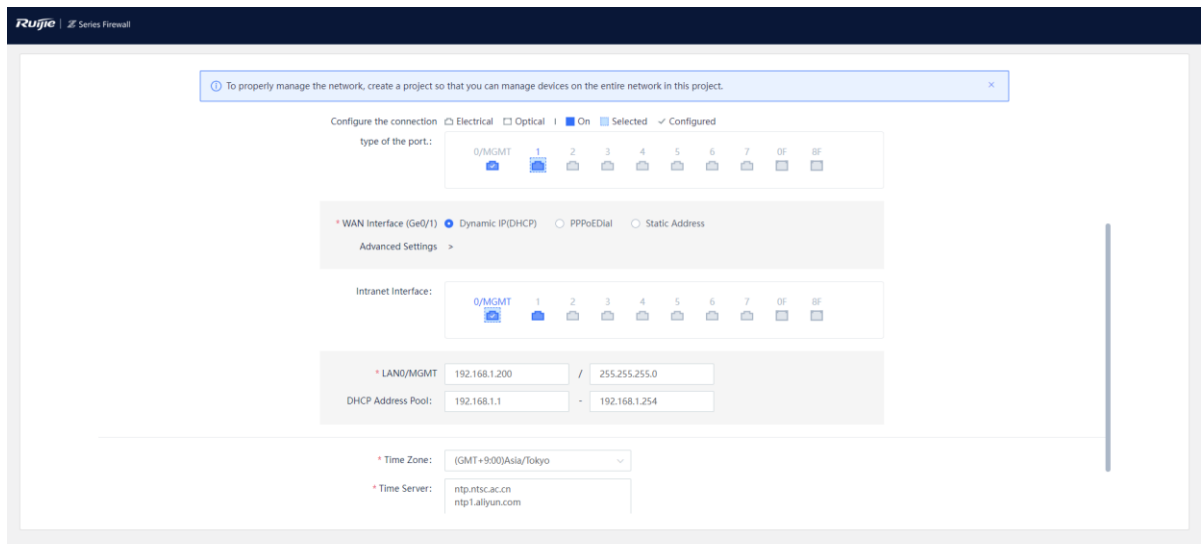
(2) Click **Start**. Enter the network project name and configure a port IP address as prompted.

### **i** 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.



Create Project and Connect to Network

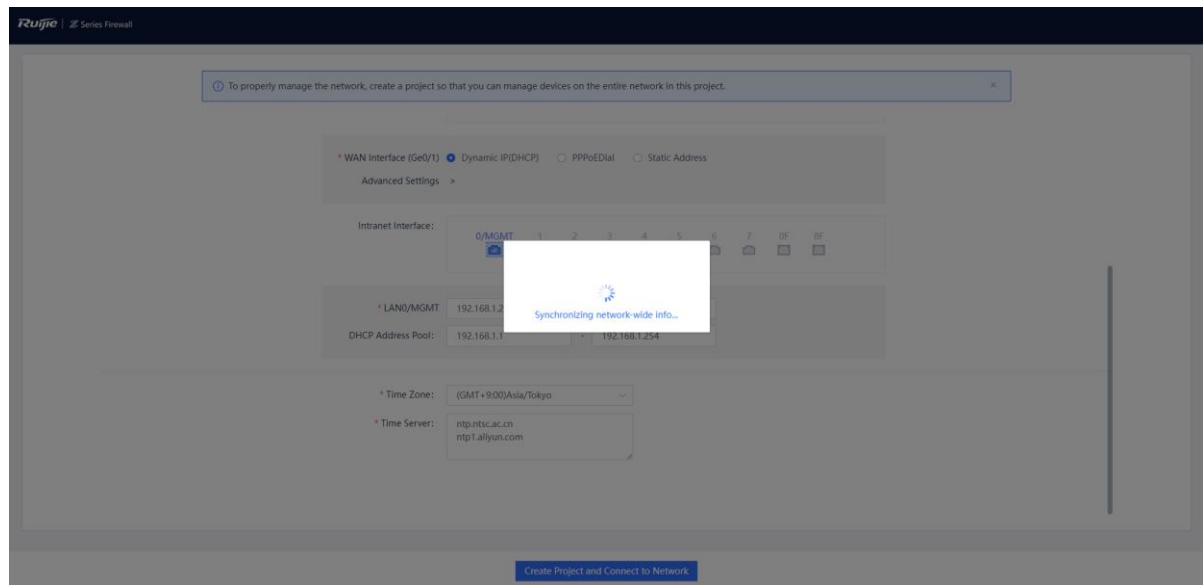


Create Project and Connect to Network

Item	Description	Remarks
WAN Interface	<p>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.</p> <p>Three methods are available for a WAN interface to obtain an IP address:</p> <ul style="list-style-type: none"> <li>● <b>Dynamic IP (DHCP):</b> 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.</li> </ul>	<p>[Example] Ge0/1 Dynamic IP (DHCP)</p>

Item	Description	Remarks
	<ul style="list-style-type: none"> <li>● <b>PPPoE:</b> Applicable for dialup access to the ISP network. The username and password of the dialup user must be configured.</li> <li>● <b>Static Address:</b> 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.</li> </ul>	
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.

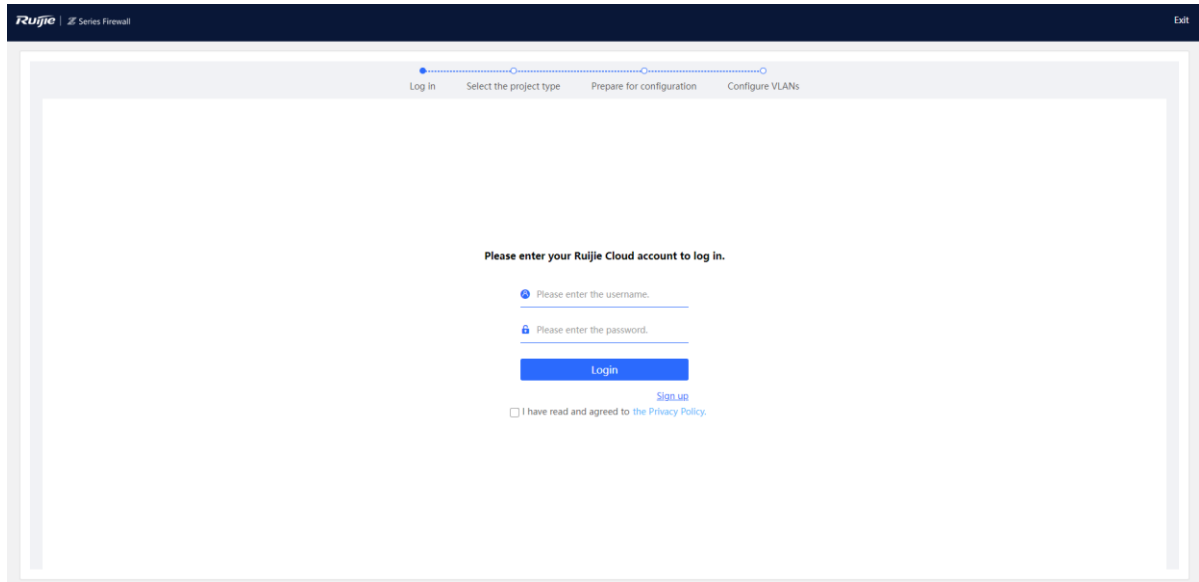


(4) Check the system prompt. A prompt indicating successful configuration is displayed after the configurations are completed. You can scan the username and password to log in to Ruijie Cloud and migrate the firewall to the cloud.



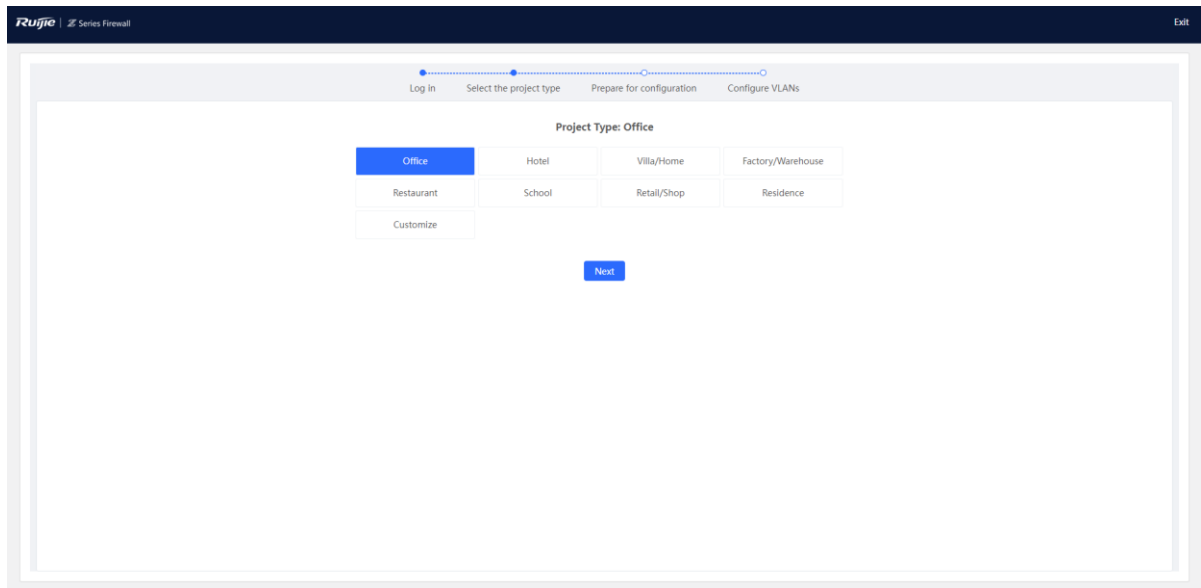
**Note**

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).

**Note**

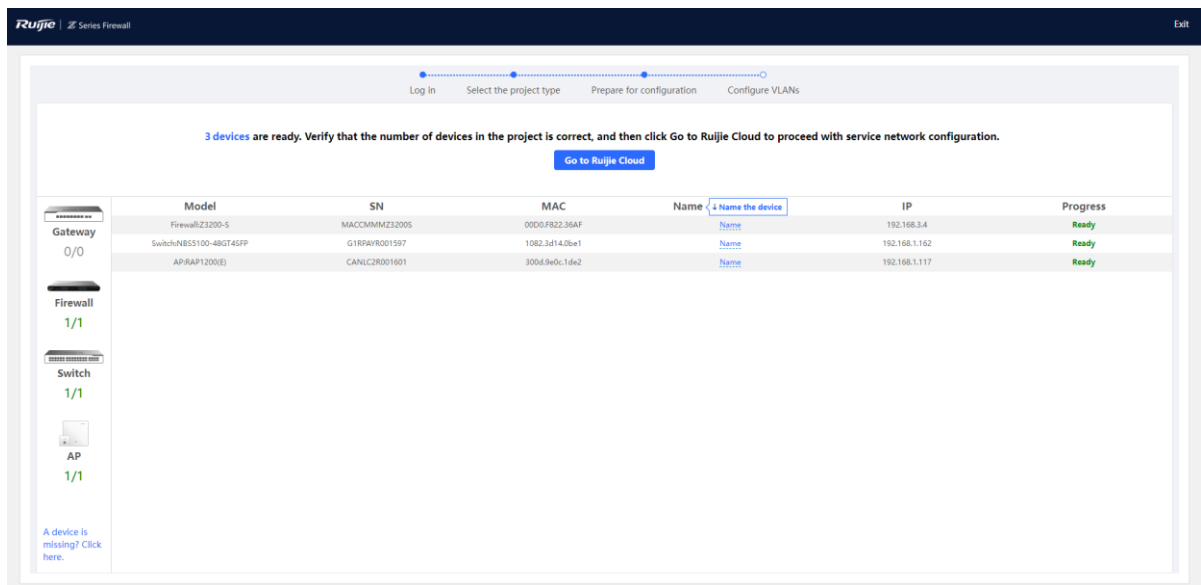
If the firewall has been bound to the Ruijie Cloud platform, the following dialog box is displayed. Click **Go to Ruijie Cloud for Network Management** to go to the Ruijie Cloud platform and manage the device. Click **Return to EWEB Homepage** to return to the home page of the firewall.

- (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.

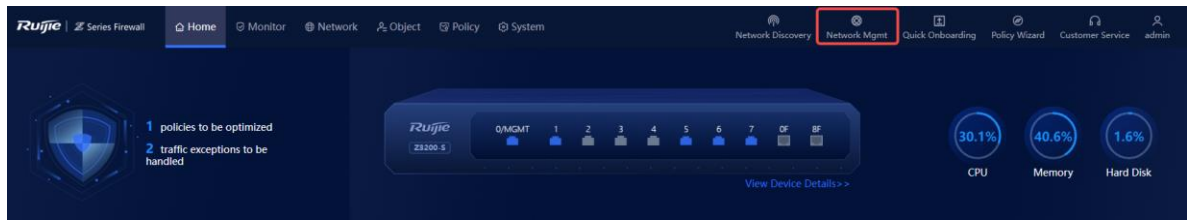


(6) Wait until preparations before configuration are complete and then configure the service network.

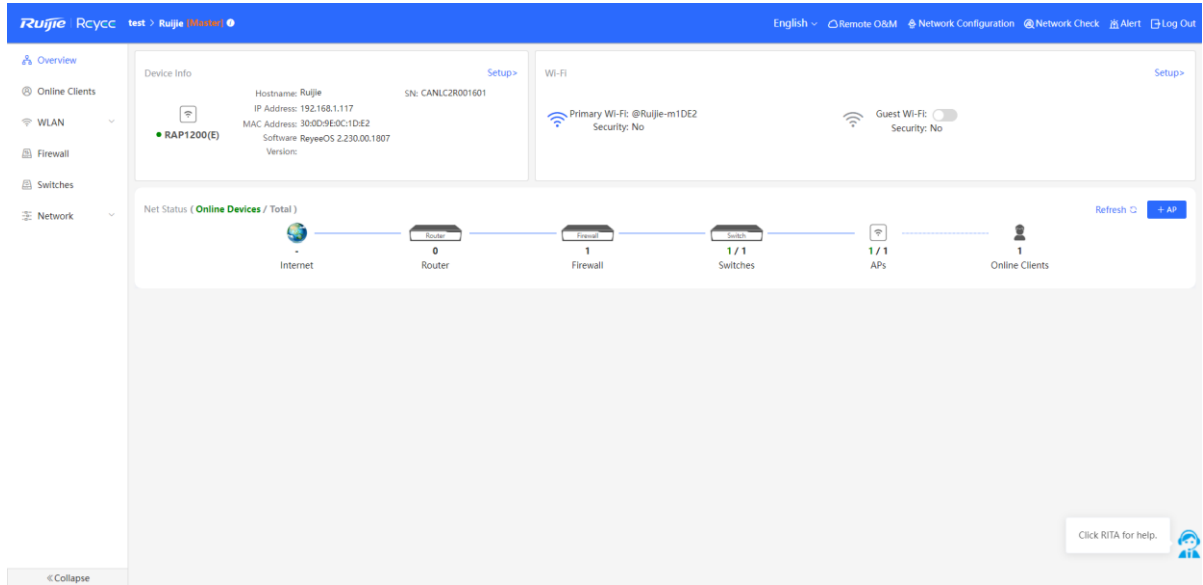
(7) After all devices go online, click **Go to the cloud platform for management** and perform service configuration on the Ruijie Cloud platform.



(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.



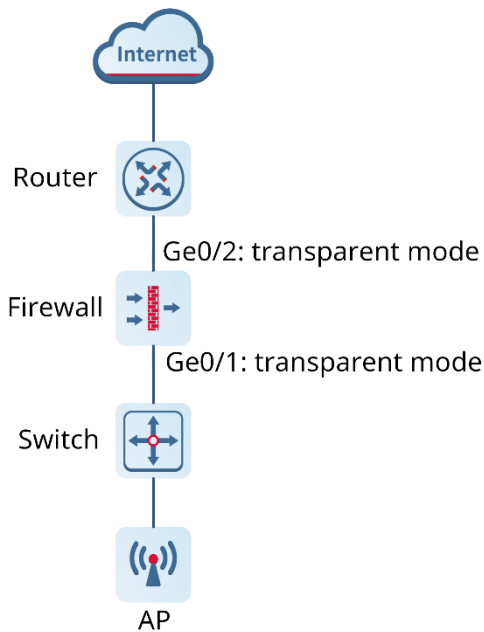
The following figure shows the **Overview** page of the master device.



## 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.



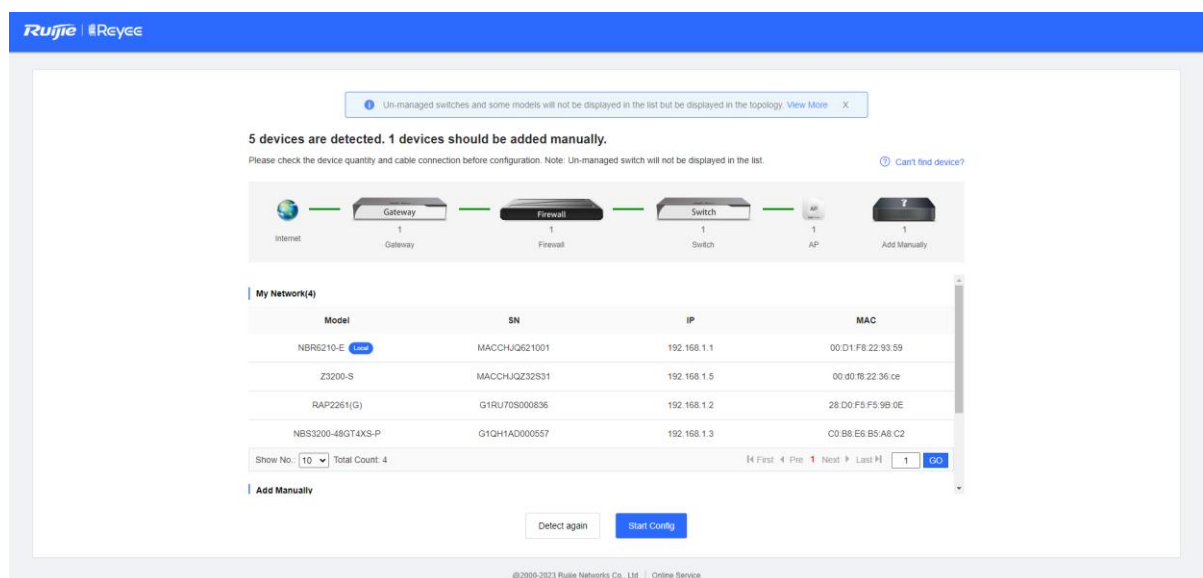
## 2. Procedure

- (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.

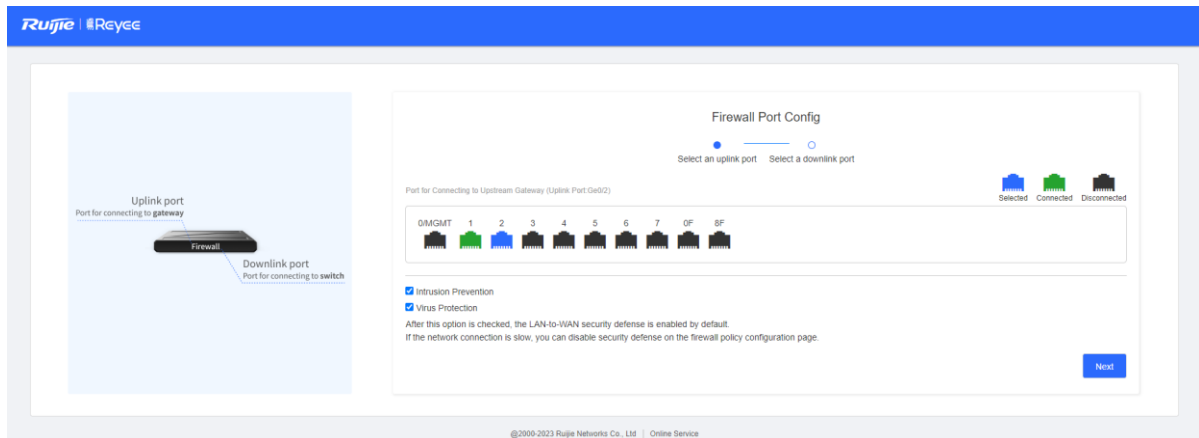
### **Note**

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**.

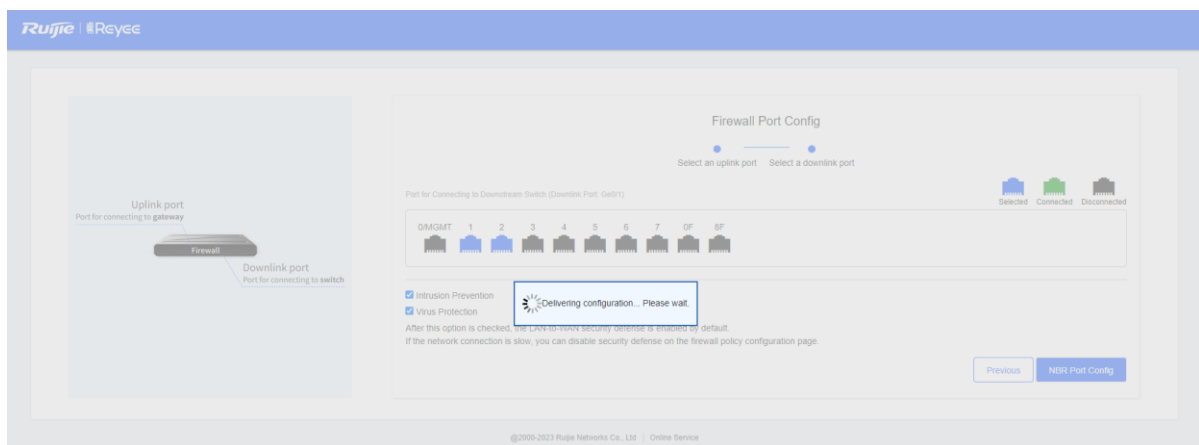
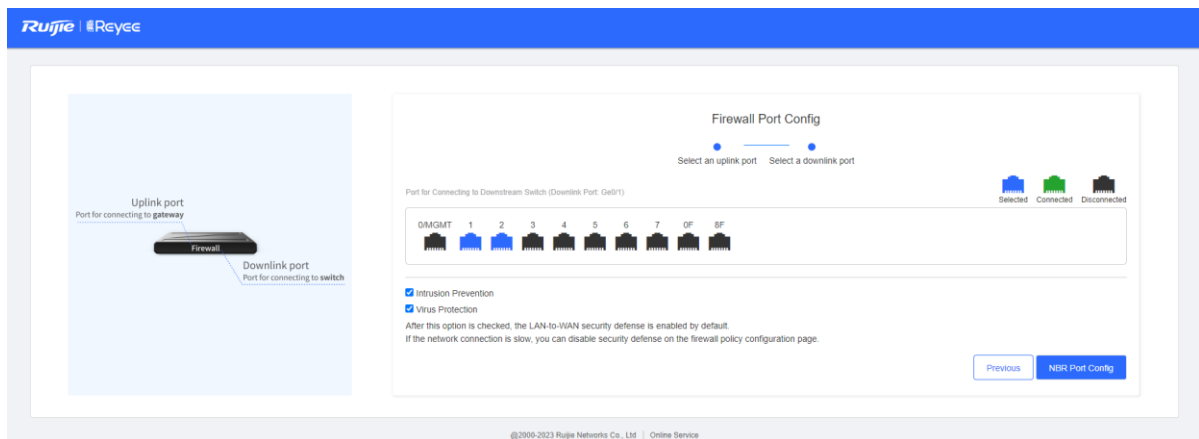
- (2) Log in to the web page of the NBR. The following page is displayed by default. Click **Start**.



- (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**.



- (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**.



- (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**.

The screenshot shows the Ruijie configuration interface. At the top, there is a blue header with the Ruijie logo and 'Reyee'. Below the header, a message box says 'Please create a project for the network so that you can manage devices on the project.' The main form contains the following fields and options:

- Project Name:** nbr\_web
- Management Password:** [Redacted]
- Port IP Assignment:**
  - WAN1 (G0/0)
  - WAN2 (G0/7)
  - SF(SFP) (G0/8)
  - SF(SFP) (G0/9)
- WAN0(G0/7):**  DHCP  PPPoE  Static IP Address
- LAN Port:**
  - LAN0(MGMT) (G0/0)
  - LAN1 (G0/1)
  - LAN2 (G0/2)
  - LAN3 (G0/3)
  - LAN4 (G0/4)
  - LAN5 (G0/5)
- LAN0(MGMT(G0/0)):** 192.168.1.1 / 255.255.255.0

A blue button labeled 'Create Project and Connect to Network' is located at the bottom of the form. The footer contains the text '@2000-2023 Ruijie Networks Co., Ltd | Online Service'.

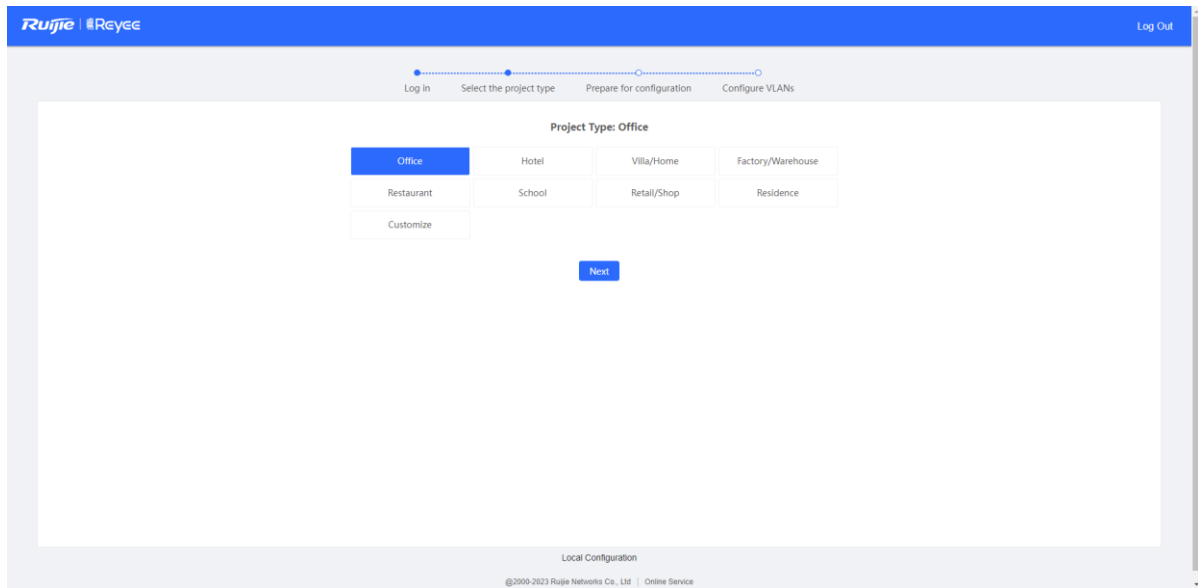
- (6) Check the system prompt. A prompt indicating successful configuration is displayed after the configurations are completed. You can scan the username and password to log in to Ruijie Cloud and migrate the firewall to the cloud.

The screenshot shows the Ruijie login page. At the top, there is a blue header with the Ruijie logo and 'Reyee'. Below the header, a progress bar shows four steps: 'Log In', 'Select the project type', 'Prepare for configuration', and 'Configure VLANs'. The main content area contains the following text and form elements:

- Please enter your Ruijie Cloud account to log in.**
- Please enter the username.
- Please enter the password.
- Login** button
- [Sign Up](#) link
- I have read and agreed to the [Privacy Policy](#).

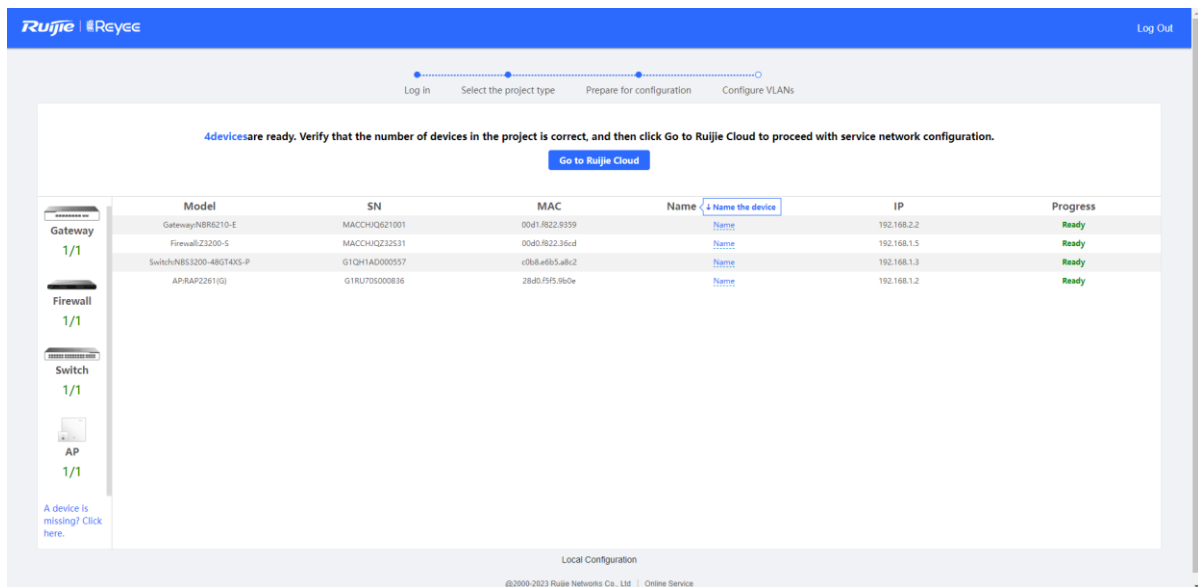
The footer contains the text 'Local Configuration' and '@2000-2023 Ruijie Networks Co., Ltd | Online Service'.

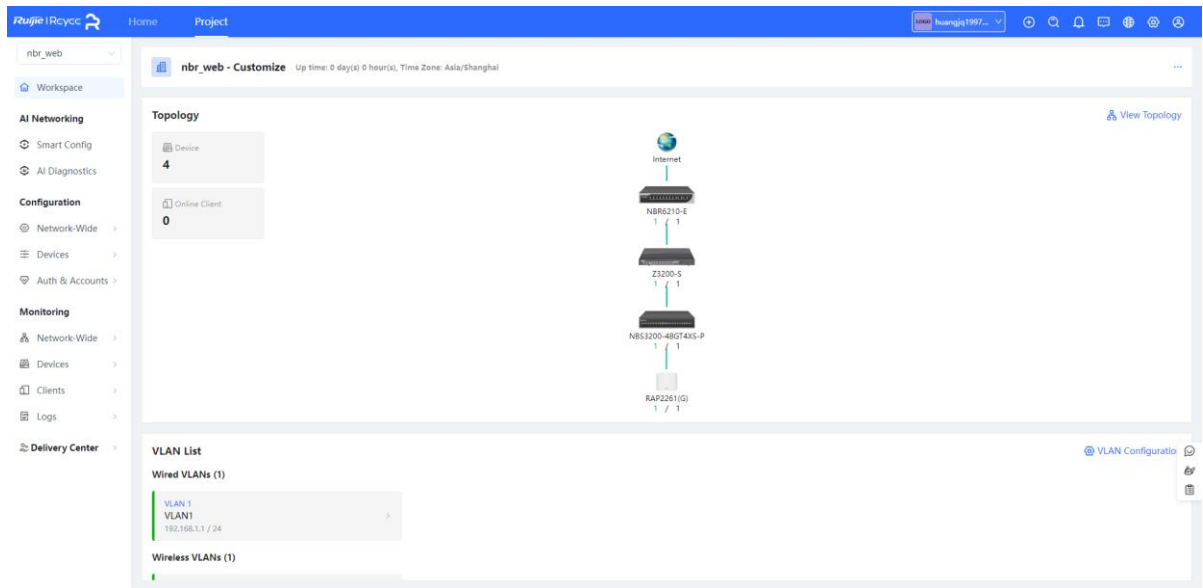
- (7) After successful login, select a project type based on the actual networking scenario (**Other** in this example) and click **Next**. The initial configuration delivered varies by the project type, so the project type must be set based on the actual service scenario.



(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.

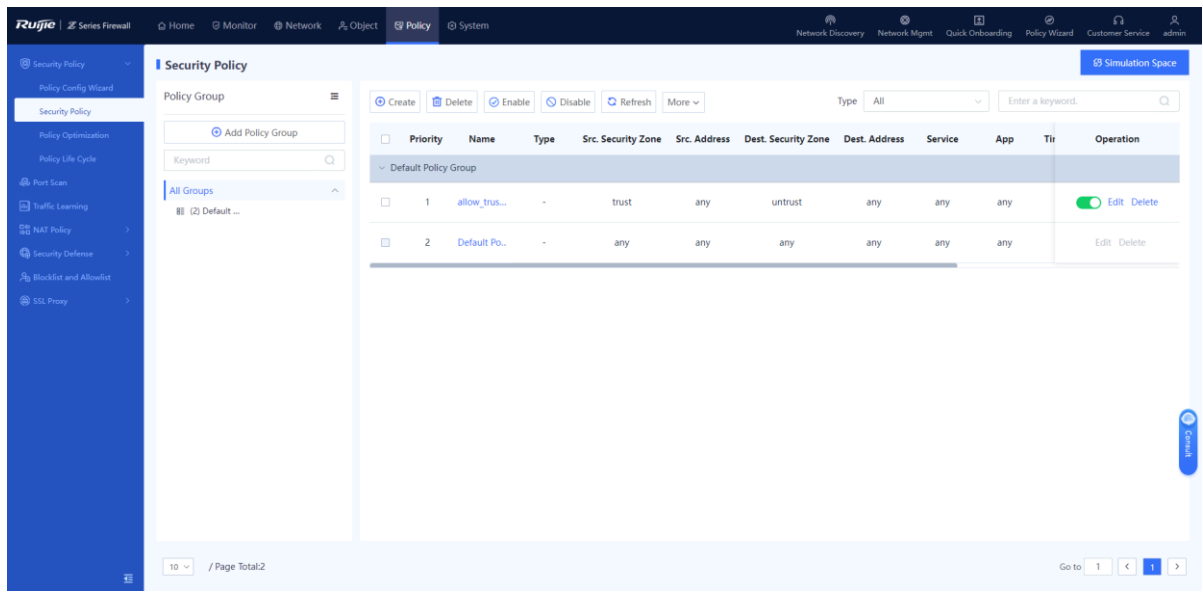




**Note**

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.





### 6.1.3 Deployment Using Ruijie Cloud App (Routing Mode)

#### 1. Application Scenario

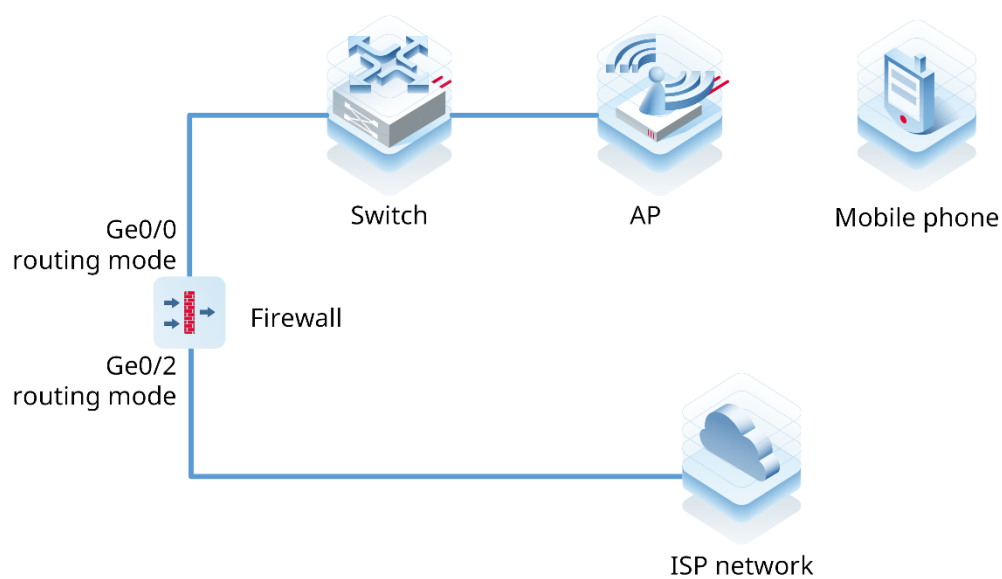
The firewall functions as a router and it is uplinked to the Internet and downlinked to a switch. You are advised to deploy the firewall in routing mode. The uplink and downlink interfaces are configured to work in routing mode.

---

#### **Note**

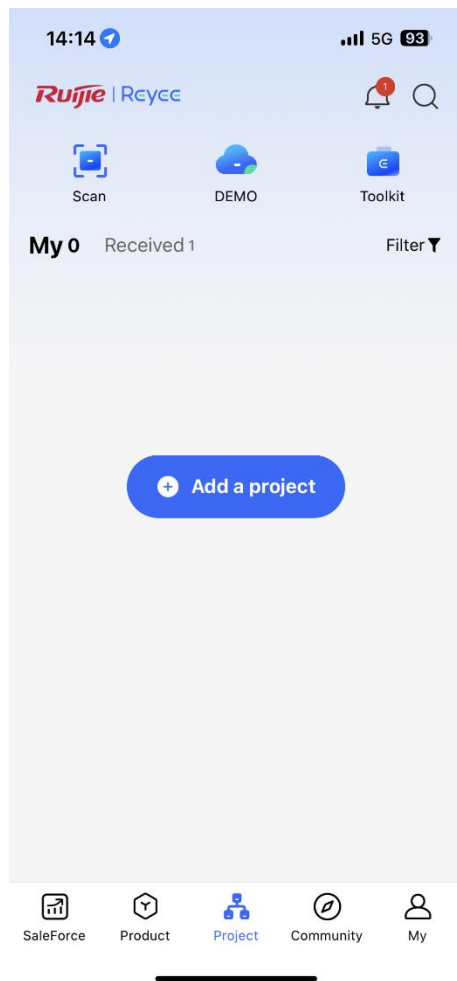
You do not need to connect the firewall to the PC in Wi-Fi deployment using the Ruijie Cloud app.

---

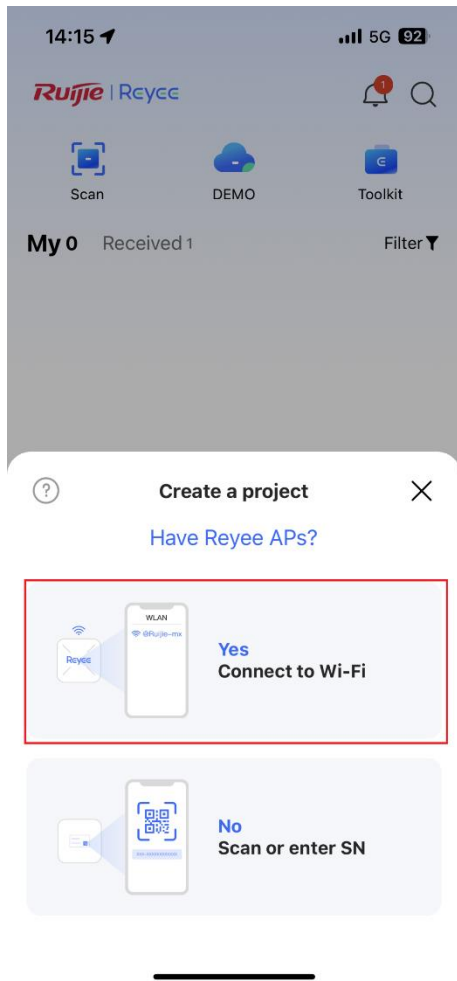


#### 2. Procedure

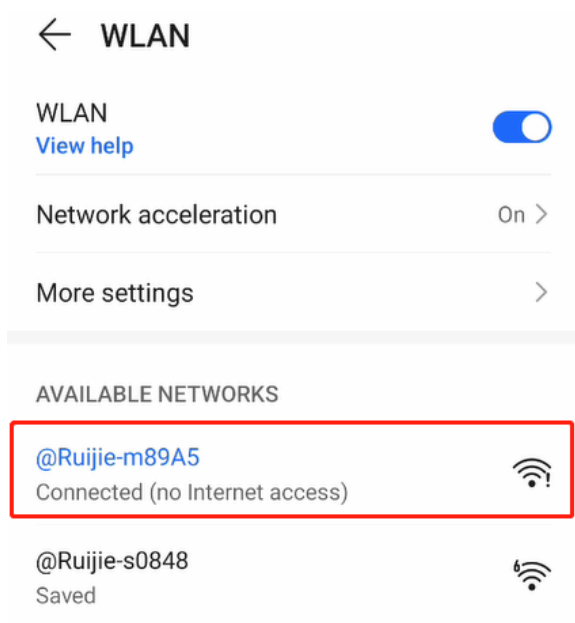
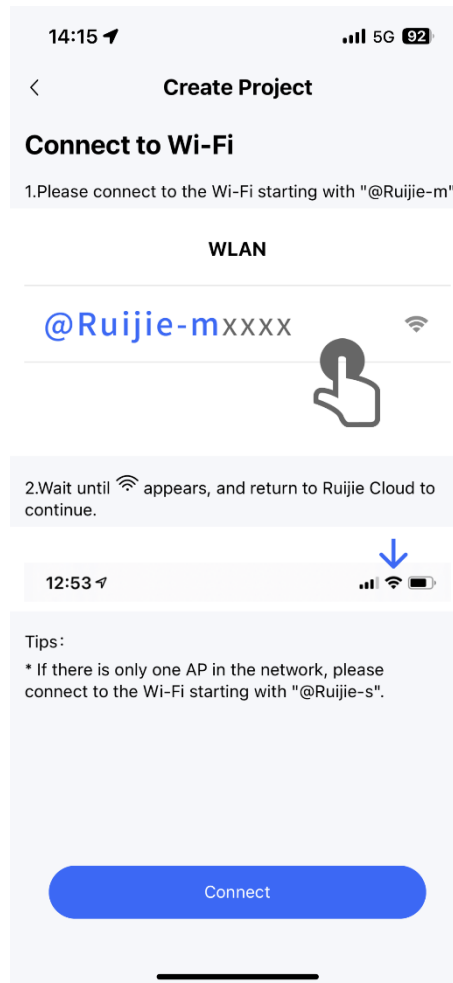
- (1) After the network environment is established according to the preceding figure, start the Ruijie Cloud app and choose **Project > Add a project**.



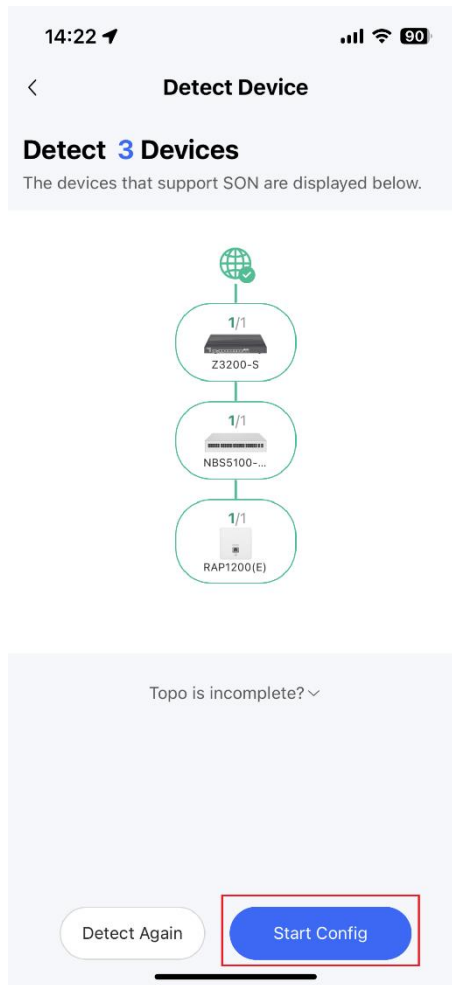
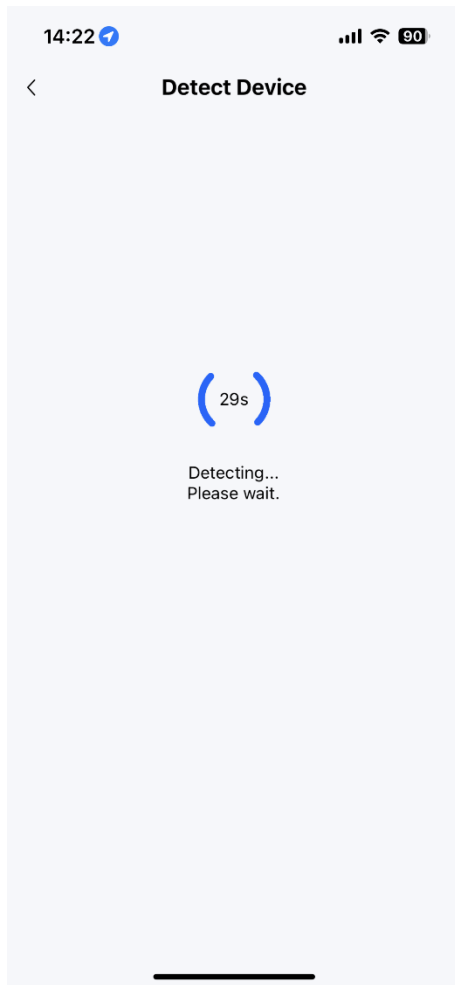
(2) Select **Connect to Wi-Fi** and add a project.



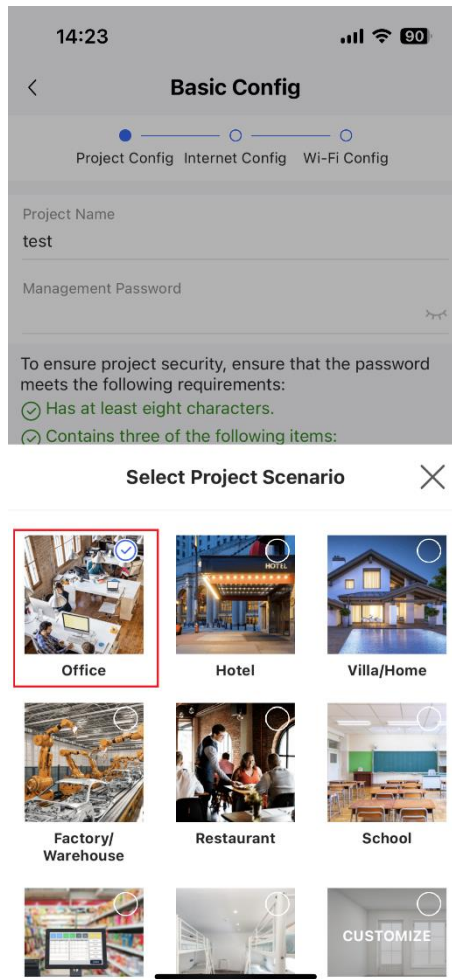
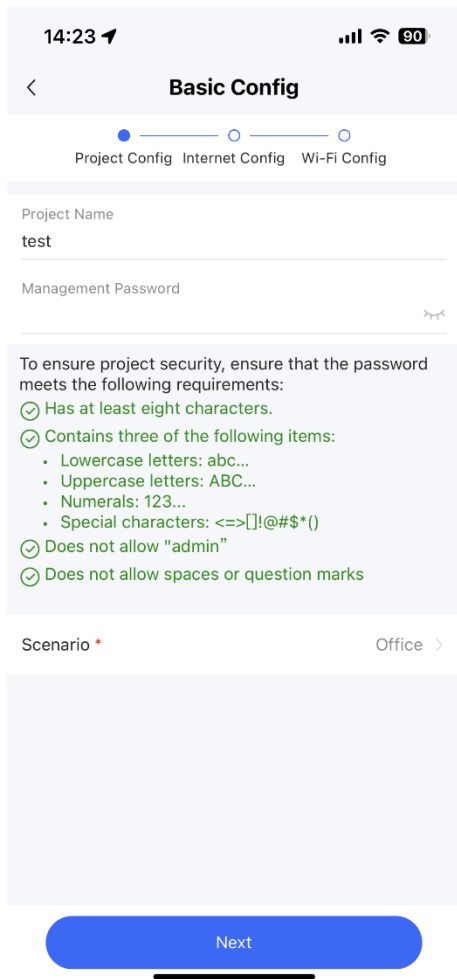
(3) Tap **Connect** to connect to the Wi-Fi signal of the Reyee AP.



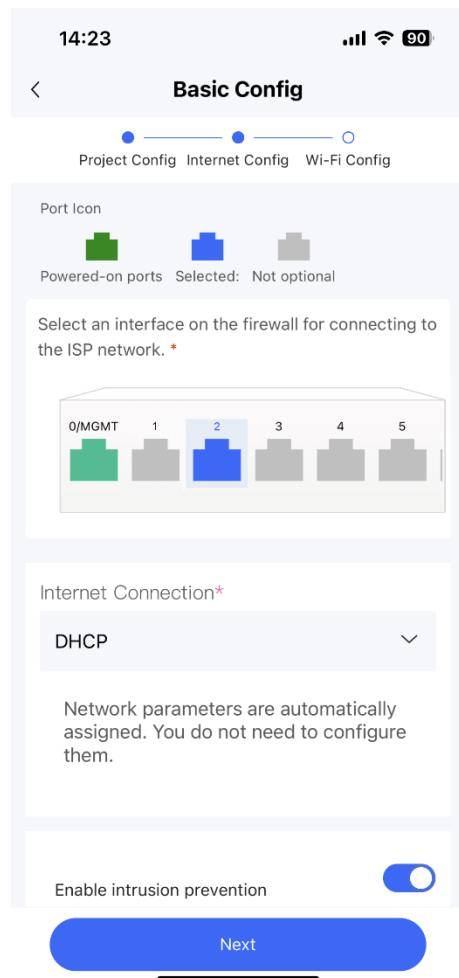
(4) Wait for about 30s until the system automatically generates the network topology. Then, tap **Start Config**.



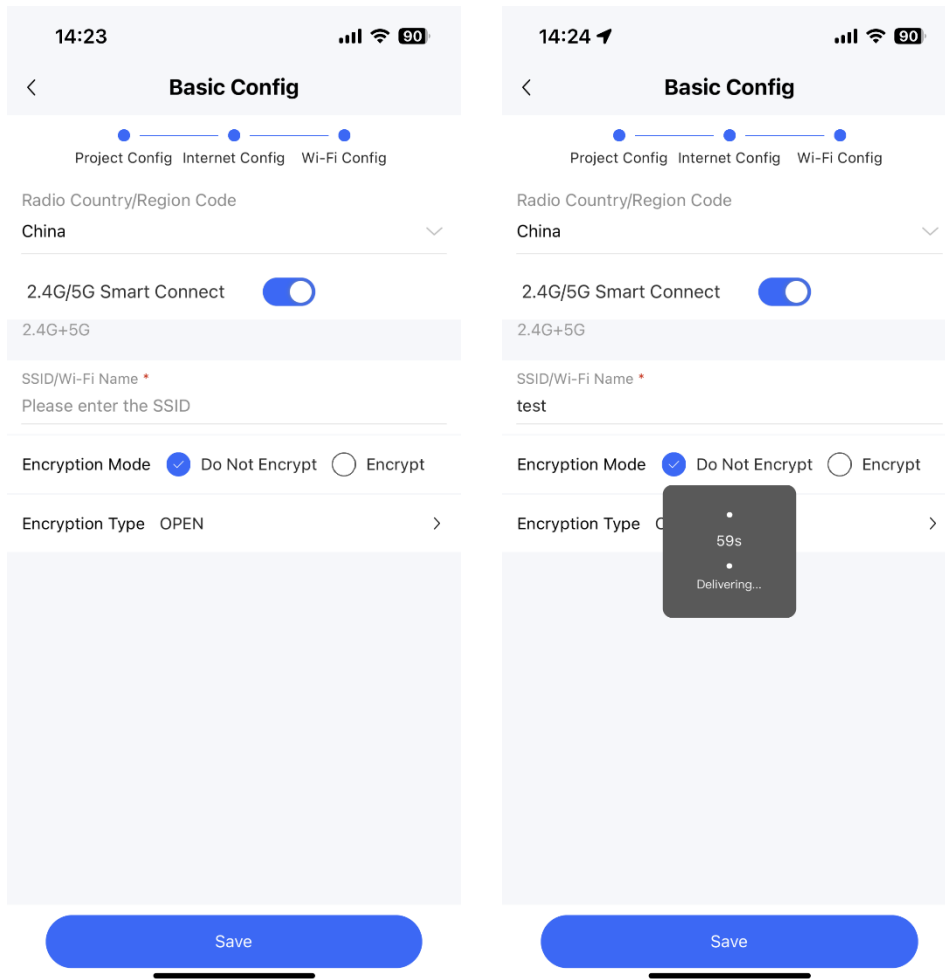
(5) Enter the project name and password and tap **Next**.



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

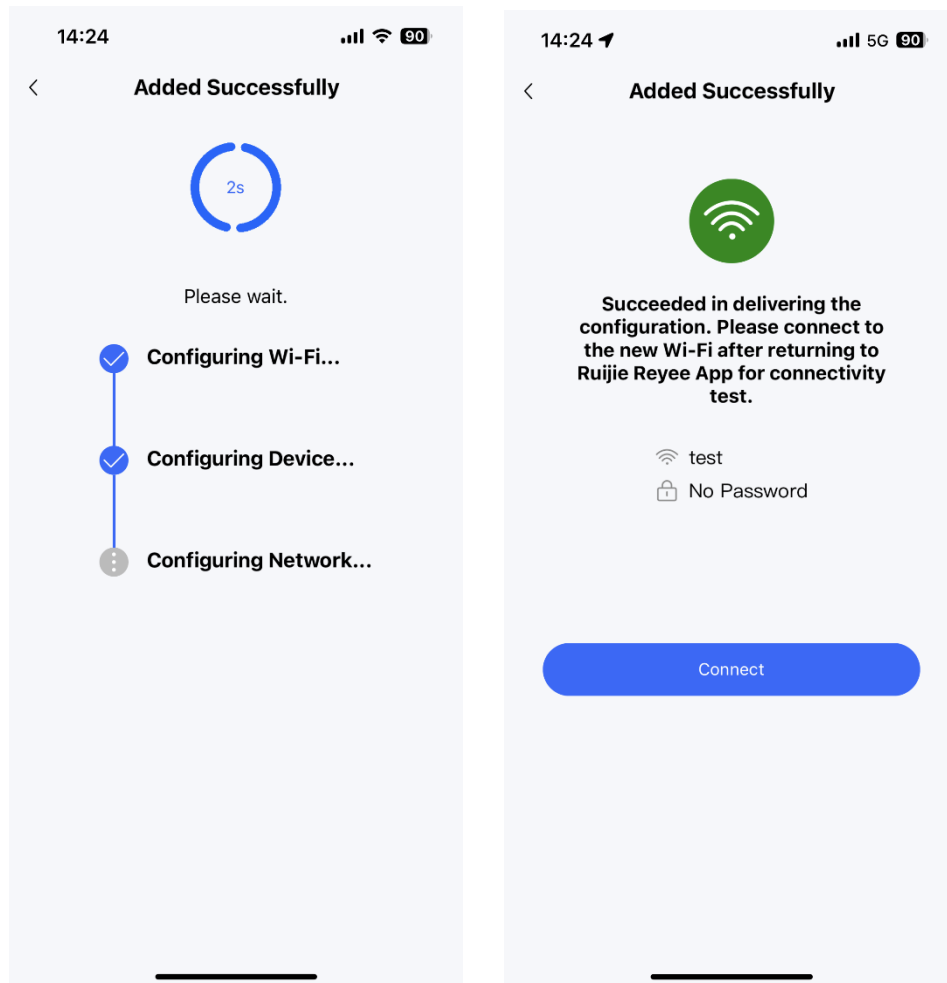


(7) Set the Wi-Fi name and password and tap **Save**.

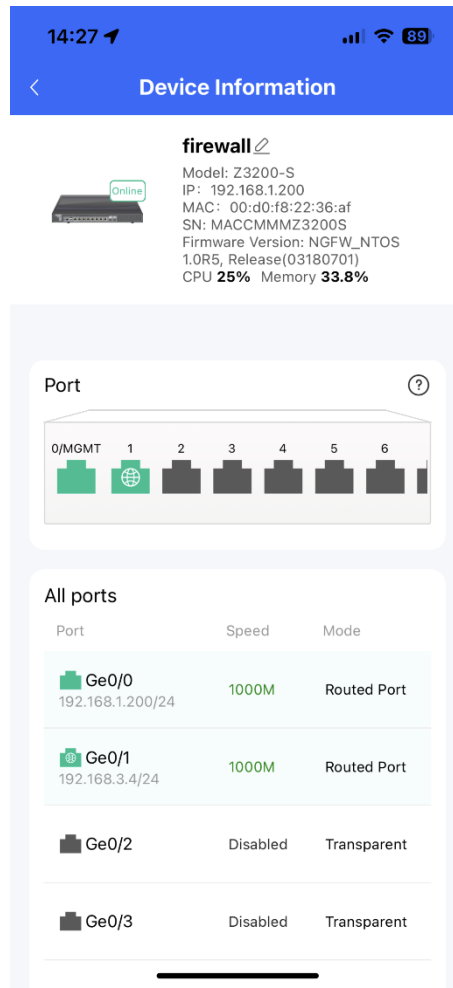
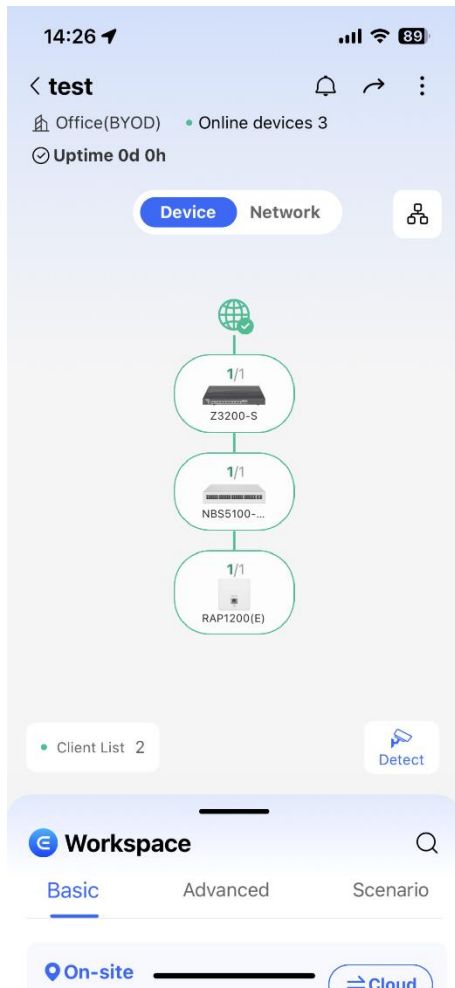


(8) After successful configuration delivery, connect to the new Wi-Fi.





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



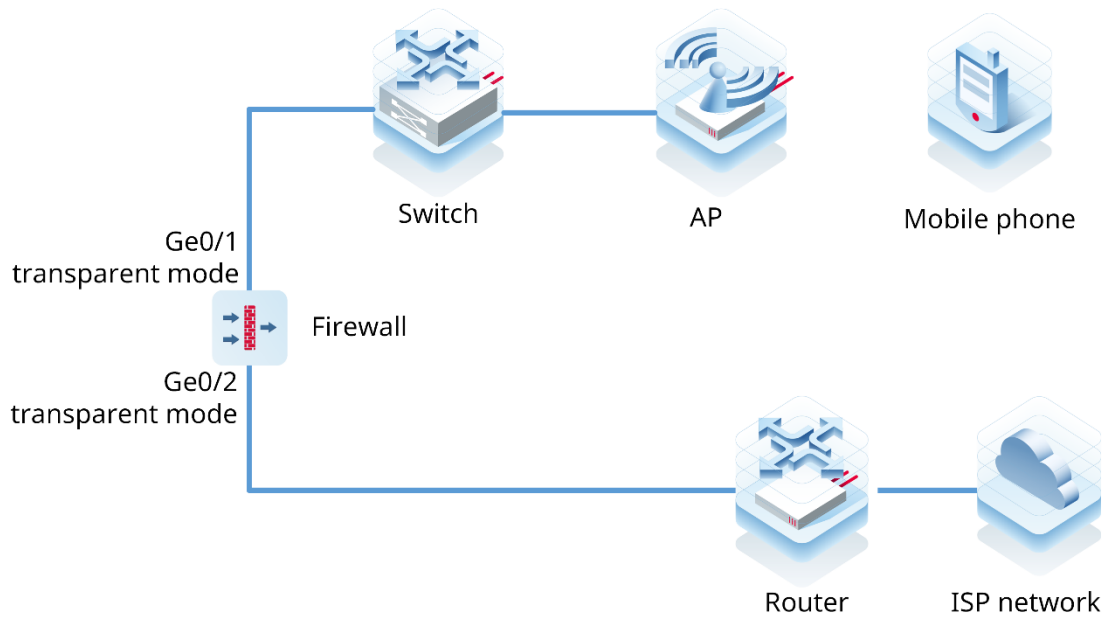
## 6.1.4 Deployment Using Ruijie Cloud App (Transparent Mode)

### 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.

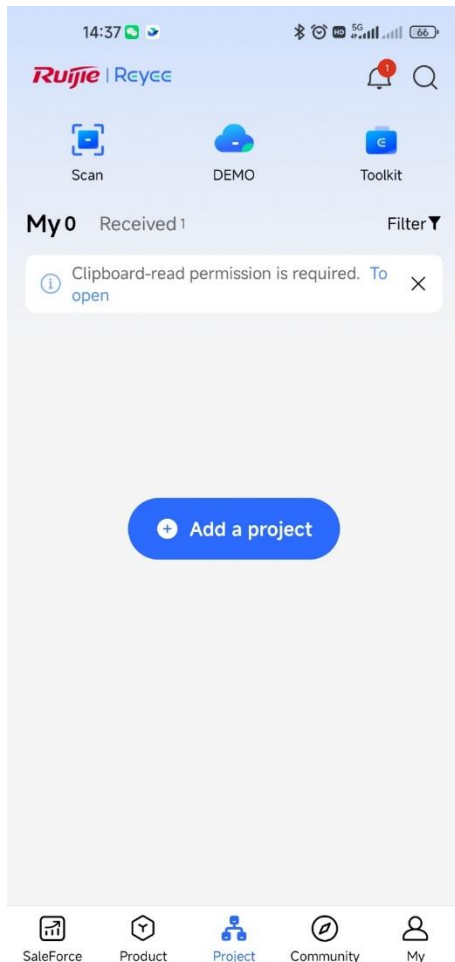
**Note**

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

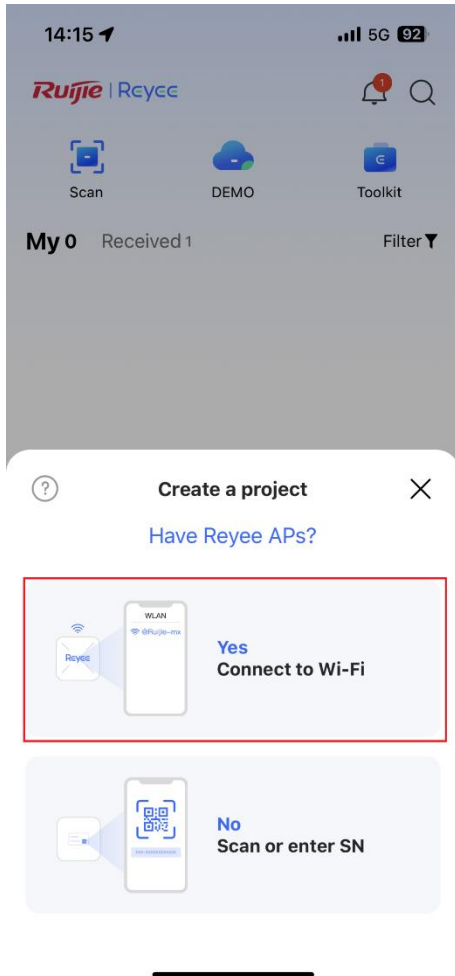


## 2. Procedure

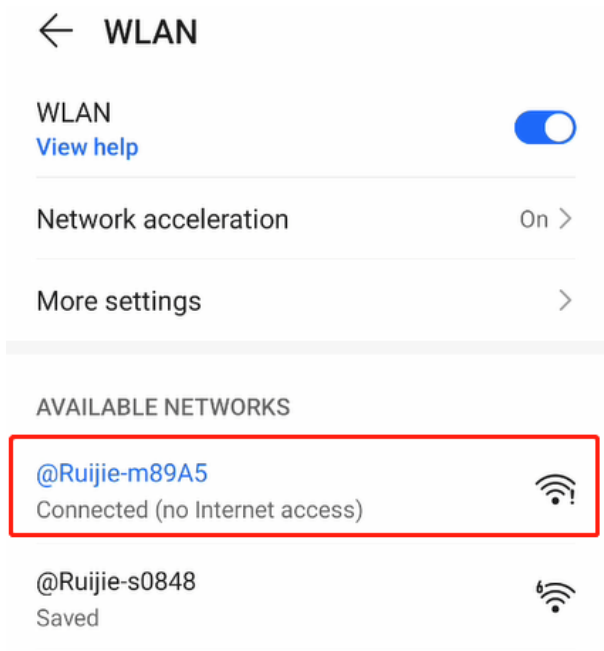
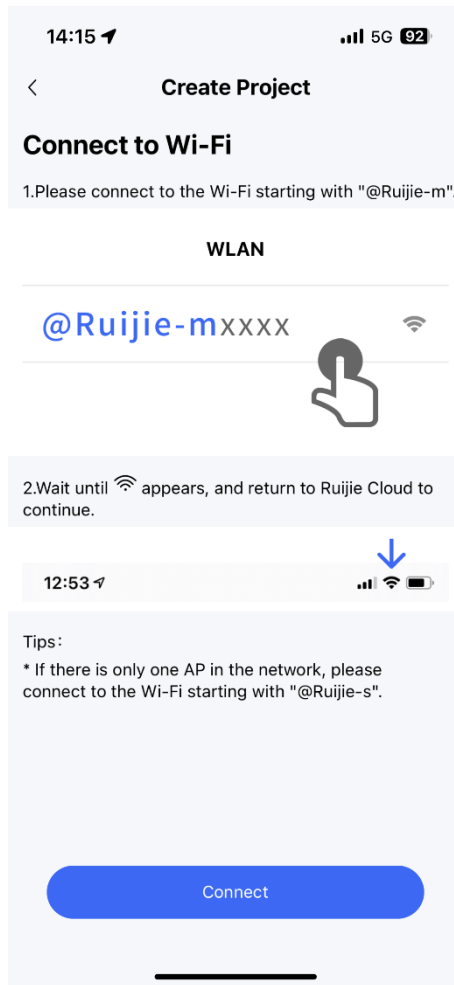
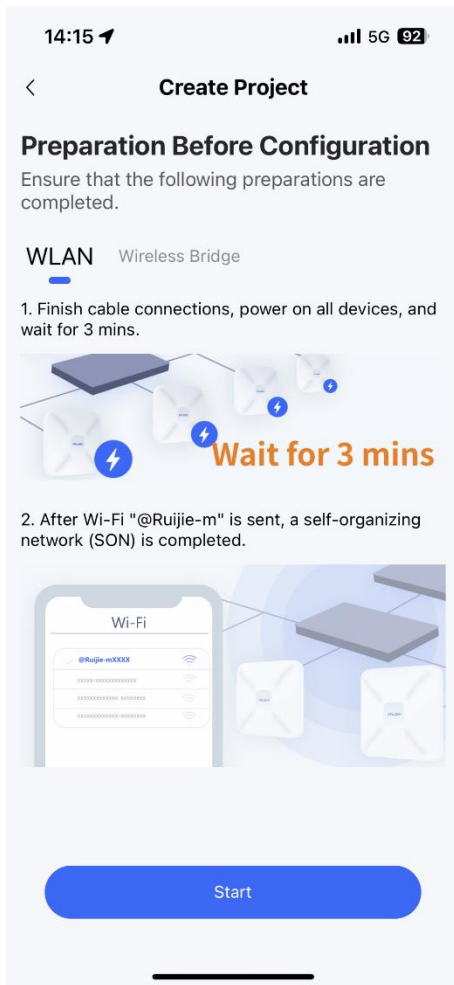
- (1) After the network environment is established according to the preceding figure, start the Ruijie Cloud app and choose **Project > Add a project**.



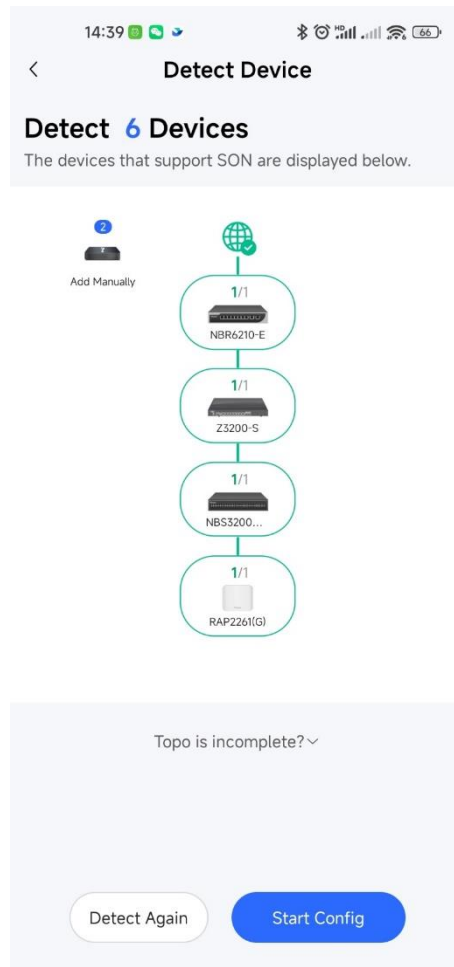
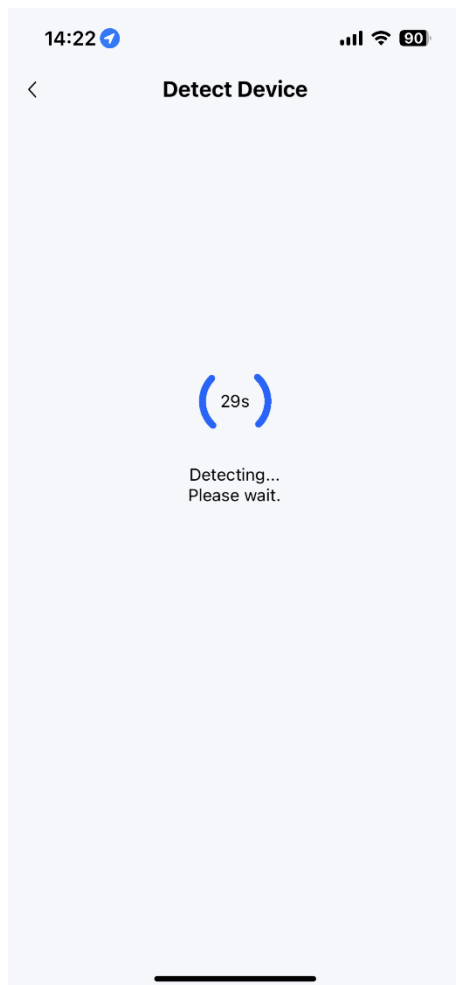
(2) Select **Connect to Wi-Fi** and add a project.



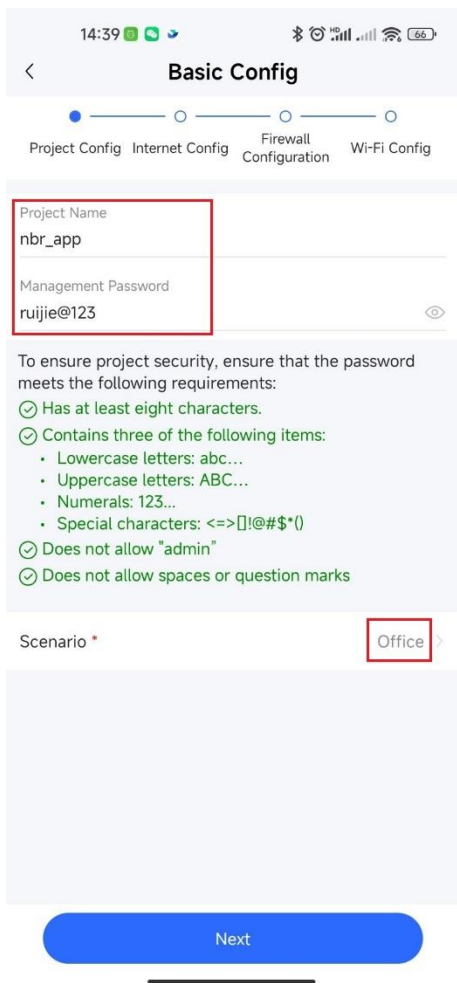
(3) Tap **Connect** to connect to the Wi-Fi signal of the Reyee AP.



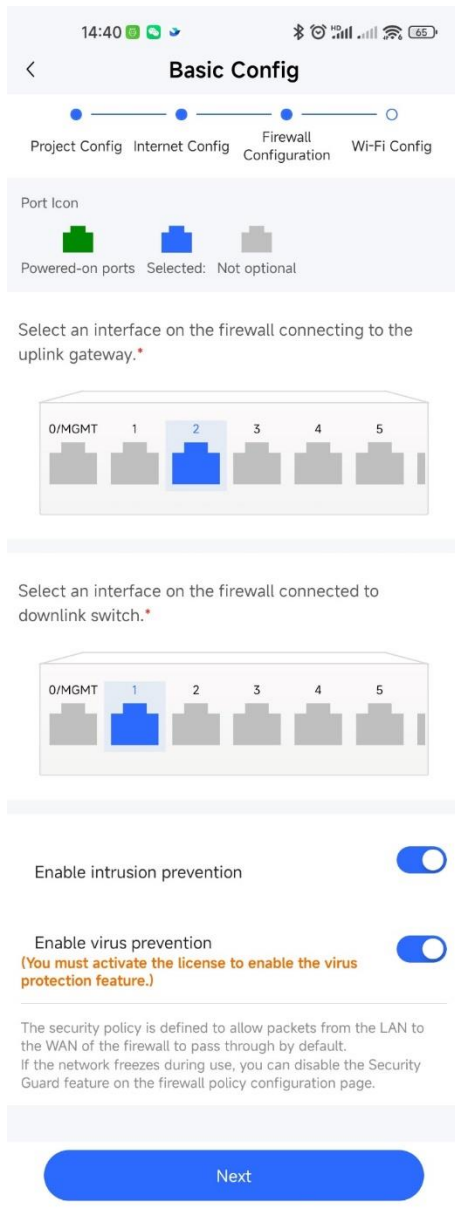
(4) Wait for about 30s until the system automatically generates the network topology. Then, tap **Start Config**.



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

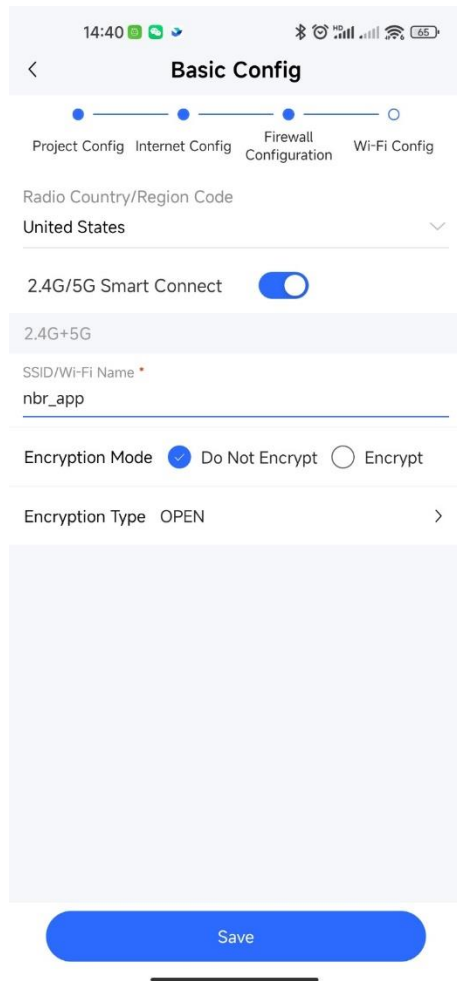


(6) Select the firewall interfaces connected to the router and switch, and tap **Next**.

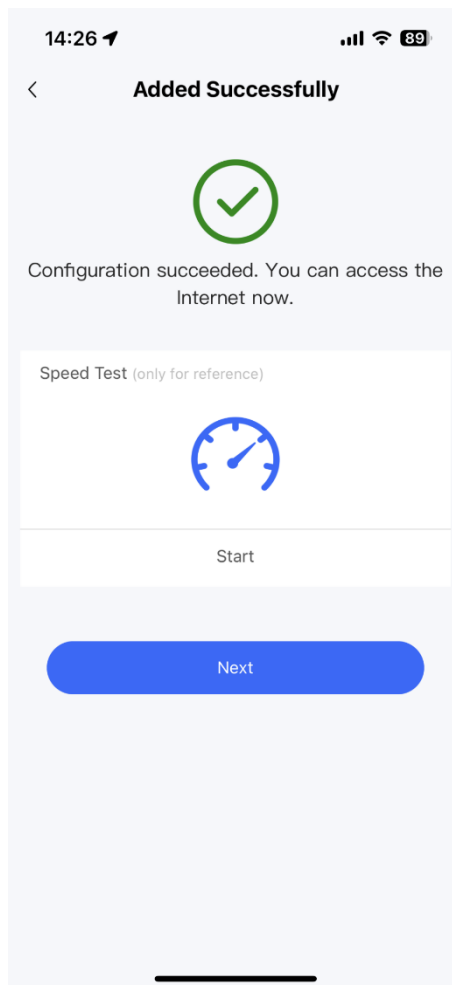
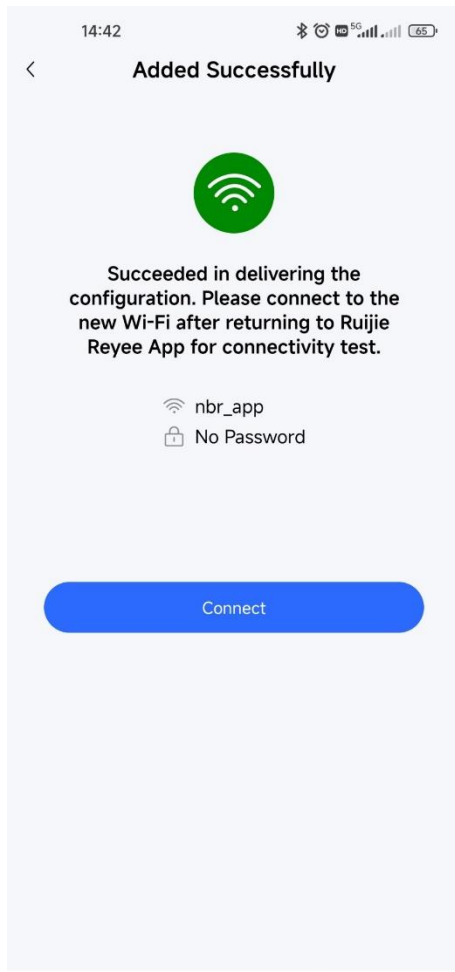


(7) Set the Wi-Fi name and password and tap **Save**.

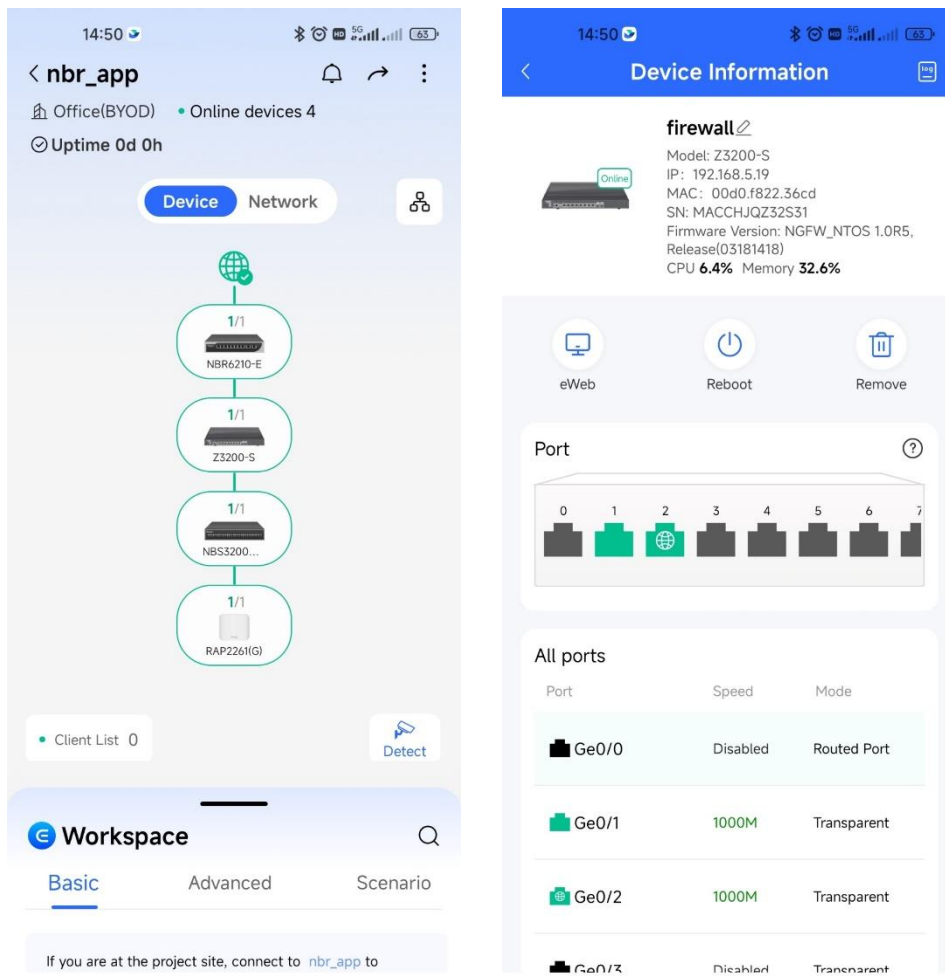




(8) After successful configuration delivery, connect to the new Wi-Fi.



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



## 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	<a href="https://www.ruijienetworks.com/">https://www.ruijienetworks.com/</a> Choose <b>Support &gt; Download &gt; Reyee</b> 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 <b>System &gt; System Maintenance &gt; System Upgrade &gt; Online Upgrade &gt; Recommended Version</b> 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 <b>Monitoring &gt; Device &gt; Firewall</b> , select a device, select a version, and click <b>Upgrade</b> .

---

**⚠ 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**.

---

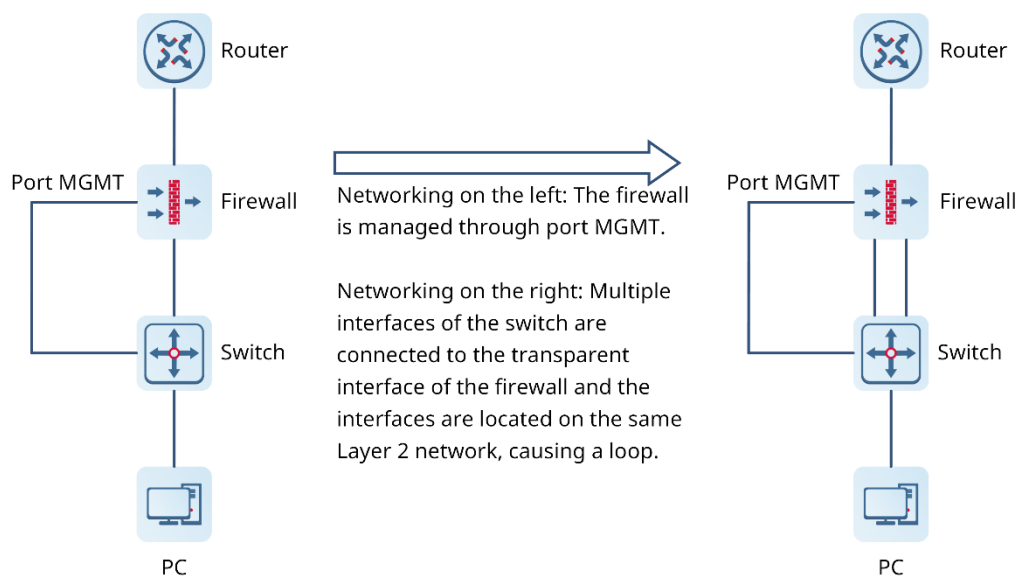
## 6.2.2 Deployment in Transparent Mode (Quick Deployment)

### 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



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.

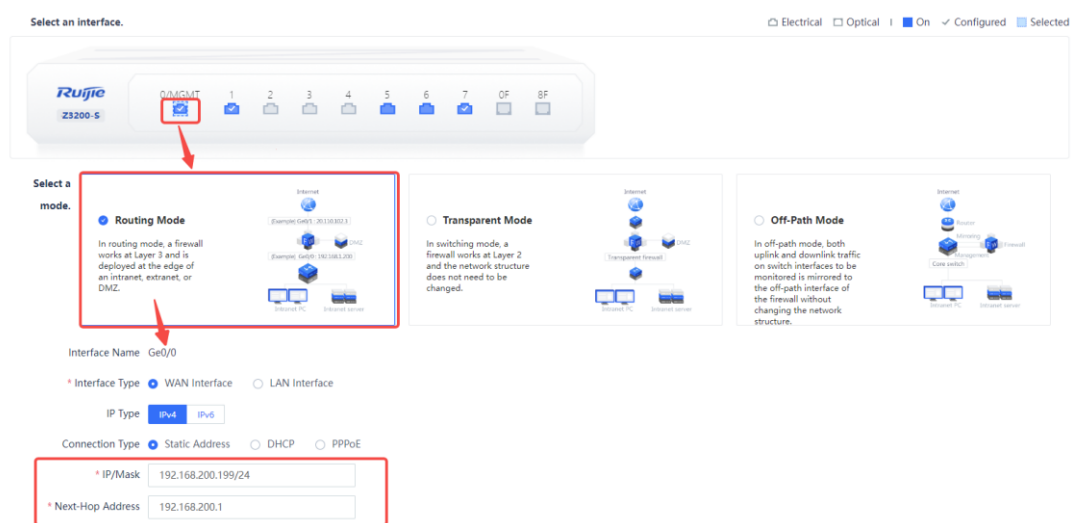
## (5) (Optional) Implement remote O&amp;M on the cloud.

**Procedure**

## (1) Implement quick onboarding.

## a Configure interfaces.

- o 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.)
- o 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.



## 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. 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

\* Bridge Interface  [Add Bridge Interface](#)

Member Interface

\* Connection Type  Static Address  DHCP

---

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 Ge0/6

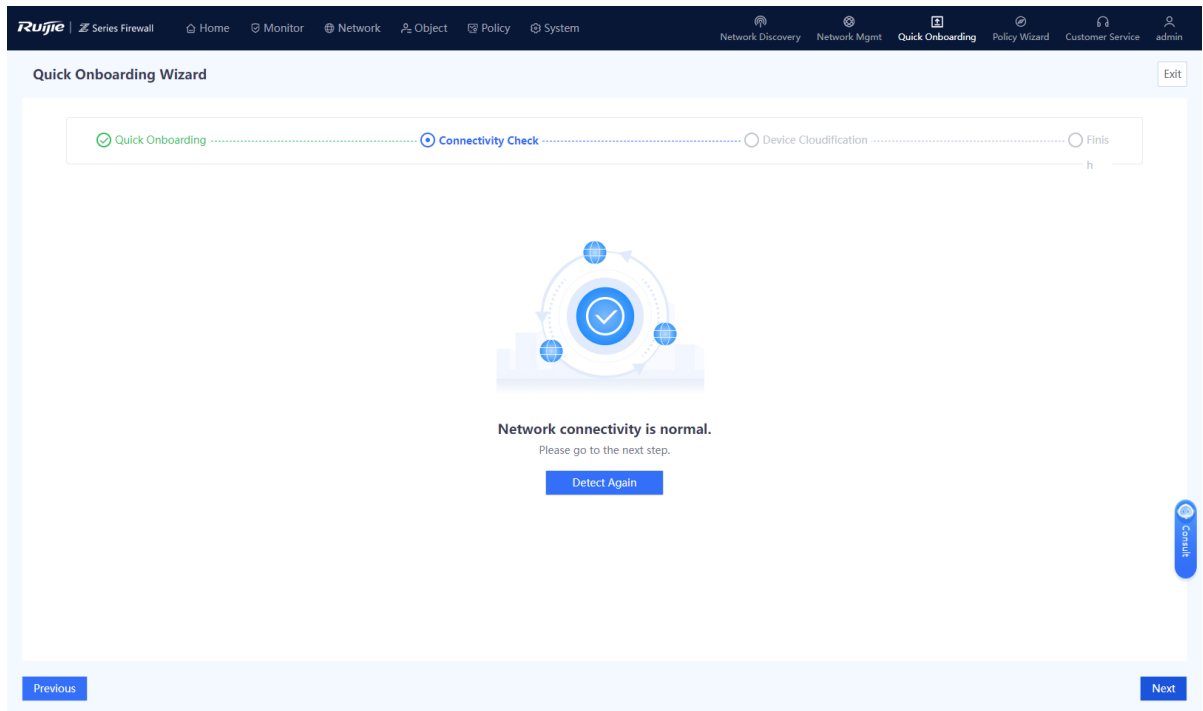
\* Interface Type  WAN Interface  LAN Interface

\* Bridge Interface  [Add Bridge Interface](#)

Member Interface

\* Connection Type  Static Address  DHCP

(2) (Optional) Check the connectivity.



### (3) Import licenses.

#### License Config

1. Before activating a device, register on and log in to Ruijie Secure Cloud Platform at <https://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](#)

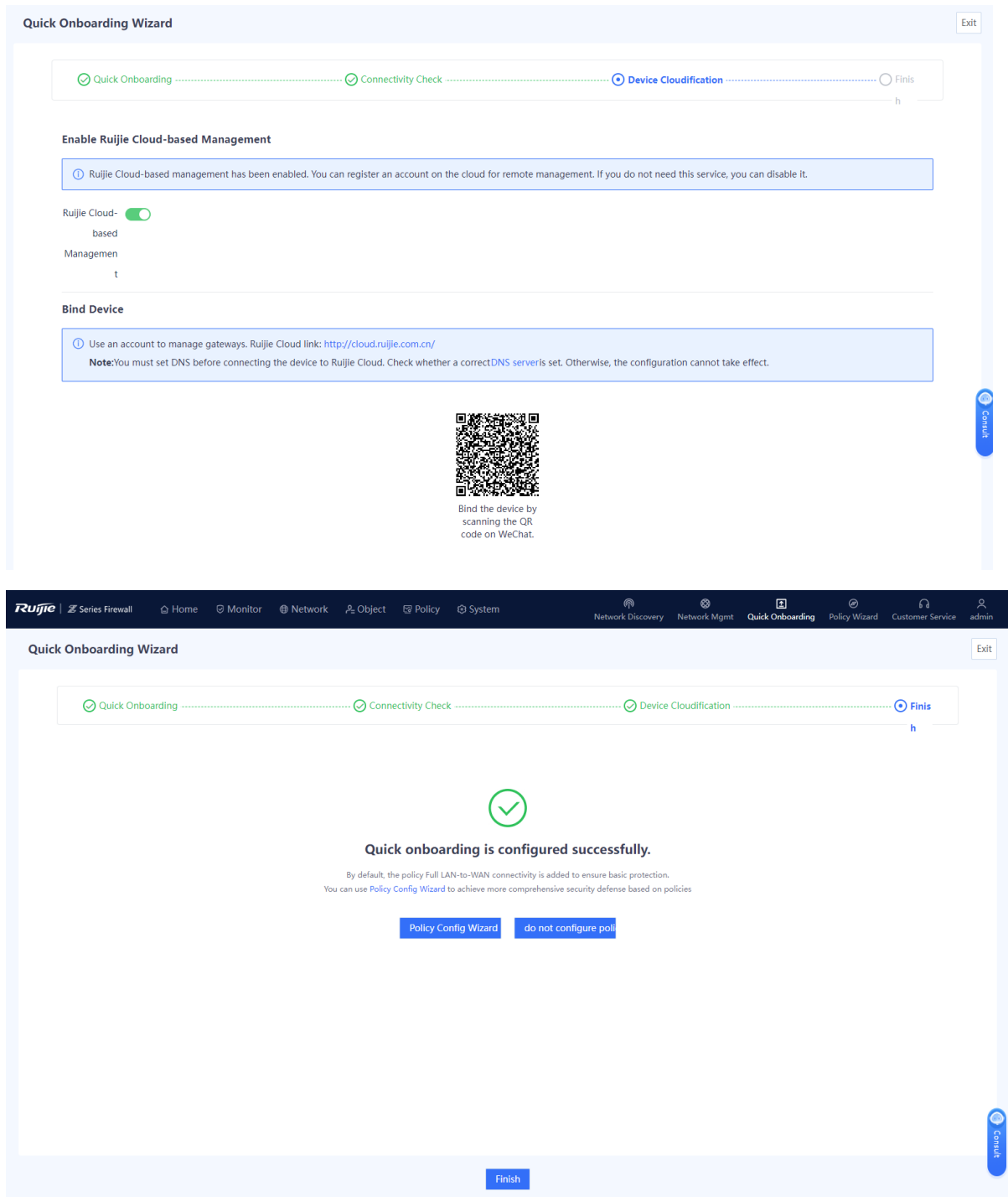
##### Performance License

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

##### SSL VPN License

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





### Configuration Verification

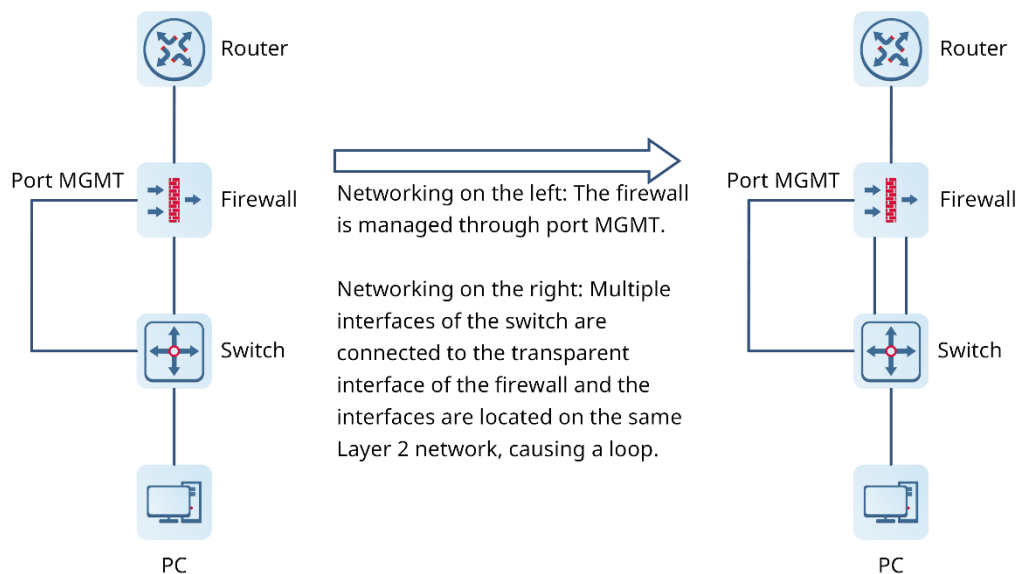
In transparent mode, the firewall can access the Internet without the need to modify the network environment, including the client IP address and gateway IP address.

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

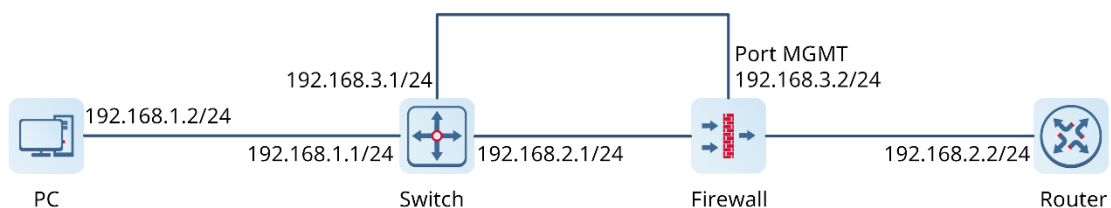
### Network Requirements

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.



### 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**.

< Back

### Edit Physical Interface

**Basic Info**

Interface Name

Description

Connection Status  Enable  Disable

Mode  Routing Mode  Transparent Mode  Off-Path Mode

\* Zone  [+ Add Security Zone](#)

Interface Type  WAN Interface  LAN Interface

---

**Address**

IP Type  IPv4  IPv6

Connection Type  Static Address  DHCP  PPPoE

\* IP/Mask

\* Next-Hop Address

Default Route

---

**Line Bandwidth**

Uplink

Downlink

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.
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**.

The screenshot shows the 'Edit Physical Interface' configuration page for interface Ge0/2. The 'Basic Info' section includes fields for 'Interface Name' (Ge0/2), 'Description', 'Connection Status' (Enable), and 'Mode' (Transparent Mode). A red box highlights the 'Bridge Interface' (br0), 'Zone' (trust), and 'Interface Type' (LAN Interface) fields. The 'Advanced' section includes 'MTU' (1500) and 'MAC' (00:d0:f8:22:37:0b).

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 <b>br0</b> .
Zone	Set to <b>trust</b> .
Interface Type	Set to <b>LAN Interface</b> .

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

< Back

## Edit Physical Interface

**Basic Info**

Interface Name

Description

Connection Status  Enable  Disable

Mode  Routing Mode  Transparent Mode  Off-Path Mode

\* Bridge Interface  [Add Bridge Interface](#)

\* Zone  [Add Security Zone](#)

Interface Type  WAN Interface  LAN Interface

---

**Advanced**

MTU

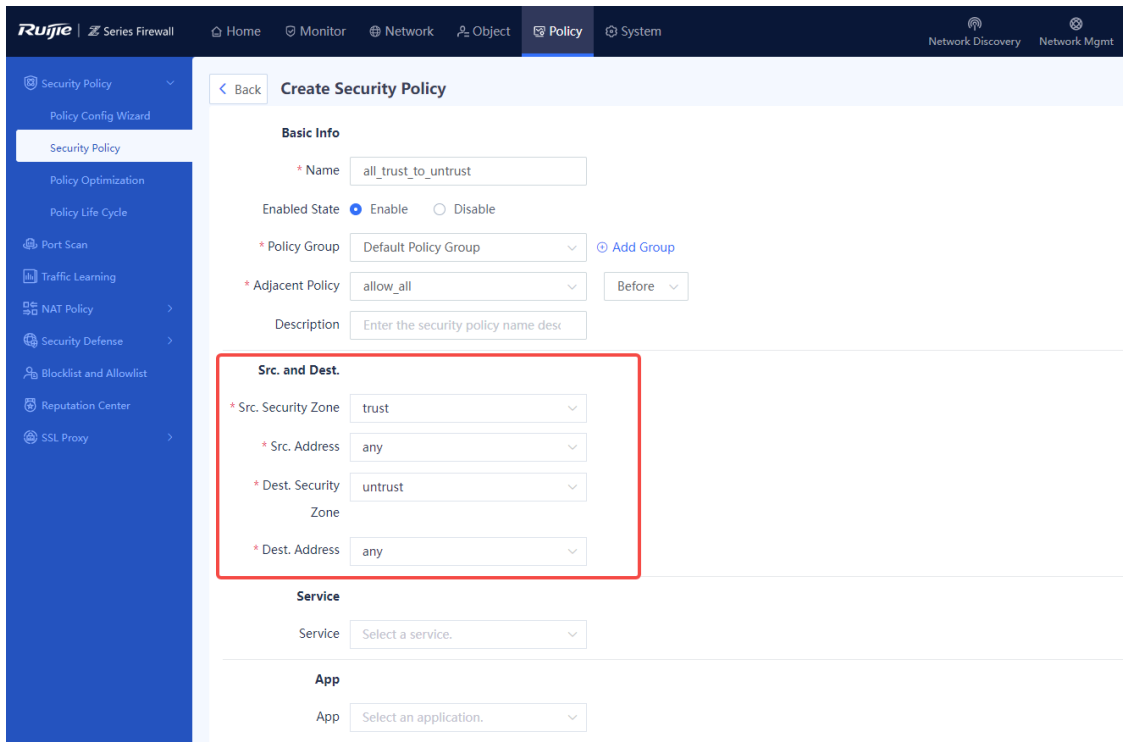
MAC  [Restore Default MAC](#)

The following figure shows the configuration result.

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**.

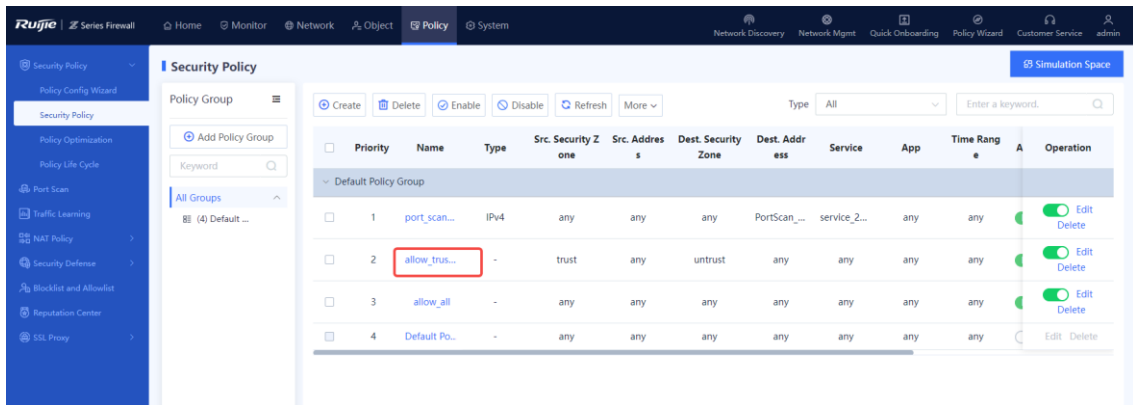
- a Choose **Policy > Security Policy > Security Policy**.
- b Click **Create**.



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

Item	Description
Policy Group	Set to the default policy group.
Src. Security Zone	Set to <b>trust</b> .
Src. Address	Set to <b>any</b> . This policy is applicable to all IP addresses in the source security zone after it takes effect.
Dest. Security Zone	Set to <b>untrust</b> .
Dest. Address	Set to <b>any</b> . This policy is applicable to all IP addresses in the destination security zone after it takes effect.

The following figure shows the configuration result.



### ⚠ 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.

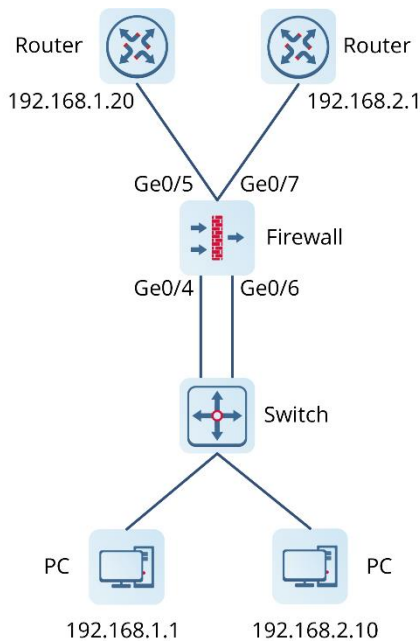
- You can successfully log in to the web management page to configure and manage the firewall.
- The PC on the same network segment as the management IP address can normally access the network.

## 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.

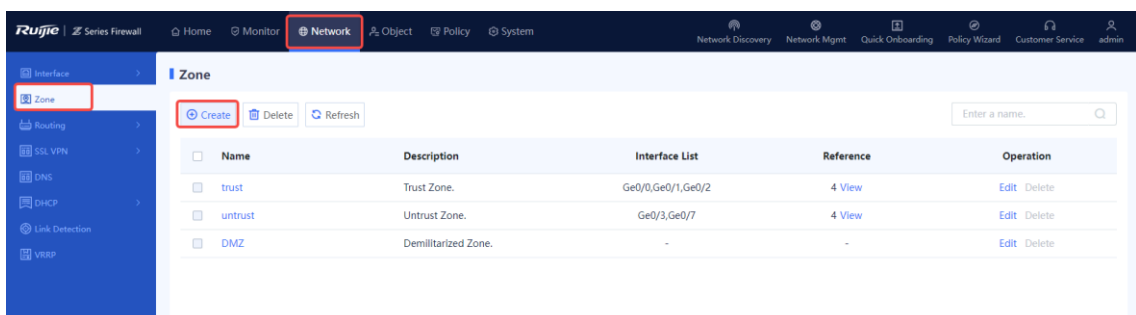
### ⚠ Caution

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**.





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

The screenshot shows the 'Add Security Zone' configuration page. At the top left, there is a '< Back' button. The main title is 'Add Security Zone'. Below the title, there are three main sections: 'Name', 'Description', and 'Interface'. The 'Name' field is labeled '\* Name' and contains the text 'trust1', which is highlighted with a red rectangular box. The 'Description' field is empty. The 'Interface' section is divided into two panes: 'To-be-selected (6)' and 'Selected (0)'. The 'To-be-selected' pane has a 'Select All' checkbox and a search input field with the placeholder text 'Enter the keyword.'. Below the search field is a list of interfaces with checkboxes: Ge0/4, Ge0/5, Ge0/6, Ge0/8, and TenGe0/0. The 'Selected' pane also has a search input field with the placeholder text 'Enter the keyword.' and a 'Clear' button. At the bottom right of the page, there is a blue 'Save' button.

- c Configure parameters for the security zone **trust1** and click **Save**.
- d Repeat the preceding steps to create other security zones.

---

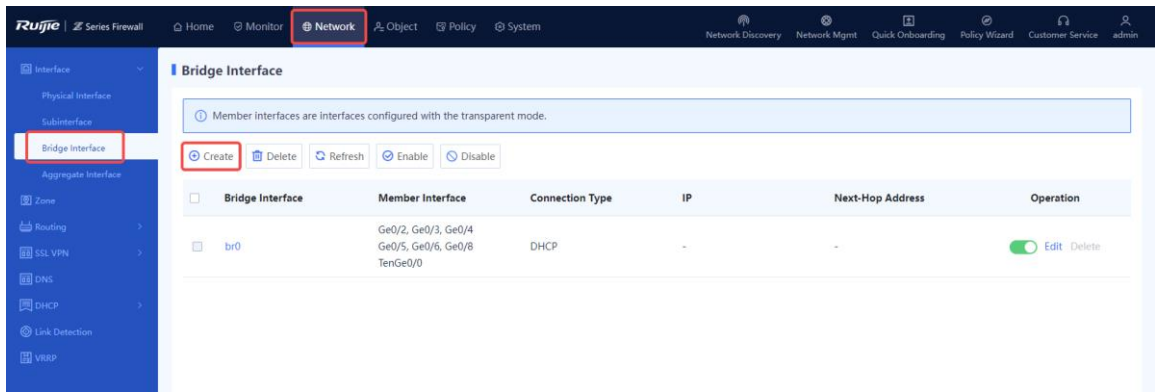
**⚠ Caution**

The security zone name must be unique.

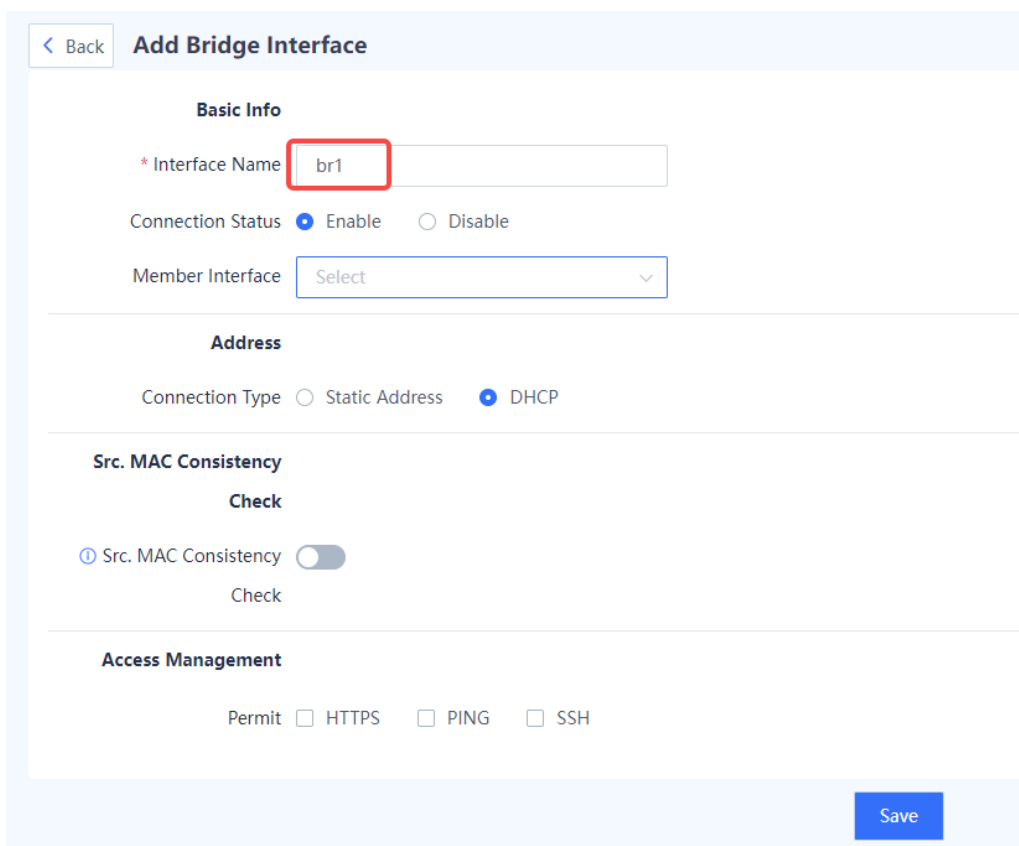
---

(2) Create bridge interfaces.

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

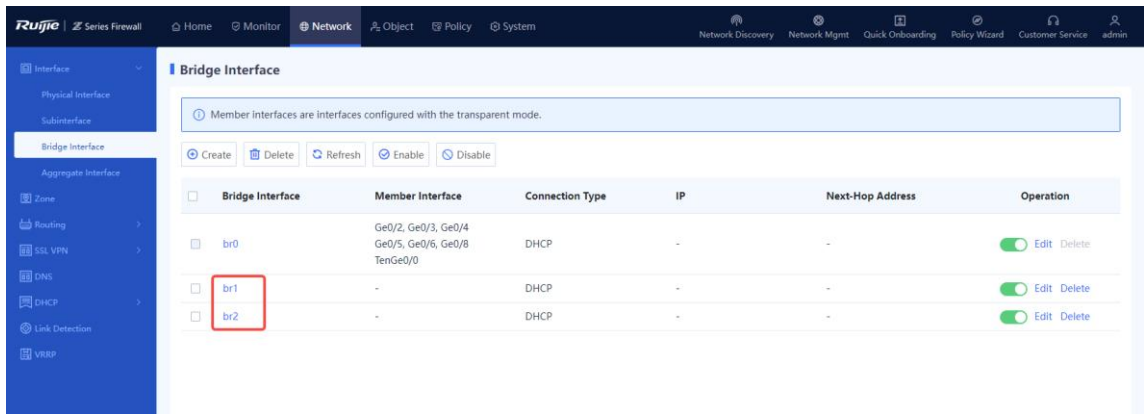


b Click **Create** and create bridge interface **br1**.



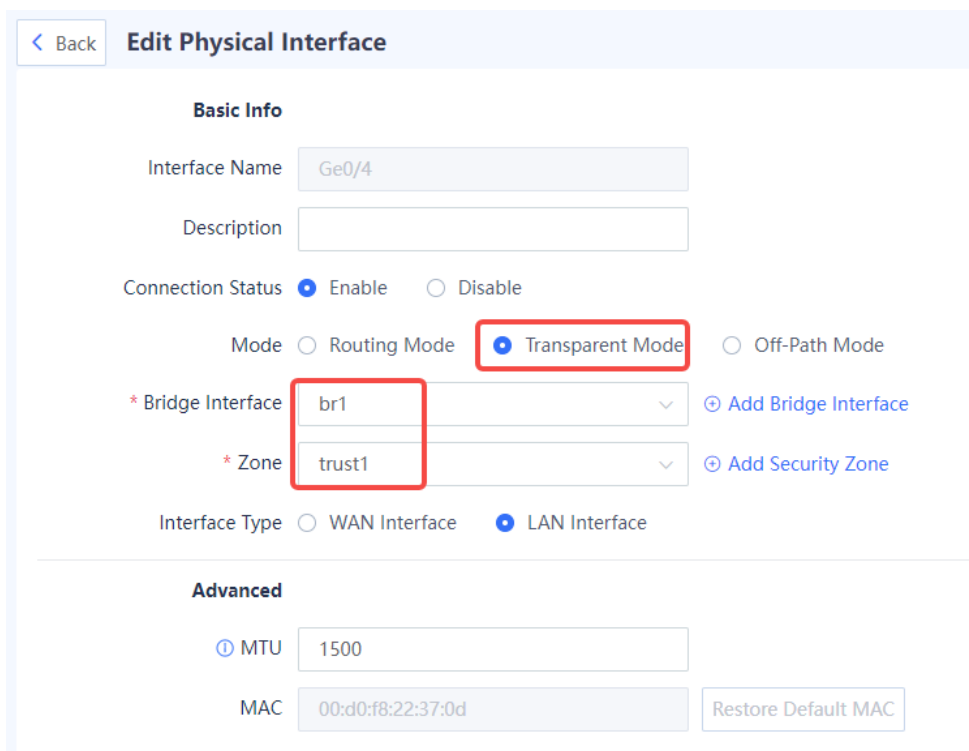
c Configure parameters for the bridge **br1** and click **Save**.

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



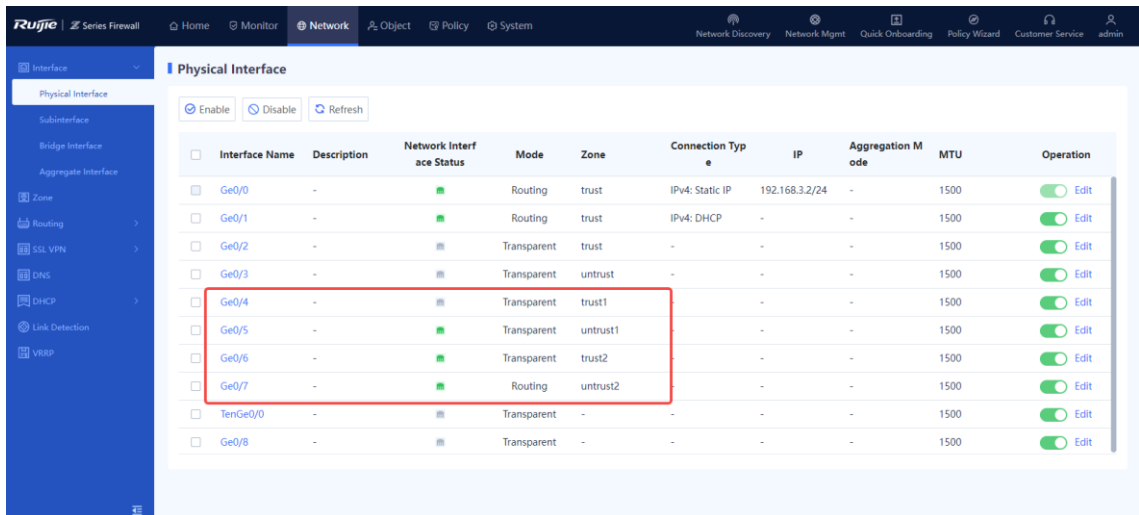
(3) Convert two pairs of interfaces to transparent mode and add them to the corresponding bridge interfaces and zones.

- a Choose **Network > Interface > Physical Interface**.
- b Select the corresponding interface and click **Edit**.



- 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**.

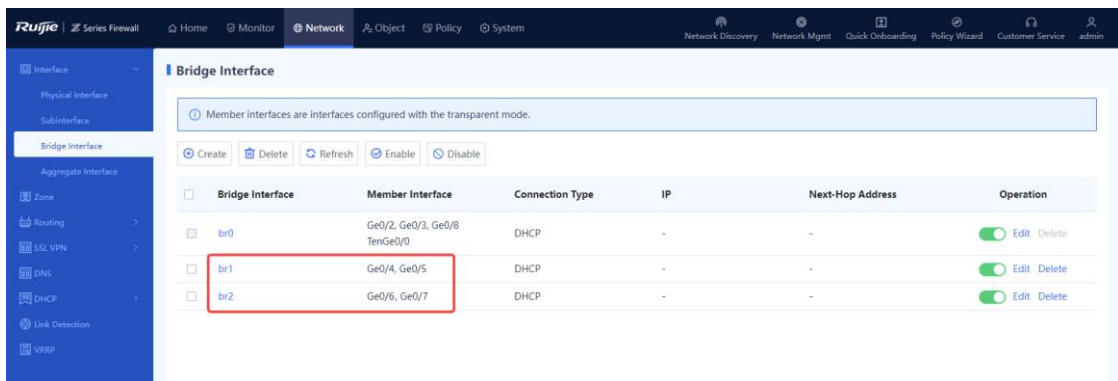
The following figure shows the configuration result.



**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.



(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

Enabled State  Enable  Disable

\* Policy Group  ⊕ Add Group

\* Adjacent Policy

Description

---

**Src. and Dest.**

\* Src. Security Zone

\* Src. Address

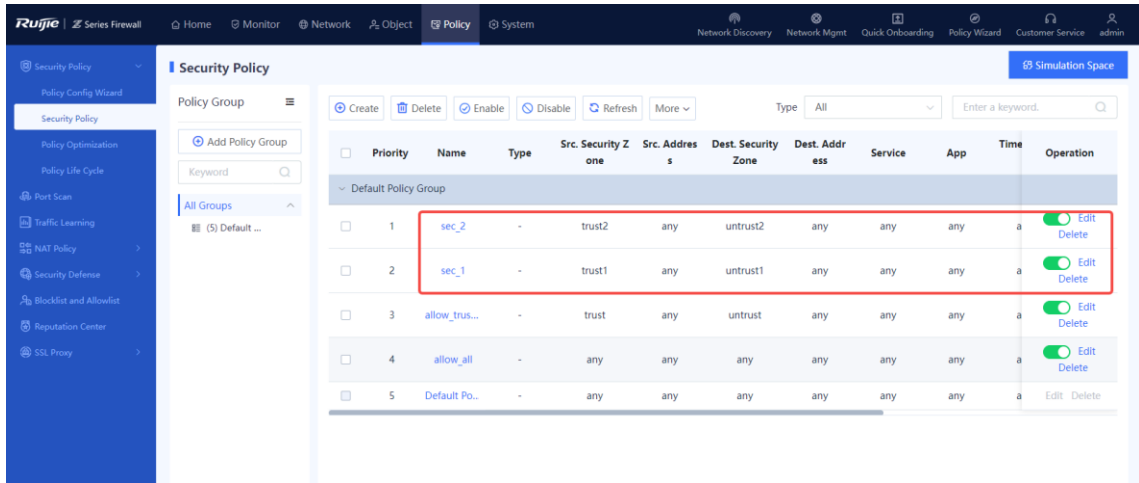
\* Dest. Security Zone

\* Dest. Address

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

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

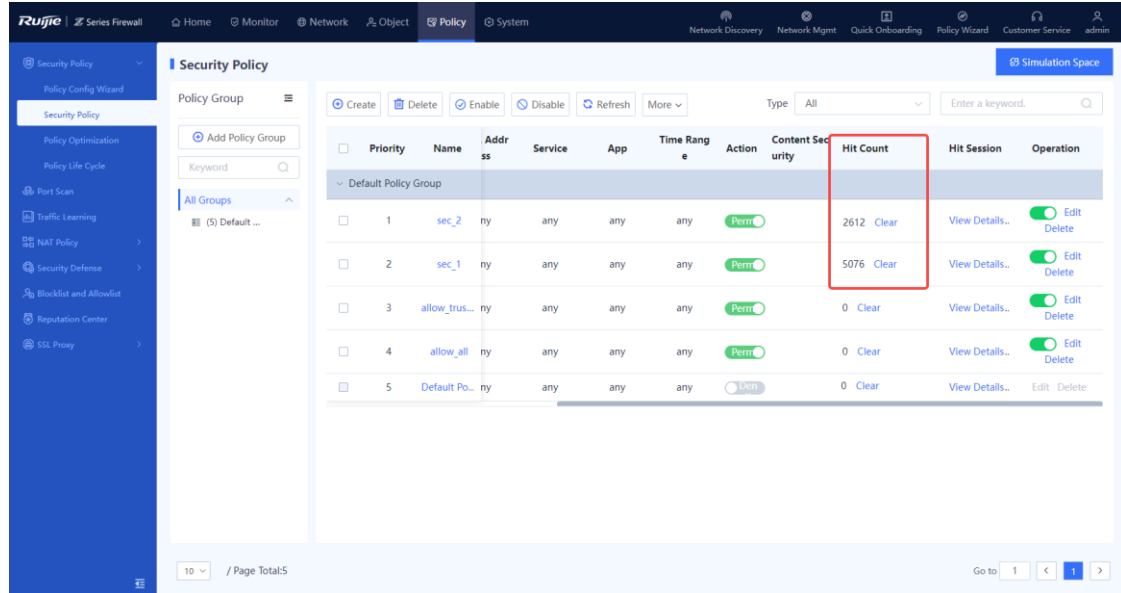
- d Repeat the preceding steps to create security policy 2 and associate it with zones **trust2** and **untrust2**.



### 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.



- (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.

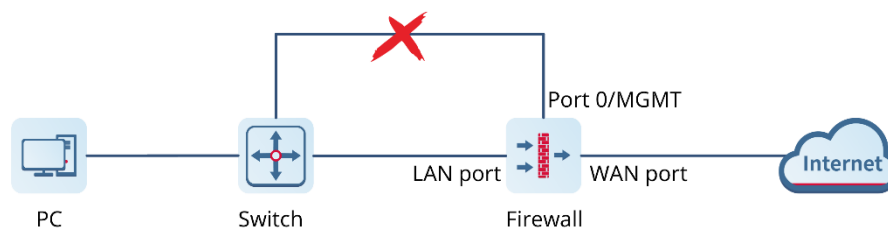
## 6.2.6 Configuring a Bridge Interface

### 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.

<input type="checkbox"/>	Bridge Interface	Member Interface	Connection Type	IP	Next-Hop Address	Operation
<input type="checkbox"/>	br0	Ge0/2, Ge0/3, Ge0/8 TenGe0/0, Ge0/5	DHCP	-	-	<input checked="" type="checkbox"/> 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

---

**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	Name of a bridge interface.	<ul style="list-style-type: none"> <li>● Characters such as `~!#%^&amp;*+ \{ };:~/'&lt;&gt;?` and spaces are not allowed.</li> <li>● The name is specified when you create a bridge interface and cannot be modified in later steps.</li> </ul> <p>[Example]</p> <p>br1</p>
Connection Status	Whether to enable the bridge interface.	[Example] Enable
Member Interface	Member interface in the bridge interface.  Members of the bridge interface	To add a member to the bridge interface, set <b>Bridge Interface</b> to the current bridge interface when you

Item	Description	Remarks
	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.	configure the corresponding member interface (such as physical interface or aggregate interface).  [Example] Ge0/2
Address		
Connection Type	<p>Connection type of the bridge interface. The options are as follows:</p> <ul style="list-style-type: none"> <li>● <b>Static Address:</b> 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. When this option is selected, you need to set IP/Mask and Next-Hop Address.</li> <li>● <b>DHCP:</b> 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.</li> </ul>	[Example] Static Address
IP/Mask	IP address and mask of the interface.	You need to set this parameter when <b>Connection Type</b> is set to <b>Static Address</b> .  [Example] 192.168.20.1/24
Next-Hop	Next router address to reach the	You need to set this parameter when

Item	Description	Remarks
Address	router with the destination address.	<b>Connection Type</b> is set to <b>Static Address</b> . [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 <b>Enable</b> , 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 check the session status of the packet but transparently forwards the packet over the bridge network directly.	[Example] Enable
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 <b>HTTPS</b> .

## 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	<p><a href="https://www.ruijienetworks.com/">https://www.ruijienetworks.com/</a></p> <p>Choose <b>Support</b> &gt; <b>Download</b> &gt; <b>Reyee</b> and find the latest version of the Z-S series firewall under RG-WALL 1600-Z-S series cloud management firewalls.</p>
Web management page of the firewall	<p>Choose <b>System</b> &gt; <b>System Maintenance</b> &gt; <b>System Upgrade</b> &gt; <b>Online Upgrade</b> &gt; <b>Recommended Version</b> to upgrade to the latest version (recommended) in online mode.</p>
Ruijie Cloud	<p>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).</p> <p>Choose <b>Monitoring</b> &gt; <b>Device</b> &gt; <b>Firewall</b>, select a device, select a version, and click <b>Upgrade</b>.</p>

---

**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**.

---

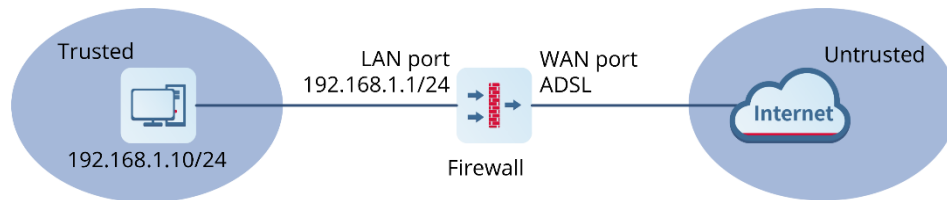
## 6.3.2 Single-Line Onboarding (Quick Deployment)

### 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 O/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 O/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:

\* DHCP Address Pool:  -

---

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

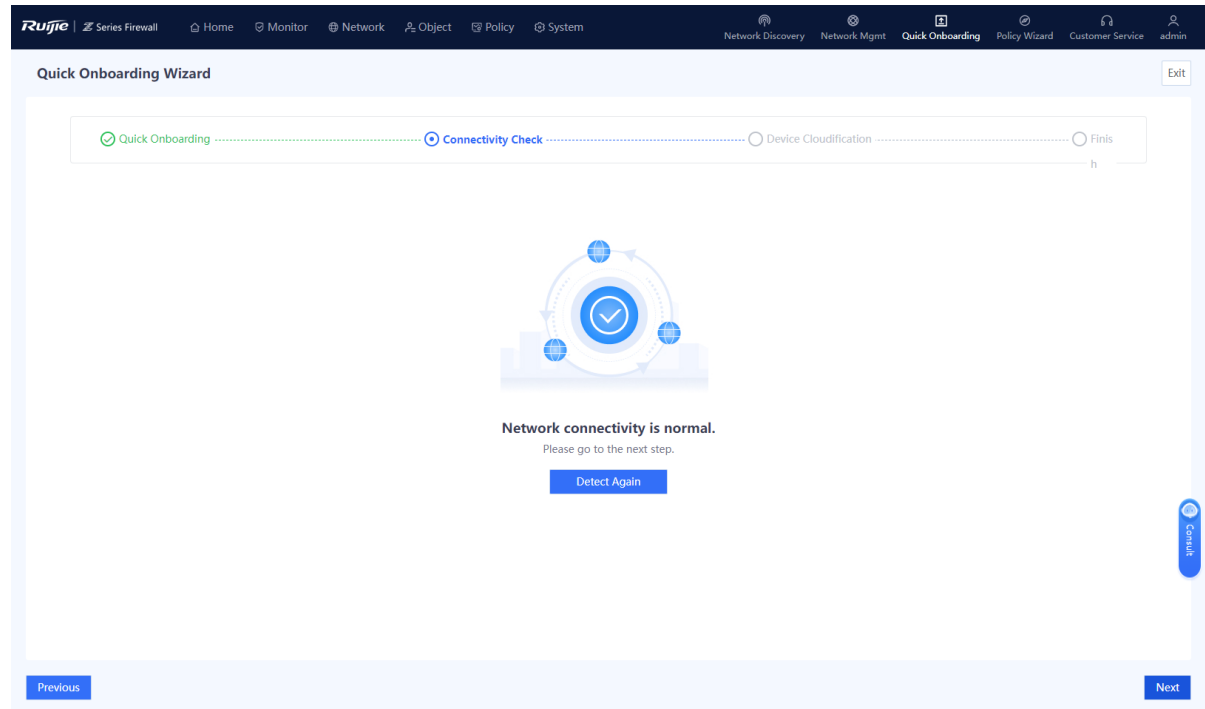
IP Type:  IPv4  IPv6

Connection Type:  **DHCP**  Static Address  PPPoE

**⚠ Caution**

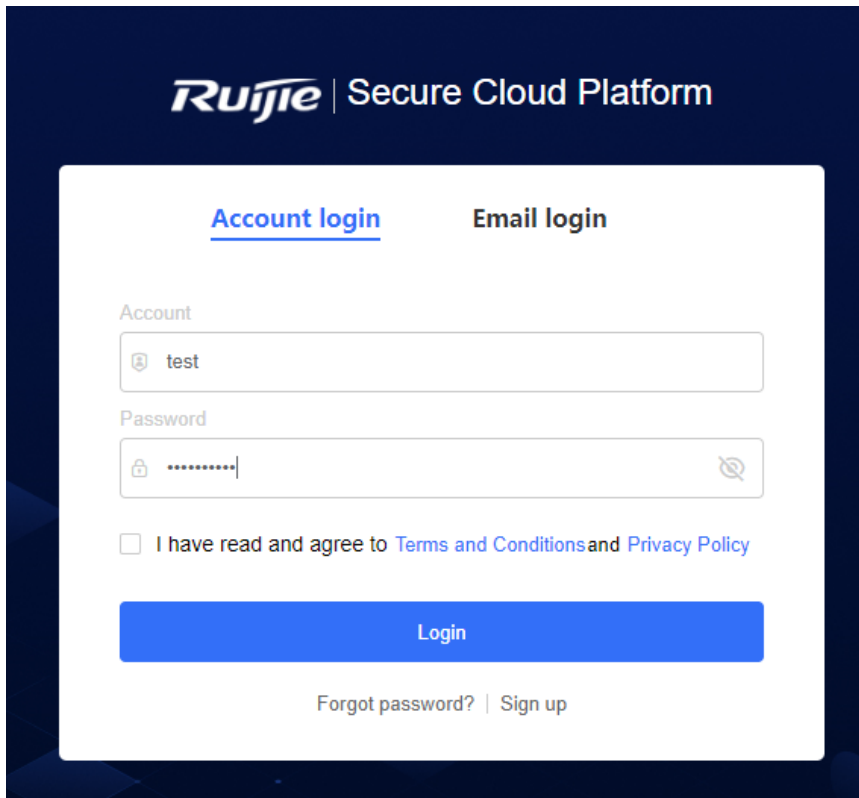
Each interface can be separately configured to work in routing or bridge mode.

(2) (Optional) Check the connectivity.



(3) (Optional) Import licenses.

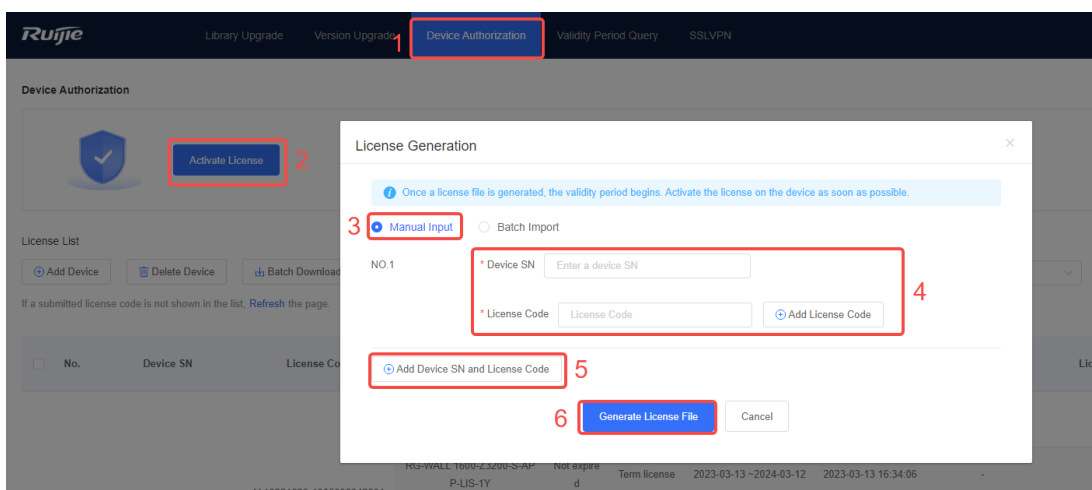
- a Before license activation, log in to the Ruijie Secure Cloud Platform (<https://secloud-en.ruijienetworks.com>).



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.)



c Download the license file.



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	ssstests1604	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	-	-	<a href="#">Download</a>
			RG-WALL 1600-Z3200-S-URL-LIS-1Y	Not expired	Term license	2023-03-13 ~ 2024-03-12	2023-03-13 15:48:19	-	-	<a href="#">Download</a>
			RG-WALL 1600-Z3200-S-AV-LIS-1Y	Not expired	Term license	2023-03-13 ~ 2024-03-12	2023-03-13 15:48:19	-	-	<a href="#">Download</a>
			RG-WALL 1600-Z3200-S-APP-LIS-1Y	Not expired	Term license	2023-03-13 ~ 2024-03-12	2023-03-13 15:48:19	-	-	<a href="#">Download</a>
			RG-WALL 1600-Z3200-S-IPS-LIS-1Y	Not expired	Term license	2023-03-13 ~ 2024-03-12	2023-03-13 15:48:19	-	-	<a href="#">Download</a>

- 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 at <https://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.

Device SN: **MACC932672666**

**License Info** [How to Obtain License](#)

- Performance License**  
Available Performance: 3G (Basic Performance 1G + Added New Performance 2G) Performance to Be Added: 0G **3G/3G**
- SSL VPN License**  
Max. Concurrent License Sessions: 25 (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**

Activate License

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
			RG-WALL 1600-Z3200-S-AV-LIS-1Y	Not expired	Term license	2023-03-13 - 2024-03-12	2023-03-13 15:48:19			<a href="#">Export License File</a> <input type="button" value="Download"/>
			RG-WALL 1600-Z3200-S-AP-LIS-1Y	Not expired	Term license	2023-03-13 - 2024-03-12	2023-03-13 15:48:19	-	-	<input type="button" value="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	-	-	<input type="button" value="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	-	-	<input type="button" value="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	-	-	<input type="button" value="Download"/>
			RG-WALL 1600-Z3200-S-AP-LIS-1Y	Not expired	Term license	2023-03-13 - 2024-03-12	2023-03-13 15:48:19	-	-	<input type="button" value="Download"/>

**Authorization Management**

**License Config**

1. Before activating a device, register on and log in to Ruijie Secure Cloud Platform at <https://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.

Device SN: **MACC932672666**

**License Info** [How to Obtain License](#)

Performance License

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

### 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 at <https://secloud1.ruijie.com.cn> On 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 License File

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

Upload

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

Quick Onboarding Wizard Exit

Quick Onboarding Connectivity Check Device Cloudification Finish

#### 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 correct DNS server is set. Otherwise, the configuration cannot take effect.

Bind the device by scanning the QR code on WeChat.

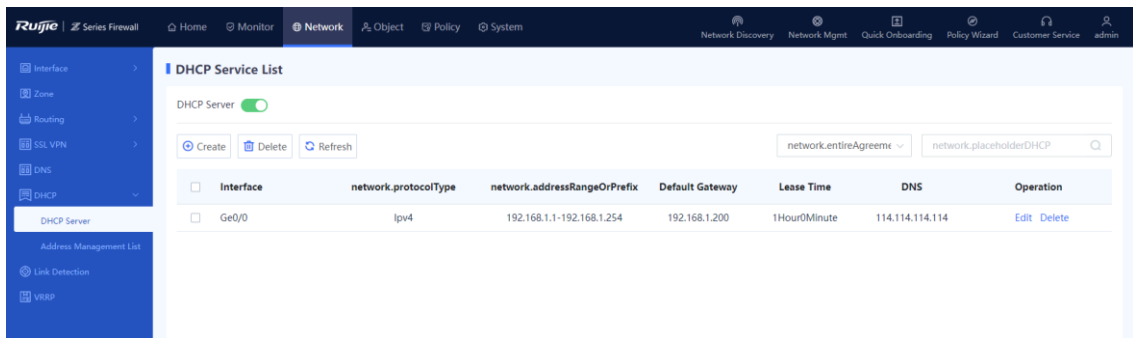
Continue

### Configuration Verification

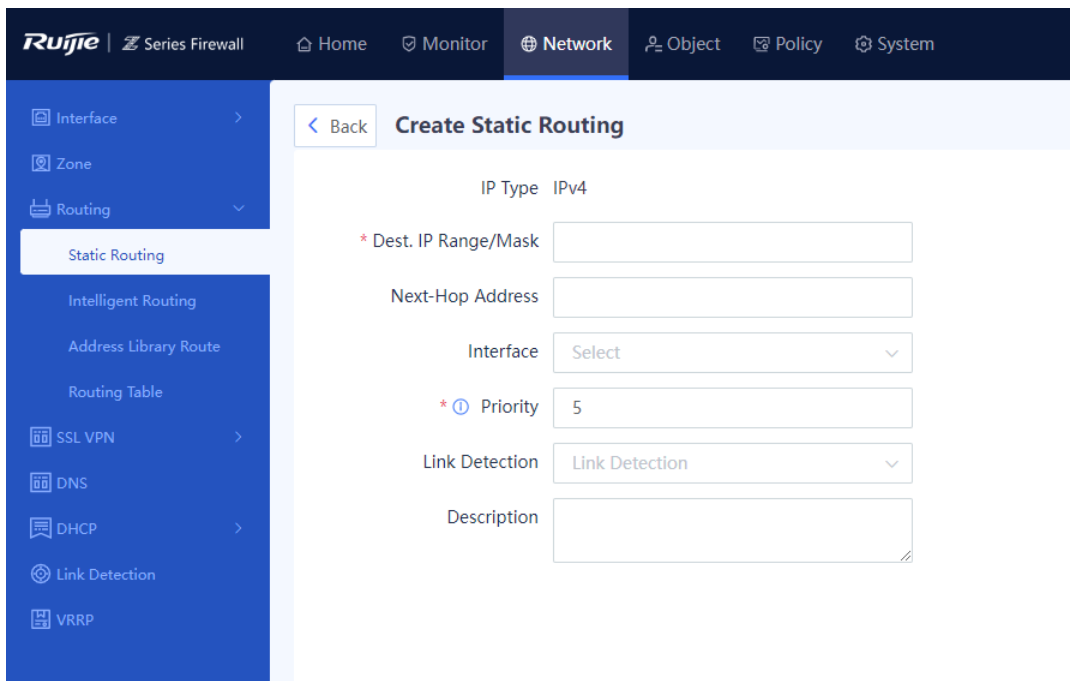
Set the IP address of the PC to 192.168.1.1/24, gateway address to 192.168.1.200, and DNS server addresses to 114.114.114.114 (primary) and 223.5.5.5 (secondary). (The address of the local DNS server must be used.) The PC can normally access the Internet.

**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**.



- 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.)



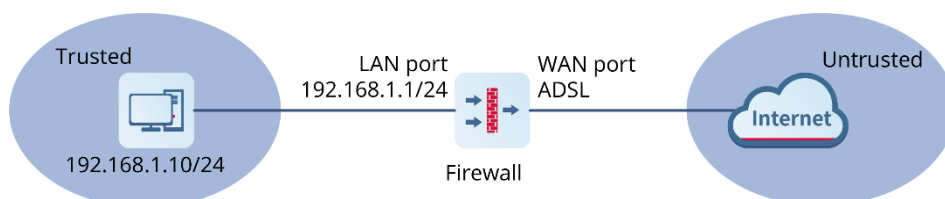
### 6.3.3 Single-Line Onboarding (Custom Deployment)

#### 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 <b>admin</b> and <b>ruijie@123</b> .

##### Configuration Points

Step	Description	Key Configuration
Configure interfaces.	<p>Select two interfaces on the device and set the interface type to WAN interface and LAN interface respectively.</p> <ul style="list-style-type: none"> <li>● WAN interface: Used to connect to the Internet.</li> <li>● LAN interface: Used to connect to the LAN.</li> </ul>	<ul style="list-style-type: none"> <li>● WAN interface: Set Connection Type to PPPoE and add the interface to the security zone untrust. The system automatically generates a default route.</li> <li>● 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</li> </ul>

		interface.
Create an address object.	To facilitate management, configure the IP address of the LAN user as an address object.	Set the name to <b>lan</b> 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.	<ul style="list-style-type: none"> <li>● Src. Security Zone: trust</li> <li>● Src. Address: lan</li> <li>● Dest. Security Zone: untrust</li> <li>● Dest. Address: any</li> </ul>
Configure NAT.	Configure source NAT to allow the LAN user to normally access the Internet.	<ul style="list-style-type: none"> <li>● Src. Security Zone: trust</li> <li>● Src. Address: lan</li> <li>● Dest. Security Zone: untrust</li> <li>● Dest. Address: any</li> <li>● Src. Address Translated to: Outbound Interface Address</li> </ul>

### 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

Description

Connection Status  Enable  Disable

Mode  Routing Mode  Transparent Mode  Off-Path Mode

\* Zone  [+ Add Security Zone](#)

Interface Type  WAN Interface  LAN Interface

---

**Address**

IP Type  IPv4  IPv6

Connection Type  Static Address  DHCP  PPPoE

\* Account

\* 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  ▾

MTU

MAC  Restore Default MAC

Link Detection  ▾

e Click **Save**.

After successful configuration, interface information marked in the red block is displayed, as shown in the following figure.

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
Ten-GigE0/0	-	■	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

Description

Connection Status  Enable  Disable

Mode  Routing Mode  Transparent Mode  Off-Path Mode

\* Zone  [+ Add Security Zone](#)

Interface Type  WAN Interface  LAN Interface

---

**Address**

IP Type  IPv4  IPv6

Connection Type  Static Address  DHCP  PPPoE

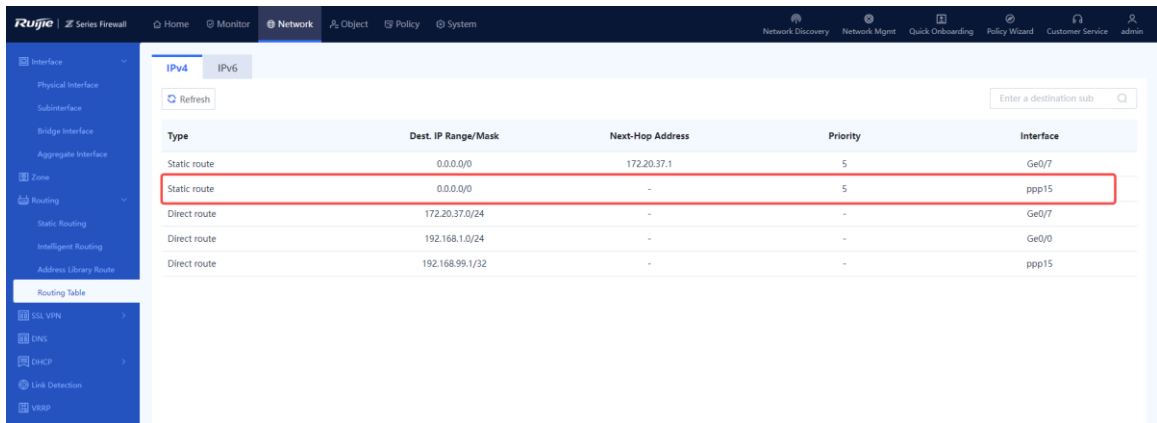
\* IP/Mask

- 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

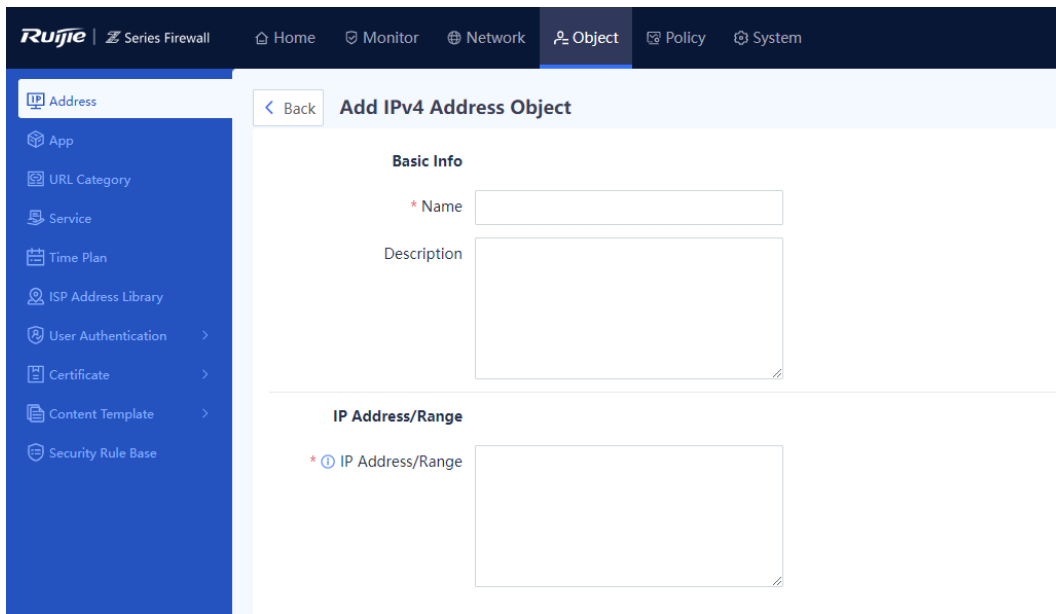
- d Enable management functions on the interface as required. You are advised to enable the HTTPS, ping, and SSH services only on the LAN interface.
- e Click **Save**.

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.



(3) Configure address resources.

- a Choose **Object > Address > IPv4 Address**.
- b Click **Create** and add an address object with a LAN IP address.



- c Set parameters for the address object.  
Set **Name** to **Ian** 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

Enabled State  Enable  Disable

\* Policy Group  [⊕ Add Group](#)

\* Adjacent Policy

Description

---

**Src. and Dest.**

\* Src. Security Zone

\* Src. Address

\* Dest. Security Zone

\* Dest. Address

---

**Service**

Service

---

**App**

App

---

**Time Range**

Time Range  [⊕ 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**

c Set parameters for the policy.

Item	Description
Src. Security Zone	trust
Src. Address	lan

Item	Description
Dest. Security Zone	untrust
Dest. Address	any
Service	any
App	any

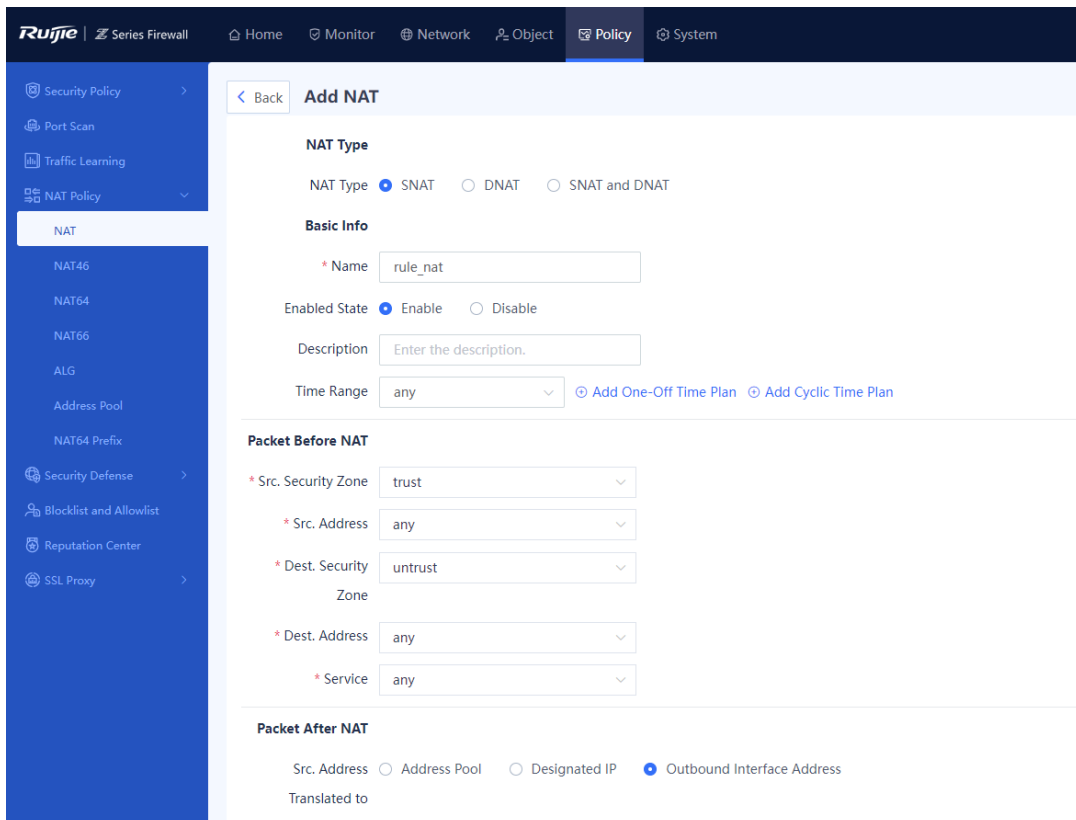
d Click **Confirm**.

(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**.



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.)

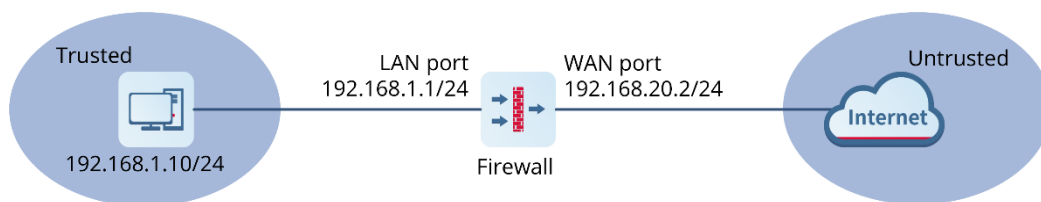
The PC can successfully ping the address 114.114.114.114.

## 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 <b>trust</b> . The IP address is 192.168.1.1/24.

---

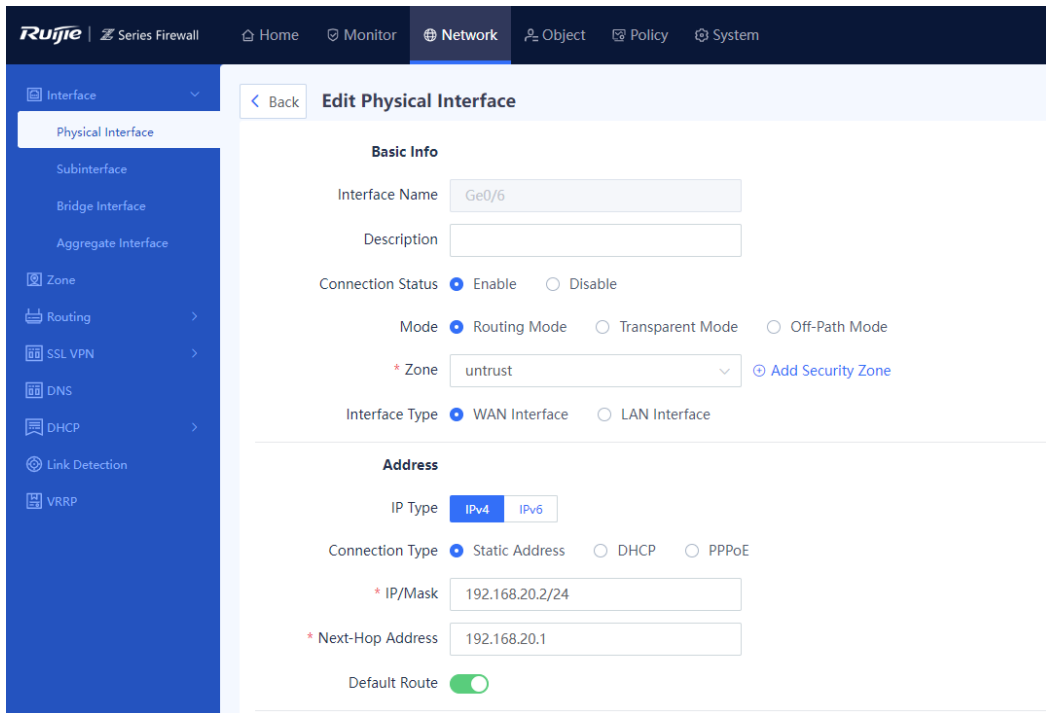
Ge0/6	WAN interface, which belongs to the security zone <b>untrust</b> . The fixed IP address allocated by the ISP to this interface and the gateway address are 192.168.20.2/20 and 192.168.20.1, respectively.
DNS	The DNS address is 192.168.58.110, which is obtained from the ISP.

### Configuration Points

Step	Description	Key Configuration
Configure interfaces.	<p>Select two interfaces on the device and set the interface type to WAN interface and LAN interface respectively.</p> <ul style="list-style-type: none"> <li>● WAN interface: Used to connect to the Internet.</li> <li>● LAN interface: Used to connect to the LAN.</li> </ul>	<ul style="list-style-type: none"> <li>● WAN interface: Set <b>Connection Type</b> to <b>Static Address</b> and configure the next-hop address.</li> <li>● Add the interface to the security zone untrust. The system automatically generates a default route.</li> <li>● 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.</li> </ul>
Create an address object.	To facilitate management, configure the IP address of the LAN user as an address object.	Set the name to <b>lan</b> 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.	<ul style="list-style-type: none"> <li>● Src. Security Zone: trust</li> <li>● Src. Address: lan</li> <li>● Dest. Security Zone: untrust</li> <li>● Dest. Address: any</li> </ul>
Configure NAT.	Configure source NAT to allow the LAN user to normally access the Internet.	<ul style="list-style-type: none"> <li>● Src. Security Zone: trust</li> <li>● Src. Address: lan</li> <li>● Dest. Security Zone: untrust</li> <li>● Dest. Address: any</li> <li>● Src. Address Translated to: Outbound Interface Address</li> </ul>

### 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**.



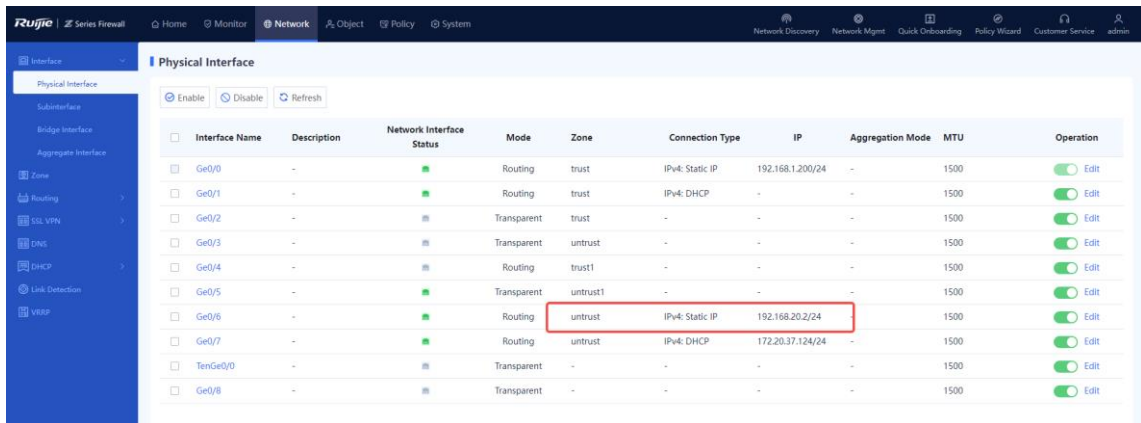
c Set parameters for the interface.

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**.

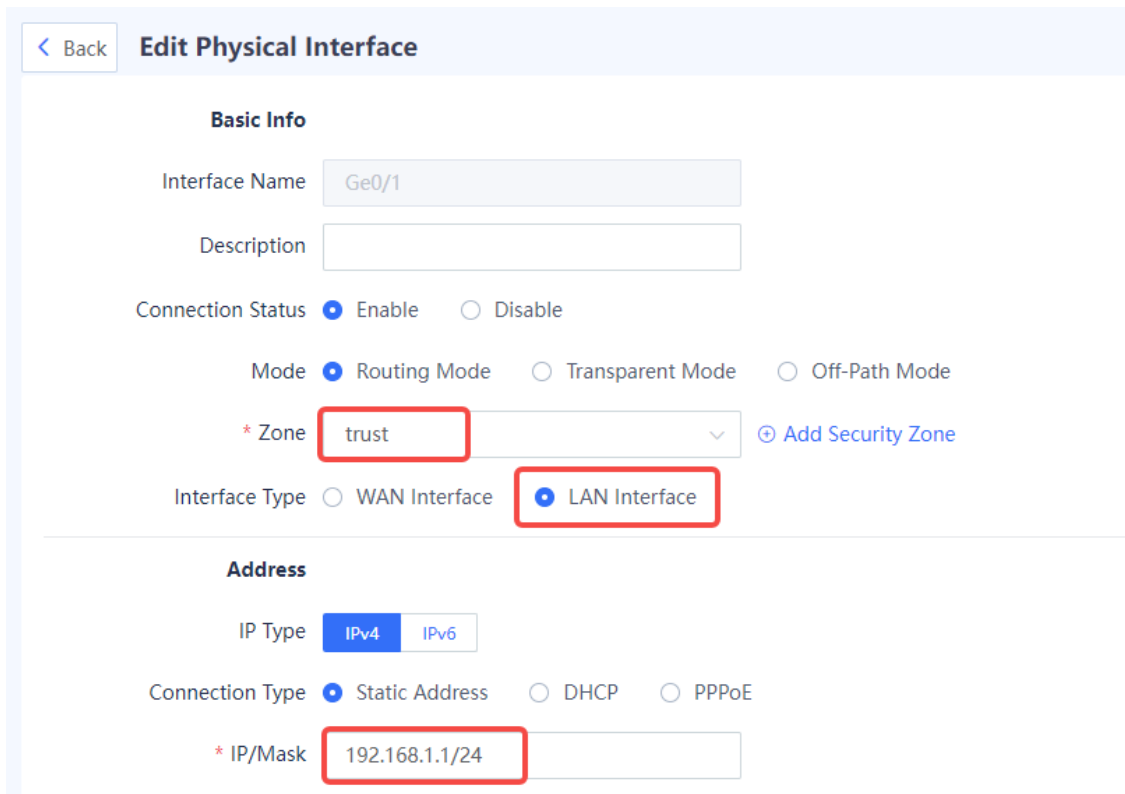
After successful configuration, interface information marked in the red block is displayed, as shown in the following figure.





(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**.



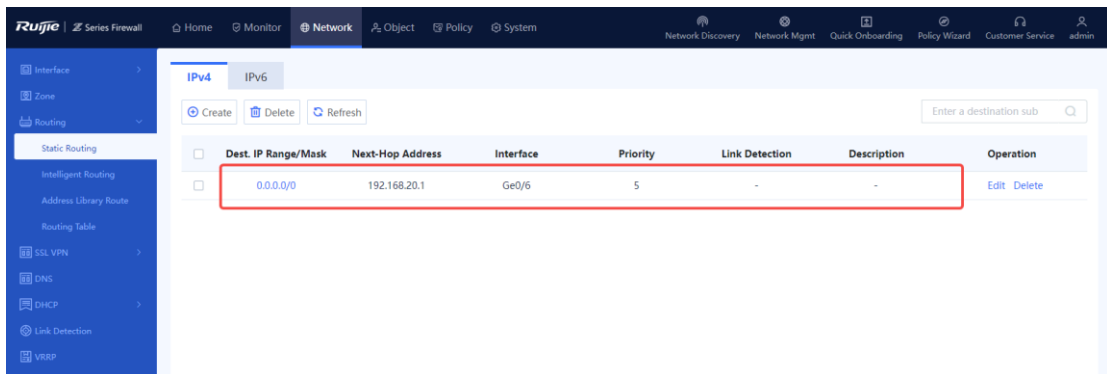
c Set parameters for the interface.

Item	Description
Mode	Routing Mode

Item	Description
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.



- (3) Configure address resources.
  - a Choose **Object > Address > IPv4 Address**.
  - b Click **Create** and add an address object with a LAN IP address.

The screenshot displays the Ruijie Series Firewall configuration interface. The top navigation bar includes 'Ruijie | Series Firewall' and tabs for 'Home', 'Monitor', 'Network', 'Object', 'Policy', and 'System'. The 'Object' tab is selected. On the left, a sidebar menu lists various configuration categories: Address, App, URL Category, Service, Time Plan, ISP Address Library, User Authentication, Certificate, Content Template, and Security Rule Base. The main content area is titled 'Add IPv4 Address Object' and contains two sections: 'Basic Info' and 'IP Address/Range'. In the 'Basic Info' section, the 'Name' field is set to 'lan' and the 'Description' field is empty. In the 'IP Address/Range' section, the 'IP Address/Range' field is set to '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

Enabled State  Enable  Disable

\* Policy Group  [⊕ Add Group](#)

\* Adjacent Policy

Description

---

**Src. and Dest.**

\* Src. Security Zone

\* Src. Address

\* Dest. Security Zone

\* Dest. Address

---

**Service**

Service

---

**App**

App

---

**Time Range**

Time Range  [⊕ 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](#)

---

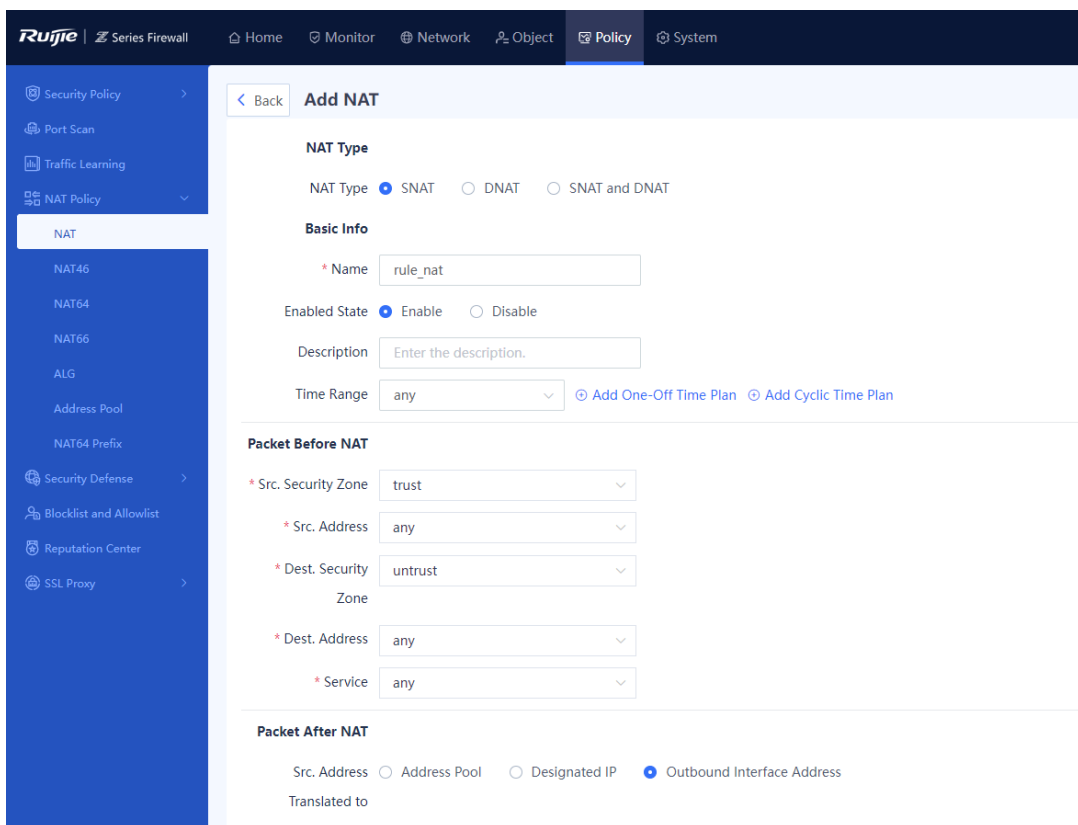
**Advanced**

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**.



- 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.)

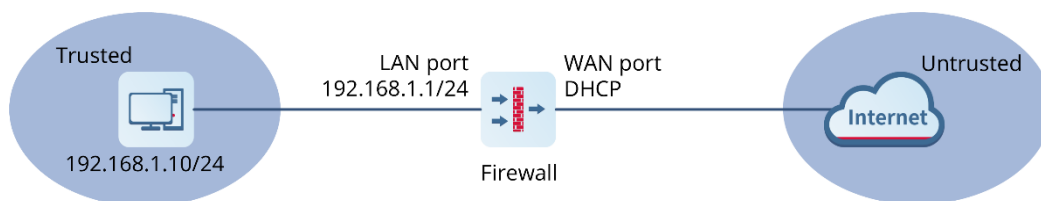
The PC can successfully ping the address 114.114.114.114.

## 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.	<p>Select two interfaces on the device and set the interface type to WAN interface and LAN interface respectively.</p> <ul style="list-style-type: none"> <li>● WAN interface: Used to connect to the Internet.</li> <li>● LAN interface: Used to connect to the LAN.</li> </ul>	<ul style="list-style-type: none"> <li>● WAN interface: Set <b>Connection Type</b> to <b>DHCP</b>. 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.</li> <li>● 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.</li> </ul>
Create an address object.	To facilitate management, configure the IP address of the LAN user as an address object.	Set the name to <b>lan</b> 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.	<ul style="list-style-type: none"> <li>● Src. Security Zone: trust</li> <li>● Src. Address: lan</li> <li>● Dest. Security Zone: untrust</li> <li>● Dest. Address: any</li> </ul>

### 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**.

The screenshot shows the 'Edit Physical Interface' configuration page. The page has a light blue header with a 'Back' button and the title 'Edit Physical Interface'. Below the header, there are several sections:

- Basic Info**:
  - Interface Name: Ge0/7
  - Description: (empty text box)
  - Connection Status:  Enable  Disable
  - Mode:  Routing Mode  Transparent Mode  Off-Path Mode
  - \* Zone: untrust (dropdown menu) [+ Add Security Zone](#)
  - Interface Type:  WAN Interface  LAN Interface
- Address**:
  - IP Type: IPv4 (selected) 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**

<input type="checkbox"/>	Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mode	MTU	Operation
<input type="checkbox"/>	Ge0/0	-		Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500	Edit
<input type="checkbox"/>	Ge0/1	-		Routing	trust	IPv4: DHCP	-	-	1500	Edit
<input type="checkbox"/>	Ge0/2	-		Transparent	trust	-	-	-	1500	Edit
<input type="checkbox"/>	Ge0/3	-		Transparent	untrust	-	-	-	1500	Edit
<input type="checkbox"/>	Ge0/4	-		Routing	trust1	-	-	-	1500	Edit
<input type="checkbox"/>	Ge0/5	-		Transparent	untrust1	-	-	-	1500	Edit
<input type="checkbox"/>	Ge0/6	-		Routing	trust	IPv4: Static IP	192.168.1.1/24	-	1500	Edit
<input type="checkbox"/>	Ge0/7	-		Routing	untrust	IPv4: DHCP	172.20.37.124/24	-	1500	Edit
<input type="checkbox"/>	TenGe0/0	-		Transparent	-	-	-	-	1500	Edit
<input type="checkbox"/>	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

Description

Connection Status  Enable  Disable

Mode  Routing Mode  Transparent Mode  Off-Path Mode

\* Zone  [+ Add Security Zone](#)

Interface Type  WAN Interface  LAN Interface

---

**Address**

IP Type

Connection Type  Static Address  DHCP  PPPoE

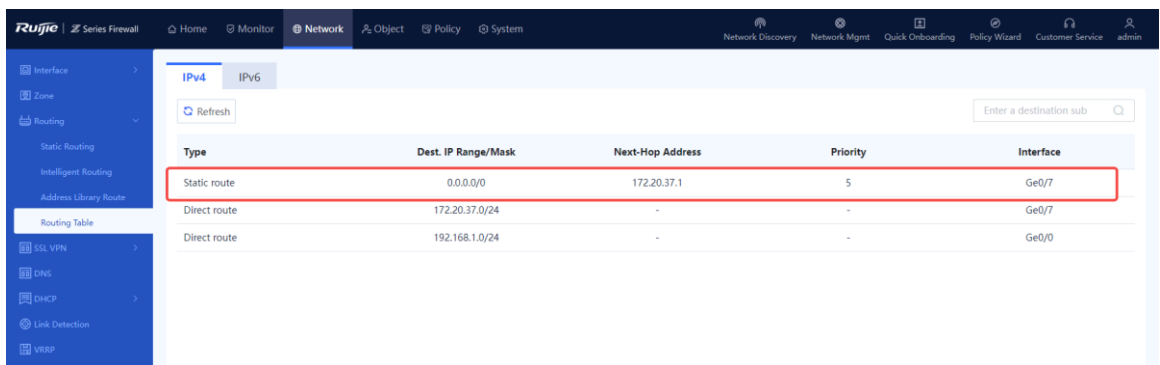
\* IP/Mask

- 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

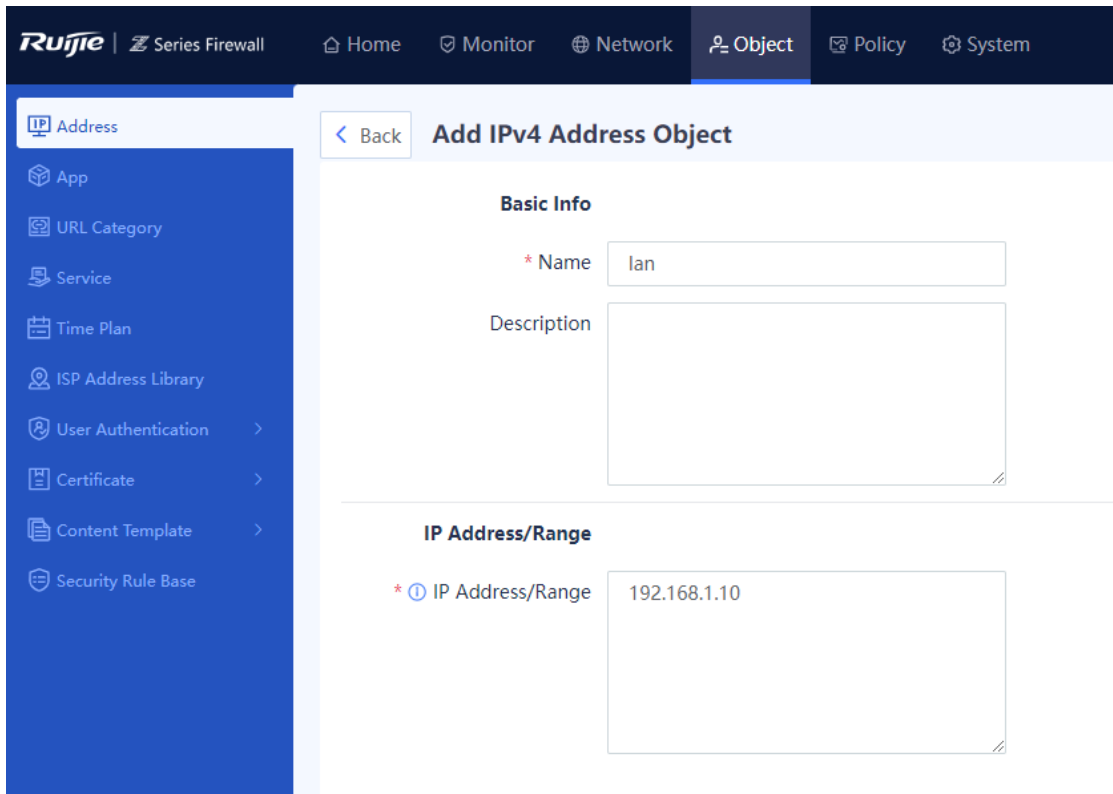
- d Enable management functions on the interface as required. You are advised to enable the HTTPS, ping, and SSH services only on the LAN interface.
- e Click **Save**.

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.

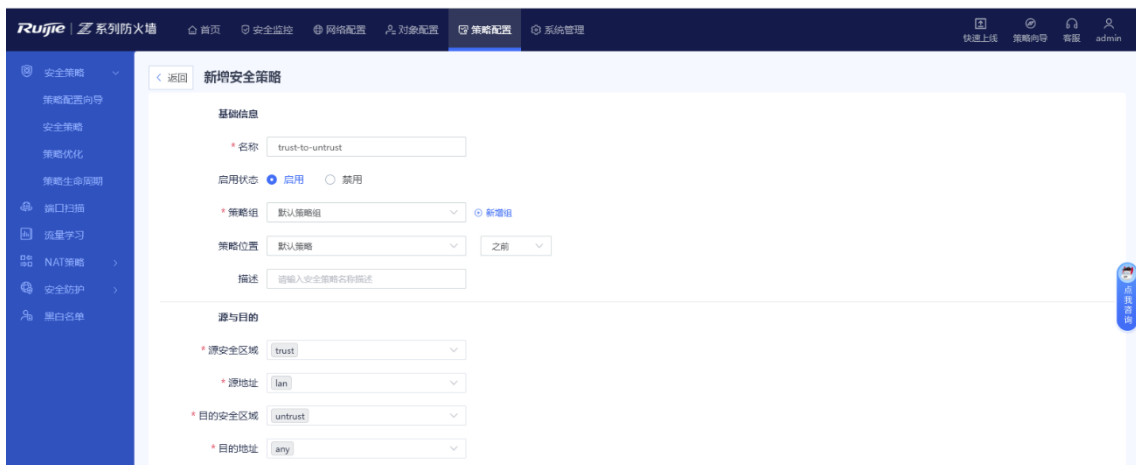


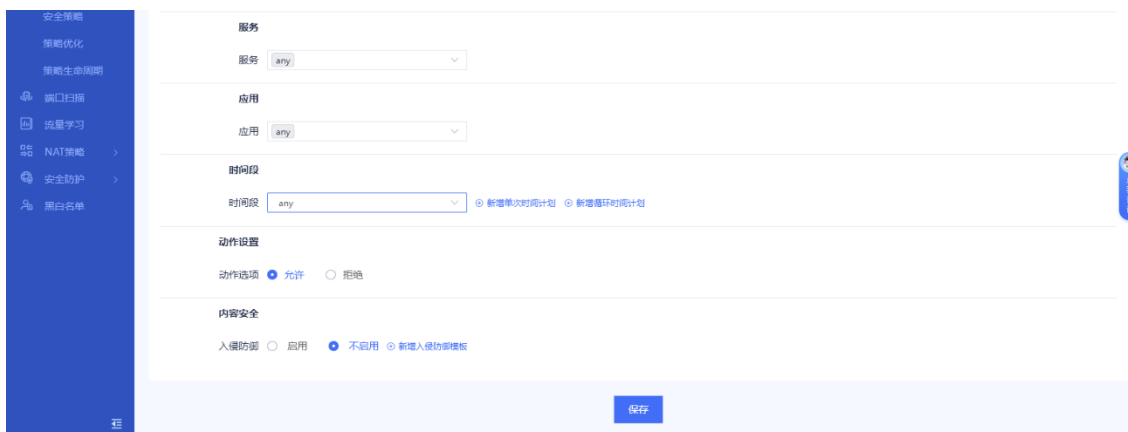
(3) Configure address resources.

- a Choose **Object > Address > IPv4 Address**.
- b Click **Create** and add an address object with a LAN IP address.



- 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**.





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**.

< Back
**Create Security Policy**

**Basic Info**

\* Name

Enabled State  Enable  Disable

\* Policy Group  [⊕ Add Group](#)

\* Adjacent Policy

Description

---

**Src. and Dest.**

\* Src. Security Zone

\* Src. Address

\* Dest. Security Zone

\* Dest. Address

---

**Service**

Service

---

**App**

App

---

**Time Range**

Time Range  [⊕ 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**

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	<a href="https://www.ruijienetworks.com/">https://www.ruijienetworks.com/</a> Choose <b>Support &gt; Download &gt; Reye</b> and find the latest version of the Z-S series firewall under RG-WALL 1600-Z-S series cloud management firewalls.
Web management	Choose <b>System &gt; System Maintenance &gt; System Upgrade &gt; Online Upgrade &gt; Recommended Version</b> to upgrade to the latest

Method	Path
page of the firewall	version (recommended) in online mode.
Ruijie Cloud	<p>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).</p> <p>Choose <b>Monitoring &gt; Device &gt; Firewall</b>, select a device, select a version, and click <b>Upgrade</b>.</p>

---

 **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**.

---

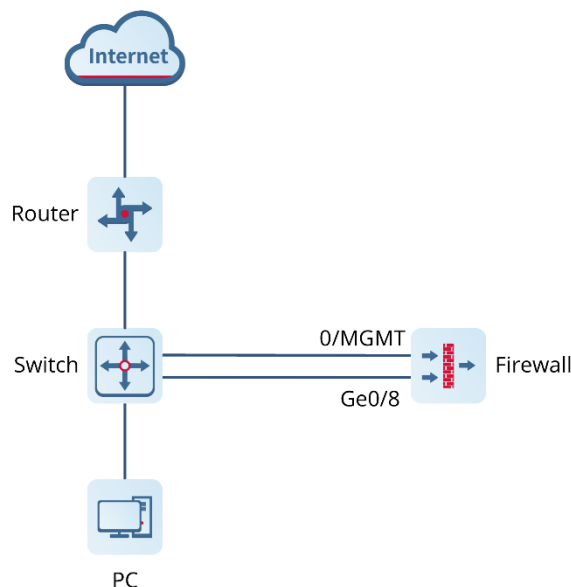
## 6.4.2 Deployment in Off-Path Mode (Quick Deployment)

### 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

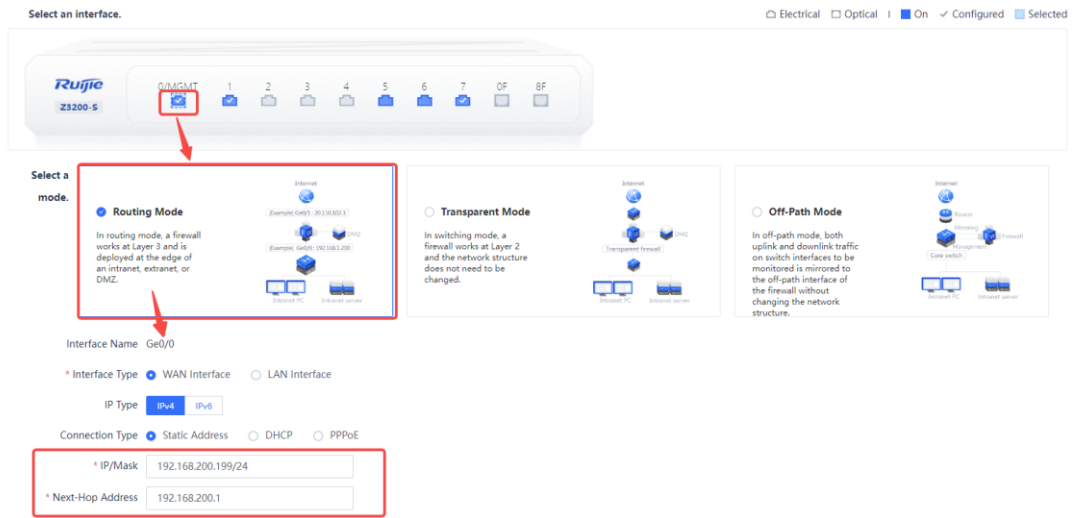
- (1) Implement quick onboarding. Select a deployment mode (off-path mode) and configure an off-path interface. Configure an IP address and the next hop for the management interface (0/MGMT) to ensure successful connection to the Internet.
- (2) (Optional) Check the connectivity. The system automatically 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

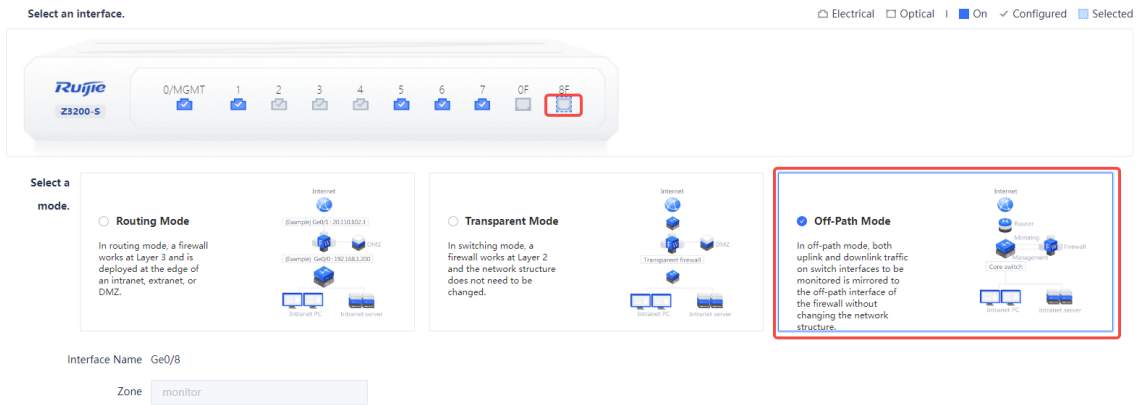
- (1) Implement quick onboarding.
  - a Configure interfaces.
    - o Configure an IP address and next hop for the 0/MGMT management interface (Ge0/0) and connect it to the network using an independent network cable to ensure that the management interface can access the Internet. (The IP addresses in this example are for



reference only.)



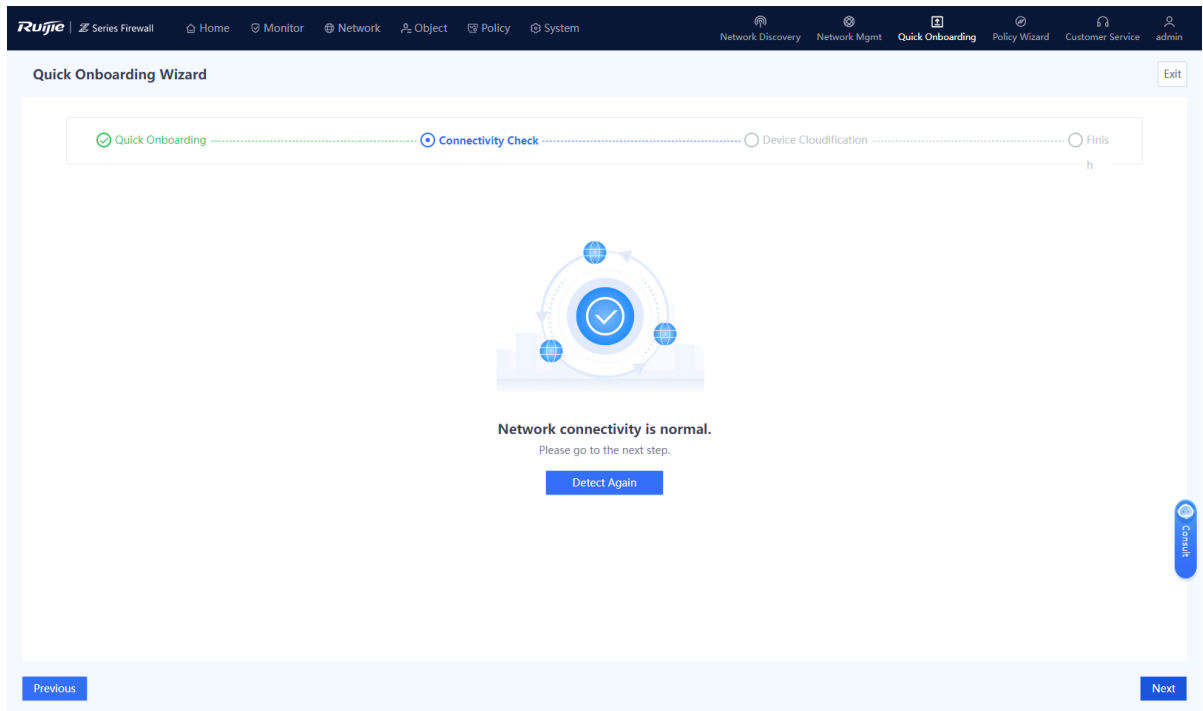
- o Configure another interface as the off-path interface. This example uses Ge0/8 as the off-path interface.



**Note**

The management interface cannot be set to the off-path mode.

- (2) (Optional) Check the connectivity.



### (3) Import licenses.

**License Config**

1. Before activating a device, register on and log in to Ruijie Secure Cloud Platform at <https://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

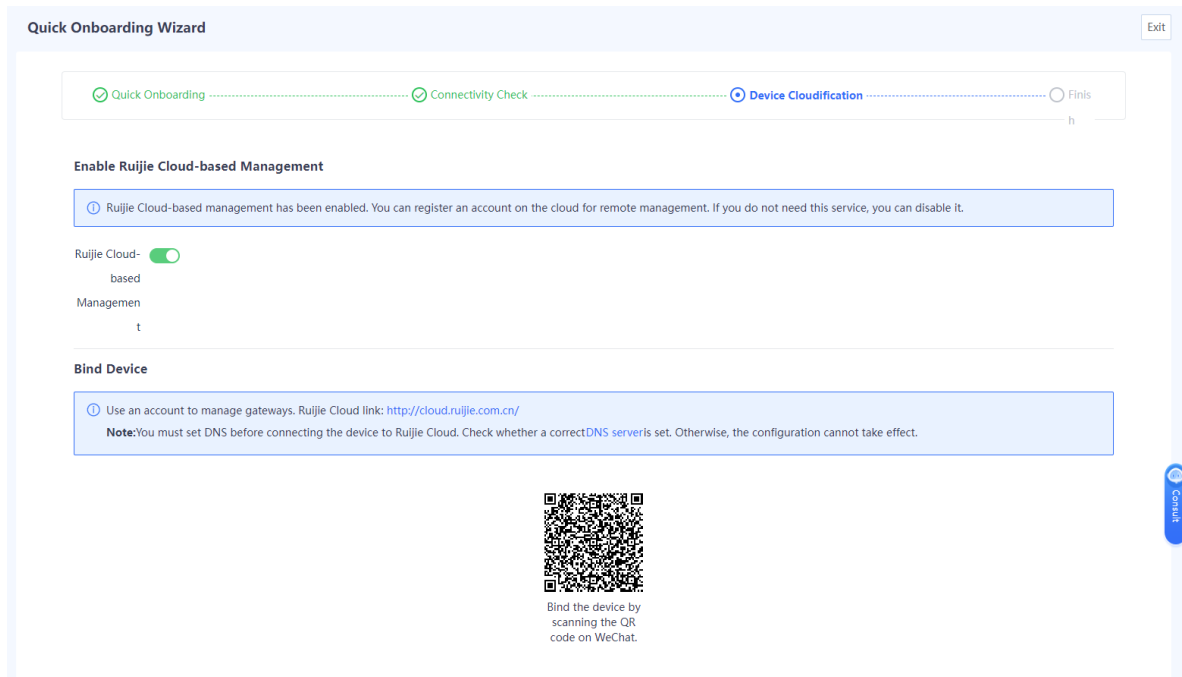
**Activate Now**

You can choose to perform manual activation.

**Activate Manually**

Device SN: **MACC932672666**

### (4) Complete the quick onboarding configuration and log in to Ruijie Cloud to implement remote O&M.



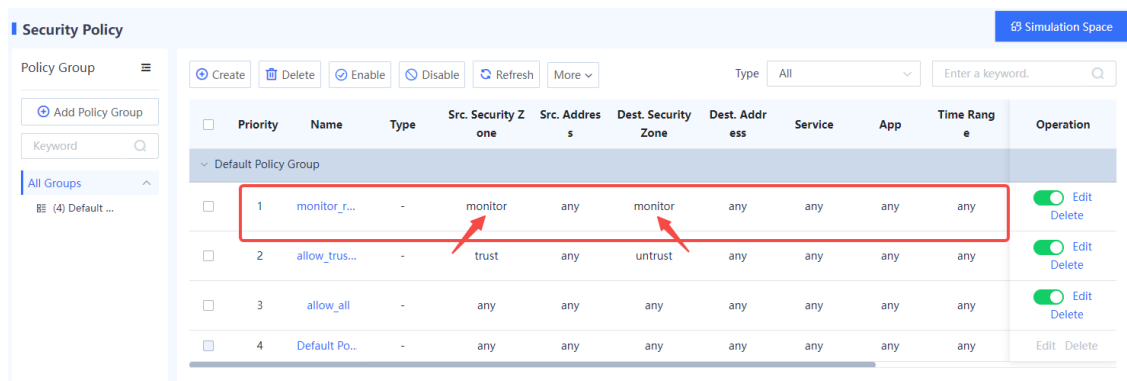
- (5) Configure the switch to mirror both uplink and downlink traffic on switch interfaces to be monitored to the off-path interface Ge0/8. (Omitted)

**Note**

There are slight differences in the configuration method of different switches. For details, see the product manual.

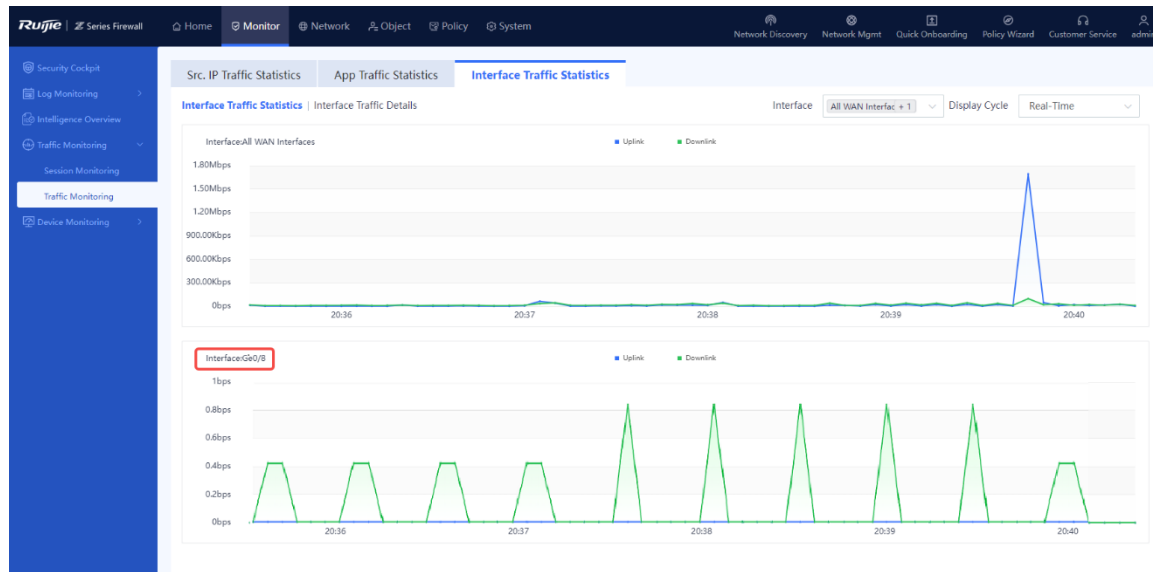
- (6) Create a security policy.

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**.



**Configuration Verification**

Choose **Monitor > Traffic Monitoring > Traffic Monitoring > Interface Traffic Statistics** and check whether there is traffic on the Ge0/8 port.



### 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**.

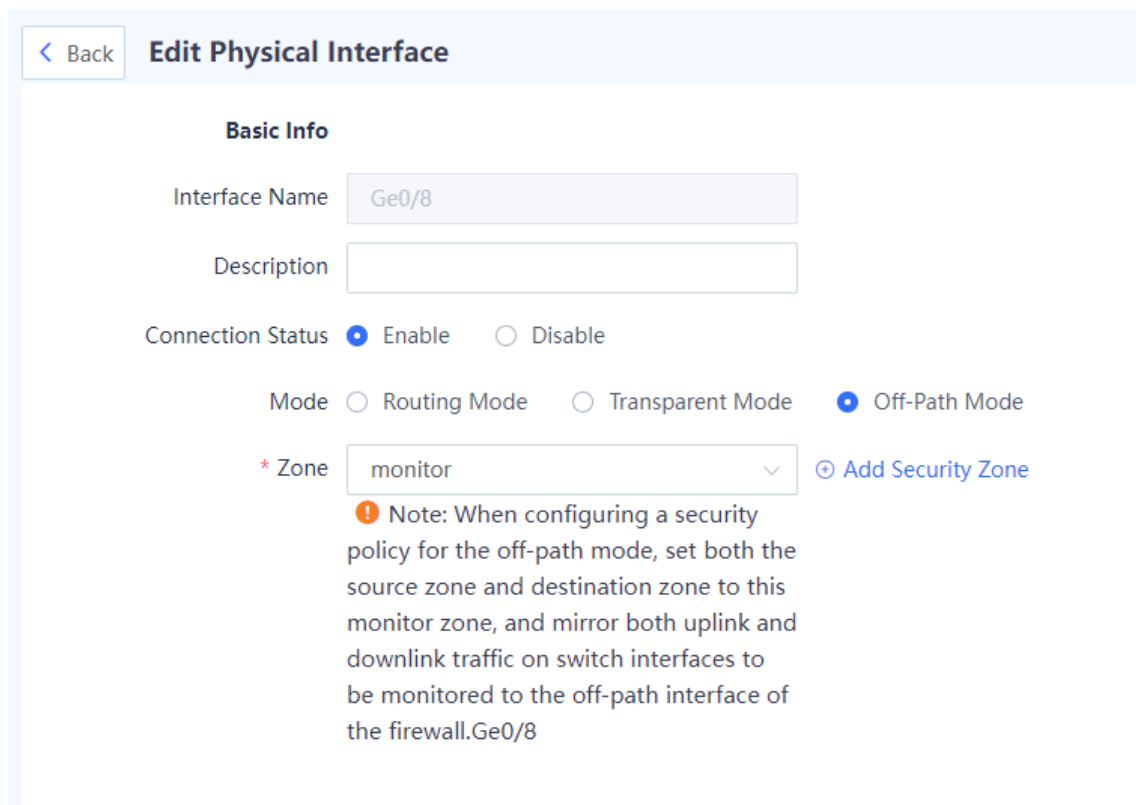
#### Procedure

- (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.

The screenshot shows the 'Physical Interface' configuration page in the Ruijie Series Firewall web interface. It features a table with columns for Interface Name, Description, Network Interface Status, Mode, Zone, Connection Type, IP, Aggregation Mode, MTU, and Operation. The 'Operation' column contains 'Edit' buttons for each interface. The 'Edit' button for the Ge0/8 interface is highlighted with a red box.

Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mode	MTU	Operation
<input type="checkbox"/> Ge0/0	-	<span style="color: green;">●</span>	Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500	<span style="color: green;">●</span> Edit
<input type="checkbox"/> Ge0/1	-	<span style="color: green;">●</span>	Routing	trust	IPv4: DHCP	-	-	1500	<span style="color: green;">●</span> Edit
<input type="checkbox"/> Ge0/2	-	<span style="color: grey;">●</span>	Transparent	trust	-	-	-	1500	<span style="color: green;">●</span> Edit
<input type="checkbox"/> Ge0/3	-	<span style="color: grey;">●</span>	Transparent	untrust	-	-	-	1500	<span style="color: green;">●</span> Edit
<input type="checkbox"/> Ge0/4	-	<span style="color: grey;">●</span>	Routing	trust1	-	-	-	1500	<span style="color: green;">●</span> Edit
<input type="checkbox"/> Ge0/5	-	<span style="color: green;">●</span>	Transparent	untrust1	-	-	-	1500	<span style="color: green;">●</span> Edit
<input type="checkbox"/> Ge0/6	-	<span style="color: green;">●</span>	Routing	trust	IPv4: Static IP	192.168.1.1/24	-	1500	<span style="color: green;">●</span> Edit
<input type="checkbox"/> Ge0/7	-	<span style="color: green;">●</span>	Routing	untrust	IPv4: DHCP	172.20.37.124/24	-	1500	<span style="color: green;">●</span> Edit
<input type="checkbox"/> TenGe0/0	-	<span style="color: grey;">●</span>	Transparent	-	-	-	-	1500	<span style="color: green;">●</span> Edit
<input type="checkbox"/> Ge0/8	-	<span style="color: grey;">●</span>	Transparent	-	-	-	-	1500	<span style="color: green;">●</span> Edit

- b Set **Mode** to **Off-Path Mode** and retain the default value **monitor** for **Zone**.

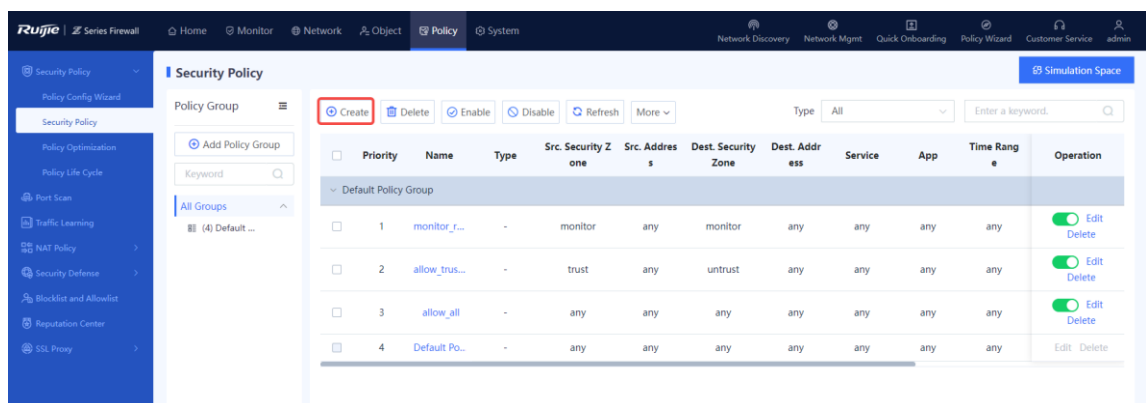


- c Click **Save**.

(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**.



- 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

**Simulation Space** Create

- 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

Enabled State  Enable  Disable

\* Policy Group  [Add Group](#)

\* Adjacent Policy

Description

---

**Src. and Dest.**

\* Src. Security Zone

\* Src. Address

\* Dest. Security Zone

\* Dest. Address

---

**Service**

Service

---

**App**

App

#### 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

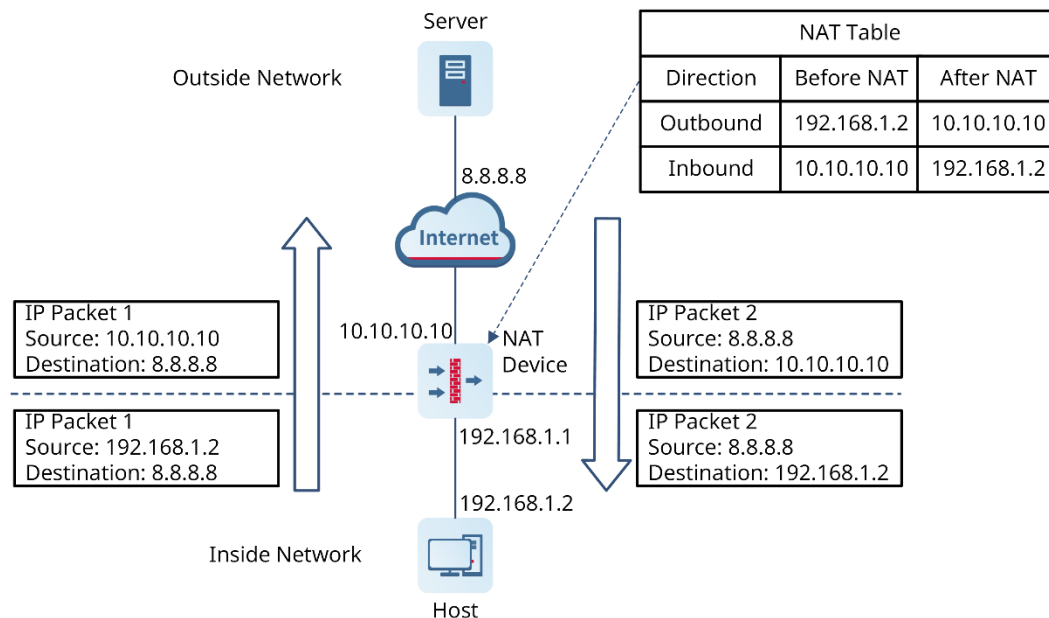
Network Address Translation (NAT) is to translate the source address (port) or destination address (port) in a packet into the desired address. NAT includes the following two steps:

- (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.



- (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.

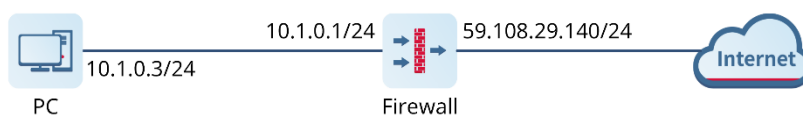
The Z-S series firewalls support multiple NAT modes to implement unidirectional and bidirectional translation between public IP addresses and private IP addresses. They are often used as specialized NAT devices. The NAT modes supported by Z-S series firewalls include:

- 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**



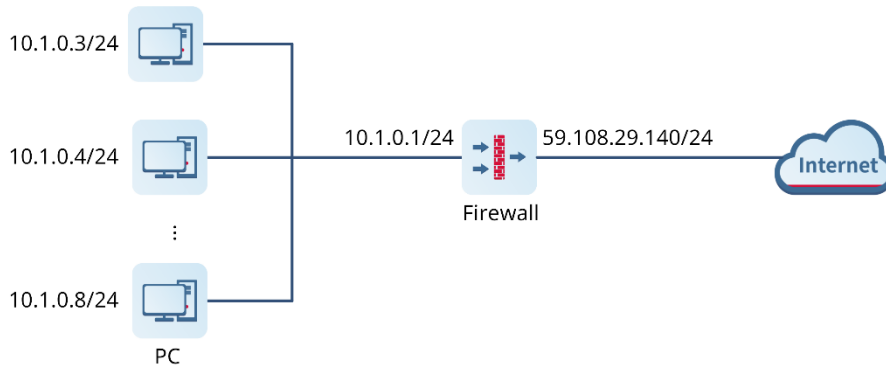
NAT Direction	Address Before NAT	Address After NAT
SNAT	10.1.0.3	59.108.29.187
DNAT	59.108.29.187	10.1.0.3

### 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**

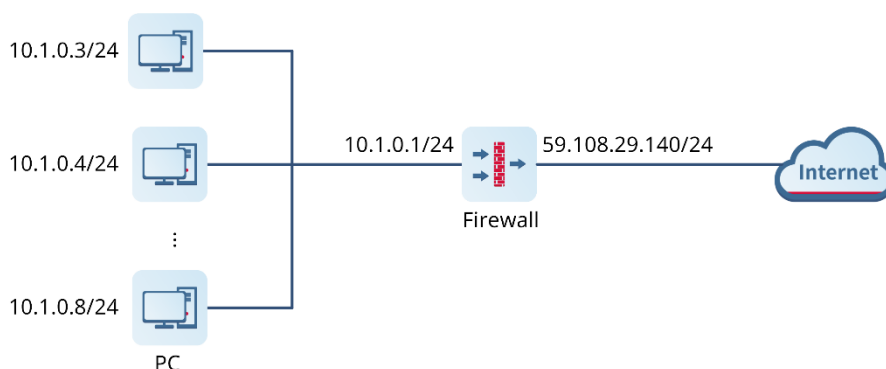


NAT Direction	Address Before NAT	Address After NAT
SNAT	10.1.0.3-10.1.0.8	59.108.29.90-59.108.29.99
DNAT	59.108.29.90-59.108.29.99	10.1.0.3-10.1.0.8

### 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 7-3PAT 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.

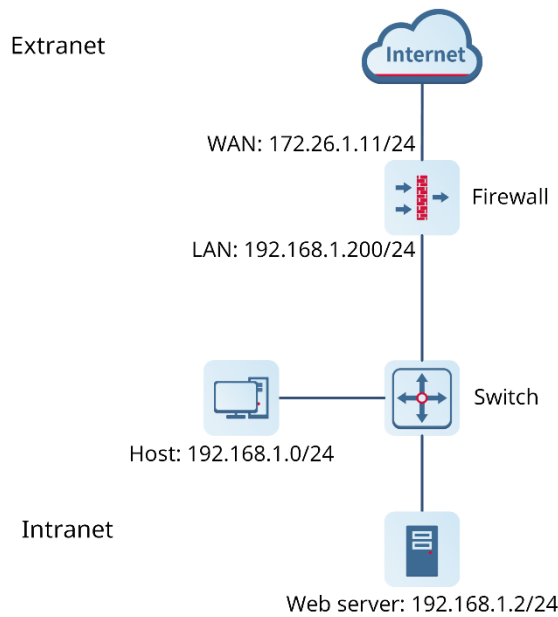
### 7.1.2 Configuring Destination Address Translation (One-to-One Port Mapping)

#### 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:

<input type="checkbox"/>	Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mode	MTU	Operation
<input type="checkbox"/>	Ge0/0	-	<span style="color: green;">■</span>	Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500	<span style="color: green;">●</span> Edit
<input type="checkbox"/>	Ge0/1	-	<span style="color: green;">■</span>	Routing	untrust	IPv4: DHCP	-	-	1500	<span style="color: green;">●</span> Edit

- (2) Configure the security policy.

For details, see [7.7 Traffic Control](#) Policy

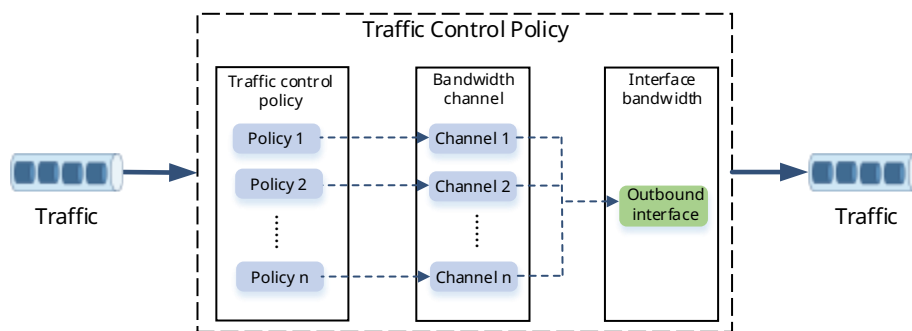
## 7.1.3 Overview

Traffic control enables a device to accurately manage and control user traffic based on source and destination addresses, services, applications, users and user groups. Different traffic control policies can be applied to different services to allocate egress bandwidth properly, thereby ensuring the normal running of key services.

As shown in the following figure, the device implements traffic control through traffic control policies, bandwidth channels, and line bandwidth (interface bandwidth).

- Traffic control policy: defines the matching conditions and processing actions for traffic, and references bandwidth channels.
- Bandwidth channel: specifies the uplink and downlink bandwidth resources to be referenced by traffic control policies.
- Line bandwidth: specifies the uplink and downlink bandwidth of the outbound interface.

The processing procedure of traffic control policies is as follows:

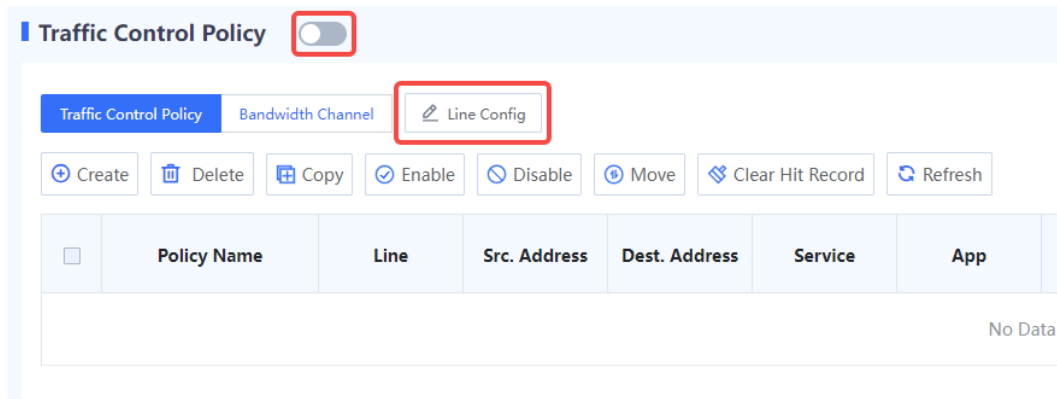


- (1) After a device receives traffic, the device matches the traffic against traffic control policies in the configured order until one policy is matched. If the traffic matches no policy, no traffic control action is performed.
- (2) The closer a policy is to the front, the higher its priority in matching. You can adjust the priority of a policy by moving its position.
- (3) If the traffic matches a policy, the device forwards the traffic based on the rate of the bandwidth channel referenced by the policy. If the actual traffic exceeds the maximum bandwidth set for the bandwidth channel, the excessive traffic is discarded.
- (4) When the traffic is sent out through the outbound interface, it is limited by the egress bandwidth. When traffic from multiple bandwidth channels is simultaneously forwarded by an interface and the actual traffic exceeds the interface bandwidth, the device forwards packets with higher priority first, such as packets configured with bandwidth guarantee. The device stores packets with lower priority in the buffer and sends them when the traffic is lower than the interface bandwidth limit. When the buffer is full, subsequent packets are discarded.

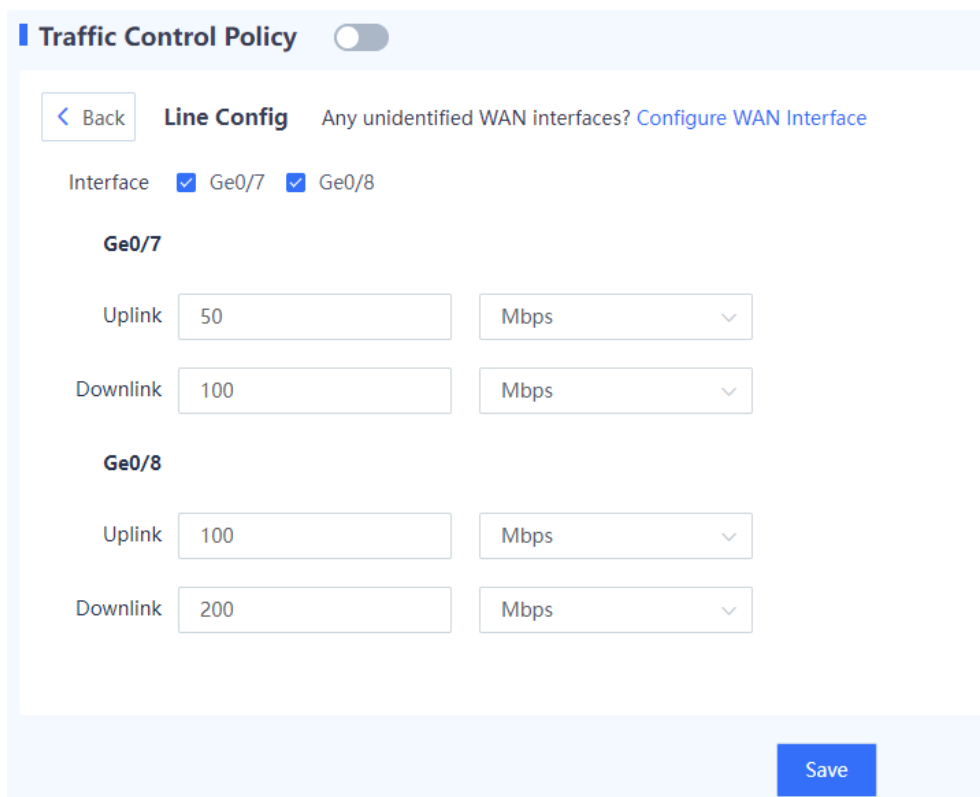
## 7.1.4 Configuring Traffic Control Policies

### 1. Configuring Egress Bandwidth

- (1) Choose **Policy > Traffic Control Policy**.
- (2) Toggle on  to enable traffic control.



(3) Select an outbound interface and configure uplink and downlink bandwidth limits.



**Note**

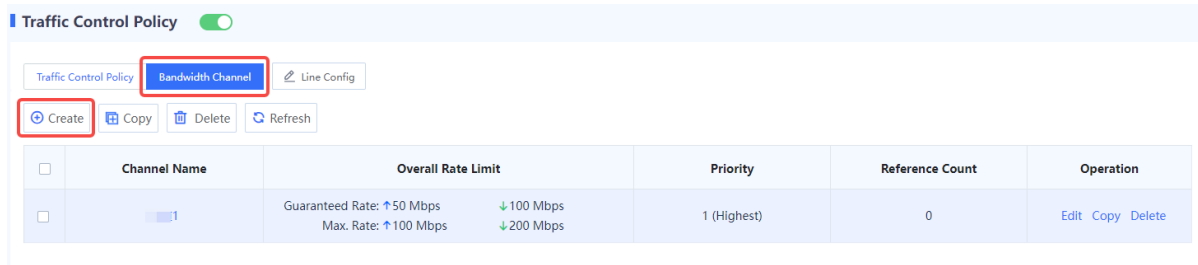
The outbound interface must be a WAN interface.

(4) Click **Save**.

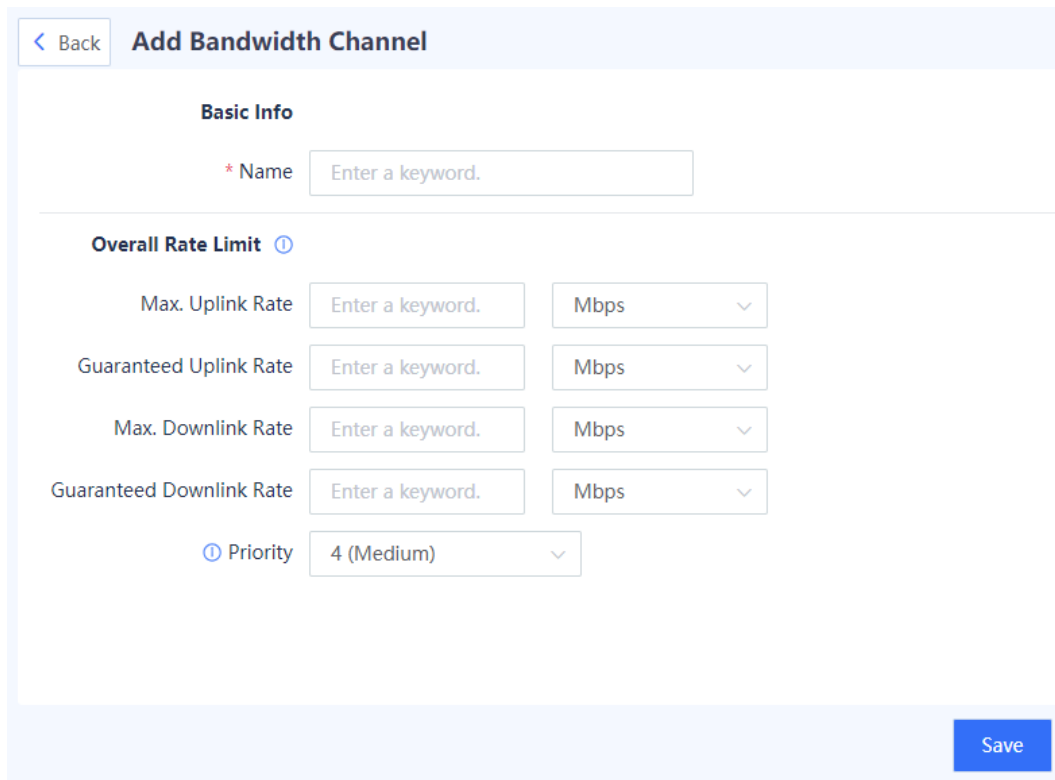
## 2. Configuring Bandwidth Channels

(1) Choose **Policy > Traffic Control Policy**.

(2) Click the Bandwidth Channel. Click Create.



(3) Enter bandwidth channel name, uplink and downlink bandwidth limits and channel priority.



Item	Description	Remarks
<b>Basic Info</b>		
Name	Bandwidth channel name.	[Example] Channel 1
<b>Overall Rate Limit</b>		
Max. Uplink Rate	The maximum bandwidth resource available to the traffic transmitted over the channel. The excessive traffic is discarded. If the parameter is not specified, the traffic is not limited.	[Example] 10 Mbps
Guaranteed Uplink Rate	The minimum bandwidth resource available to the traffic transmitted over the channel. If the	[Example]

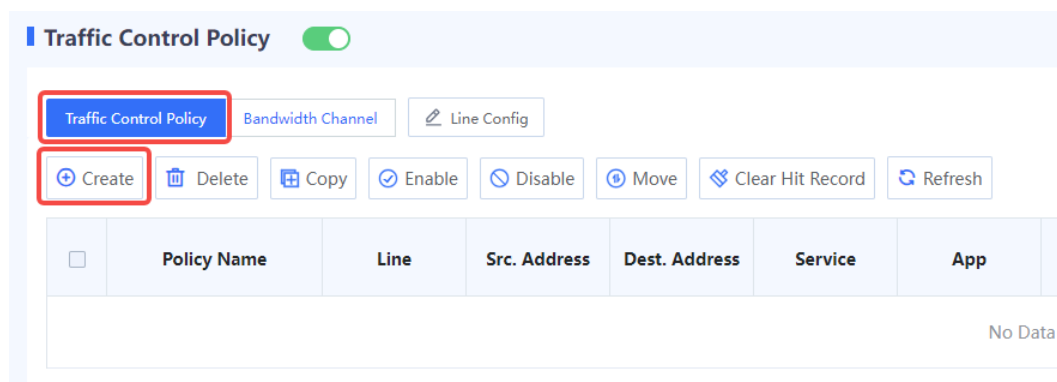
Item	Description	Remarks
	parameter is not specified, no bandwidth resource is guaranteed.	10 Mbps
Max. Downlink Rate	The maximum bandwidth resource available to the traffic transmitted over the channel. The excessive traffic is discarded. If the parameter is not specified, the traffic is not limited.	[Example] 10 Mbps
Guaranteed Downlink Rate	The minimum bandwidth resource available to the traffic transmitted over the channel. If the parameter is not specified, no bandwidth resource is guaranteed.	[Example] 10 Mbps
Priority	Bandwidth channel priority. When traffic from multiple bandwidth channels is simultaneously forwarded by an interface and traffic congestion occurs on the interface, the device forwards traffic from channels with higher priority first.	[Example] 1

(4) Click **Save**.

### 3. Configuring Traffic Control Policies

(1) Choose **Policy > Traffic Control Policy**.

(2) Click **Traffic Control Policy**. Click **Create**.



(3) Configure the following information for a traffic control policy.



< Back

## Add Traffic Control Policy

**Basic Info**

\* Name

Enabled State  Enable  Disable

---

**Line**

Line

---

**Src. and Dest.**

Src. Address

Dest. Address

---

**Services and Apps**

Service

App

---

**User/User Group**

User/User Group

---

**Action Execution**

Action  Limit  No Rate Limit  Block

\* Bandwidth  [⊕ Add Bandwidth Channel](#)

Channel

**Time Range**

Time Range  [⊕ Add One-Off Time Plan](#) [⊕ Add Cyclic Time Plan](#)

Item	Description	Remarks
<b>Basic Info</b>		
Name	Name of the traffic control policy	[Example] Policy_1
Enabled	Whether to enable the new traffic control policy	[Example] Enable

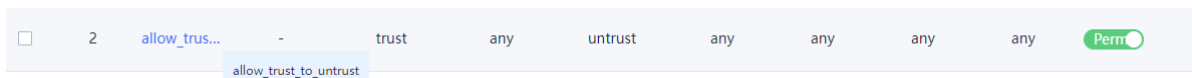
Item	Description	Remarks
State		
Line	Select the outbound interface to forward the traffic matching the policy.	[Example] Ge0/7
Policy position	Move the new policy above or below the specified policy. The closer a policy is to the front, the higher its priority in matching.	-
<b>Src. and Dest.</b>		
Src. Address	The packets with specified source IP addresses match the policy.	[Example] Any
Dest. Address	The packets with specified destination IP addresses match the policy.	[Example] Any
<b>Services and Apps</b>		
Service	The traffic of specified services matches the policy.	[Example] Any
App	The traffic of specified applications matches the policy.	[Example] Any
<b>User/User Group</b>		
User/User Group	The traffic of specified users or user groups matches the policy.	[Example] UserGroup_1
<b>Action Execution</b>		
Action	<p>The action the device performs for the traffic matching the policy.</p> <ul style="list-style-type: none"> <li>● Limit: The device forwards the packets based on the bandwidth limits configured for the selected bandwidth channel.</li> <li>● No Rate Limit: The device does not limit the traffic and forwards the packets.</li> <li>● Block: The device discards packets to block the service traffic.</li> </ul>	-

Item	Description	Remarks
<b>Time Range</b>		
Time Range	Effective time range.	[Example] Any

(4) Click **Save**.

DHCP Management.

The policy configuration is as follows:



(3) Configure port mapping.

- a Choose **Policy > NAT Policy > NAT**.
- b Above the operation area, click **Create**.

The system displays the **Add NAT** page.

< Back
**Add NAT**

**NAT Type**

NAT Type  SNAT  DNAT  SNAT and DNAT

**Basic Info**

\* Name

Enabled State  Enable  Disable

Description

Time Range  [⊕ Add One-Off Time Plan](#) [⊕ Add Cyclic Time Plan](#)

---

**Packet Before NAT**

\* Src. Security Zone

\* Src. Address

\* Dest. Address

\* Service

---

**Packet After NAT**

\* IP

ⓘ Port

Item	Description
Basic Info	
Name	WebServer
Enabled State	Enable
Packet Before NAT	
Src. Security Zone	untrust and trust
Src. Address	any
Dest. Address	WAN interface address: 172.26.1.116

Item	Description
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.

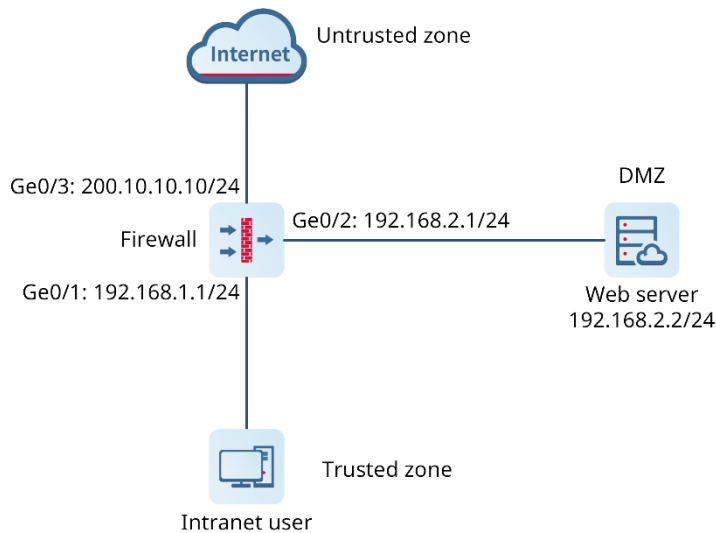
## 7.1.5 Configuring Bidirectional Address Translation (Allowing Intranet PCs to Access the Map Server by Using a Public Network Address)

### 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.

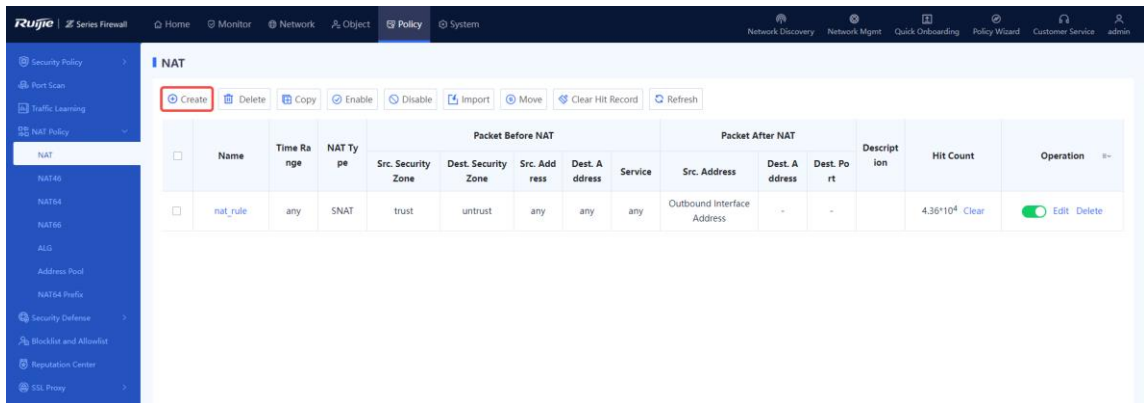
The policy configuration is as follows:

<input type="checkbox"/>	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														
<input type="checkbox"/>	1	permit_loca	IPv4	trust	lan_users	untrust	any	any	any	any	Permi		0	<a href="#">Edit</a> <a href="#">Delete</a>

- (3) Configure port mapping.

Configure the destination address translation policy for extranet users.

- a Choose **Policy > NAT Policy > NAT**.
- b Click **Create**.



c Set the parameters related to destination address translation.

< Back

## Add NAT

**NAT Type**

NAT Type  SNAT  DNAT  SNAT and DNAT

**Basic Info**

\* Name

Enabled State  Enable  Disable

Description

Time Range  [+ Add One-Off Time Plan](#) [+ Add Cyclic Time Plan](#)

**Packet Before NAT**

\* Src. Security Zone

\* Src. Address

\* Dest. Address

\* Service

**Packet After NAT**

\* IP

Port

Item	Description

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 <b>server_map</b> (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

Enabled State  Enable  Disable

Description

Time Range  [⊕ Add One-Off Time Plan](#) [⊕ Add Cyclic Time Plan](#)

---

**Packet Before NAT**

\* Src. Security Zone

\* Src. Address

\* Dest. Address

\* Service

---

**Packet After NAT**

Src. Address  Address Pool  Designated IP  Outbound Interface Address

Translated to

\* Designated IP

---

\* Dest. Address

Translated to

ⓘ Dest. Port

Number Translated to

Item	Description
Basic Info	
Name	rule_2
Enabled State	Enable
Packet Before NAT	
Src. Security Zone	trust

Item	Description
Src. Address	any
Dest. Address	Extranet port IP address of the firewall
Service	Create a customized service <b>server_map</b> (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.

## 7.1.6 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

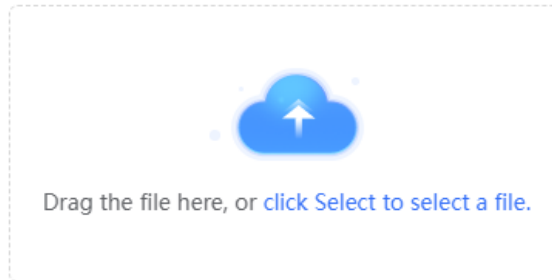
- (1) Choose **Policy > NAT Policy > NAT**.
- (2) In the operation area, click **Import**.

The system displays a tip.

**Tip**

**i** 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](#)



If imported configurations conflict with existing configurations,

Display Conflicting Data  Skip

OK

Cancel

- (3) Click **Download CSV Sample File** to download the configuration file template and fill in the configuration information.

**i 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.

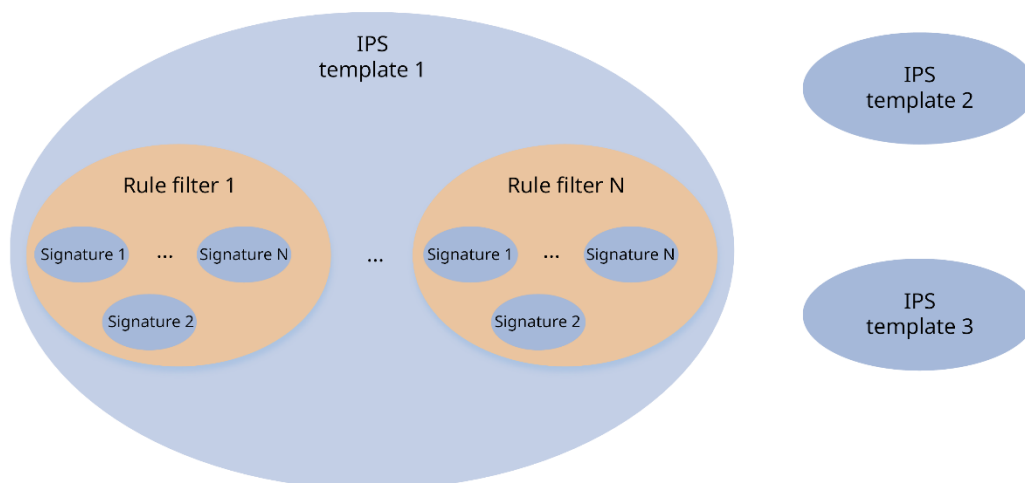
The IPS function of Z-S series firewalls is implemented using templates. Different templates can correspond to different signatures. You can customize the templates according to your needs. In addition, the device is delivered with a built-in "predefined template" that has been strictly verified.

- 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**

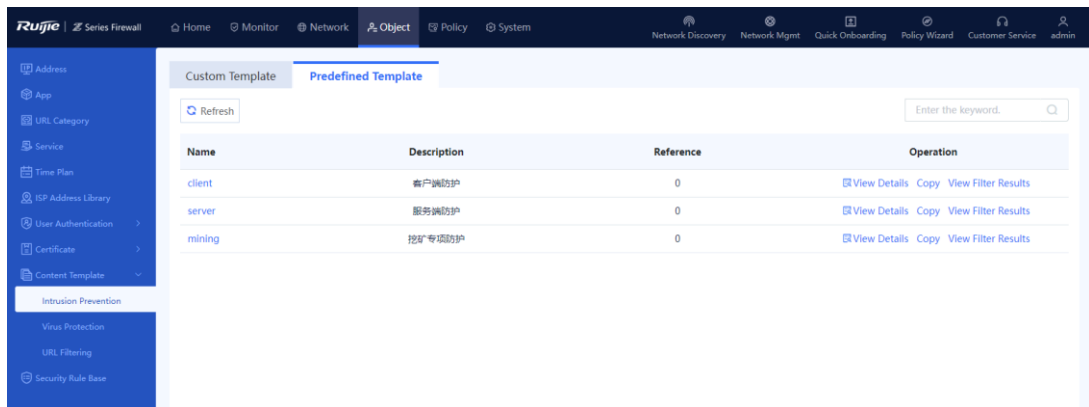


IPS supports multiple templates. An IPS template supports multiple rule filters. Each rule filter supports multiple signatures.

- 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.



- 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.)**



## 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

**Virus Protection  Enable  Not Enabled default Action: Block**

URL Filtering  Enable  Not Enabled



## 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:

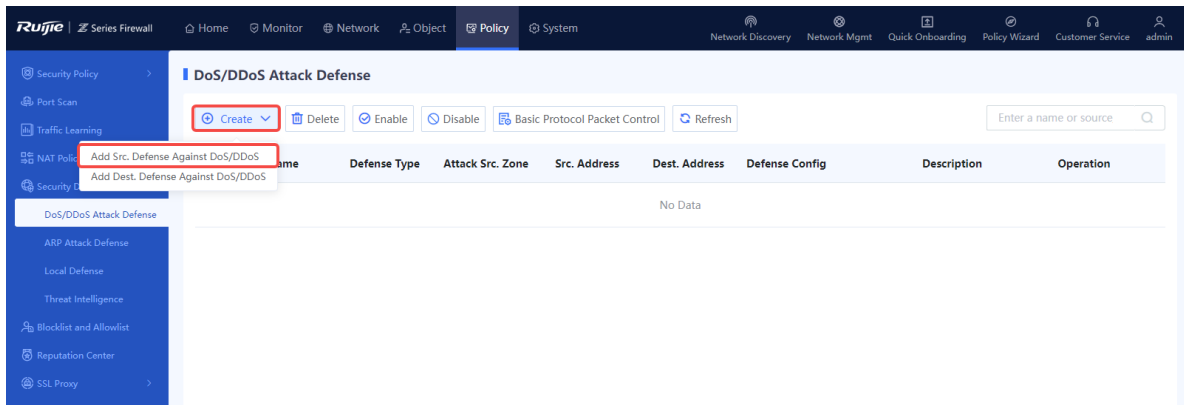
- Threat intelligence signature library: Contains a large amount of threat signature data and can be upgraded to obtain the latest data. After the TI authorization is activated, the firewall can perform security detection based on the threat intelligence signature library to enhance the capability of 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**.



(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.

[Back](#) **Add Src. Defense Against DoS/DDoS**

**Basic Info**

\* Name

Enabled State  Enable  Disable

Description

---

**Protected Host Range**

\* Attack Src. Zone  [Add Security Zone](#)

\* Src. Address

\* Dest. 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

Filtering out IPv6 Packets with Specific EHS

[Save](#)

(3) Set the parameters related to DoS/DDoS attack defense policy.

Item	Description	Remarks
Basic Info		

Item	Description	Remarks
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 defense policy.	Characters such as `~!#%^&*+\\{ };:'"/<>? are not 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.	<b>any</b> indicates all addresses. [Example] any
Dest. Address	The policy checks the traffic to this address set.	<b>any</b> indicates all addresses. [Example] any
Defense Config		
Scan Attack Types		
IP Scan	Whether IP scan defense is enabled.	[Example]

Item	Description	Remarks
Defense		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 <b>SYN Flood Attack Defense</b> .
Src. IP Blocking Limit (pps)	Global trigger threshold of flood attack defense.	[Example] 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: <b>Log</b> : Only record a security log, but not	[Example] Select <b>Log</b> and <b>Block</b> .

Item	Description	Remarks
	block traffic. <b>Block:</b> Only block traffic, but not record a security log.	
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.

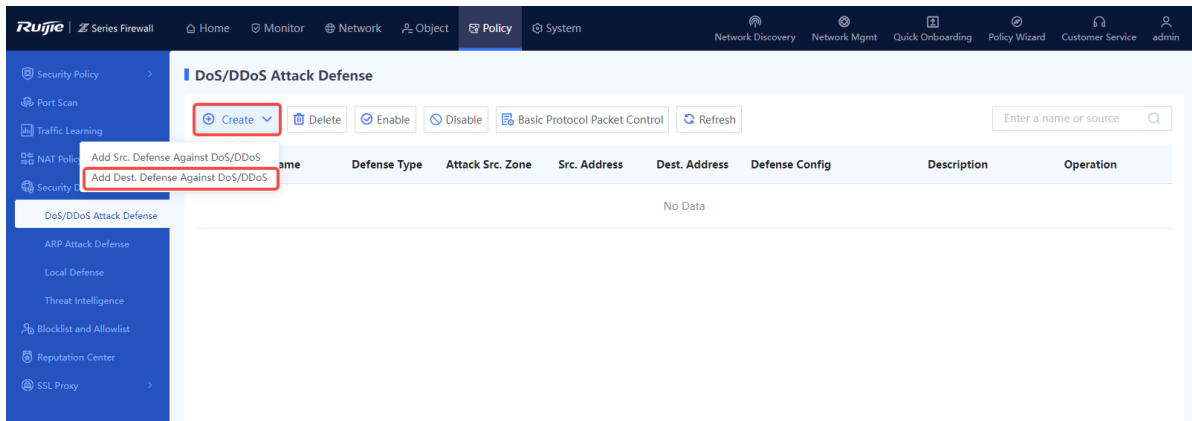
#### Follow-up Procedure

- 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.

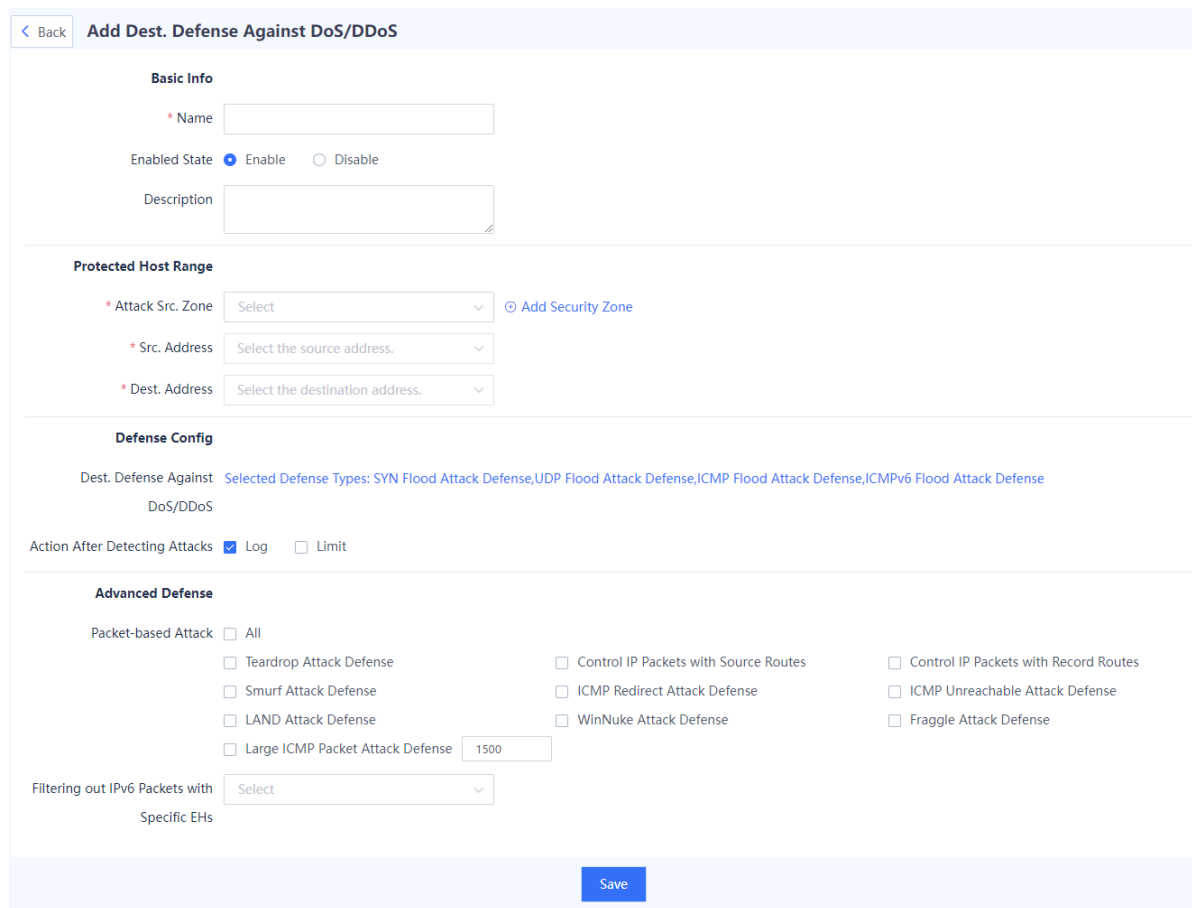
## 2. Configuring Destination Defense Against DoS/DDoS

#### 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.



(3) Set the parameters related to DoS/DDoS attack defense policy.

Item	Description	Remarks
Basic Info		

Item	Description	Remarks
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 defense policy.	Characters such as `~!#%^&*+\\ {};:'"/<>? are not allowed. [Example] New policy
<p>Protected Host Range</p> <p>Range of the attack source associated with the policy. The policy takes effect when matching.</p>		
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.	<p><b>any</b> indicates all addresses.</p> [Example] any
Dest. Address	The policy checks the traffic to this address set.	<p><b>any</b> indicates all addresses.</p> [Example] any
<p>Defense Config</p>		
<p>Dest. Defense Against DoS/DDoS</p>		
Attack defense type.	Defense against SYN flood, UDP flood, ICMP flood, and ICMPv6 flood.	Click an attack defense type to enable defense against the

Item	Description	Remarks
		specific attacks. [Example] Select <b>SYN Flood Attack Defense</b> .
Dest. IP Rate Limit (pps)	Global trigger threshold of flood attack defense.	[Example] 10000
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: <b>Log:</b> Only record a security log, but not limit the traffic rate. <b>Limit:</b> Only limit the traffic rate, but not record a security log.	[Example] Select <b>Log</b> and <b>Limit</b> .
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

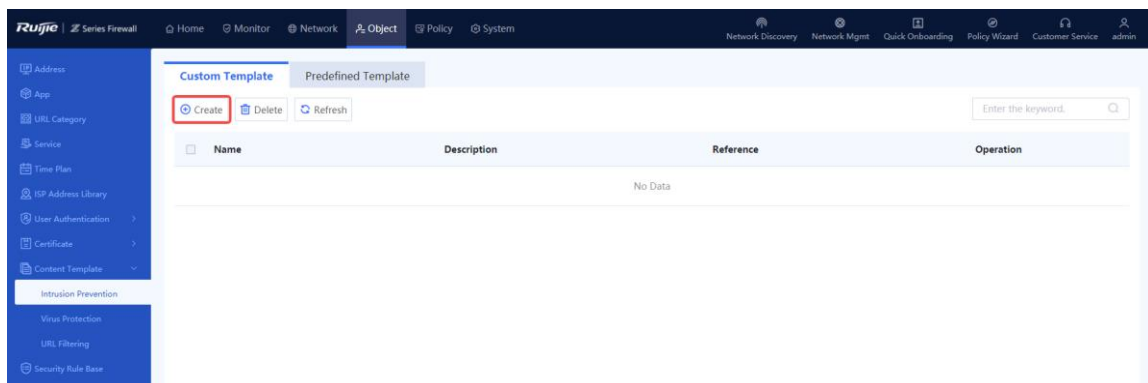
By performing in-depth detection on the traffic passing the firewall in real time, IPS can report alarms and block traffic in real time to protect user hosts from malicious traffic.

### 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.



< Back
**Add Intrusion Prevention Template**

**Basic Info**

\* Template Name

Description

---

**\* Rule Filter**

Create
 Delete

<input type="checkbox"/>	Name	Object	Severity	Protocol	Threat Type	Operation
No Data						

共 0 条

[Advanced Settings](#)

Save

(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**.

< Back
**Add Intrusion Prevention Template**

**Basic Info**

\* Template Name

Description

---

**\* Rule Filter**

Create
 Delete

<input type="checkbox"/>	Name	Object	Severity	Protocol	Threat Type	Operation
No Data						

共 0 条

[Advanced Settings](#)

Save

**Add Rule Filter**
⊗

---

\* Name

\* Object  All  Server  Client

\* Severity  All  High  Medium  Low  Tip

Protocol  To-be-selected (5)  Select All

- DNS
- HTTP
- TCP
- TLS
- UDP

Selected (0) Clear

Threat Type  To-be-selected (93)  Select All

- ▶  Brute Force
- ▶  DDOS
- ▶  Deserialization
- ▶  Event Monitor
- ▶  Information Leakage
- ▶  Injection Attack

Selected (0) Clear

- o **Name:** Customized. You are advised to configure a name that can describe the filter function.
  - o **Object:** Objects to be protected.
  - o **Severity:** Defense severity. For example, if only **High** is selected, only the security rules with high severity can hit the filter.
  - o **Protocol:** Protocols to be detected. The protocol traffic that is not specified does not hit the filter.
  - o **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...	<input checked="" type="radio"/> Block <input type="radio"/> Alert <input type="radio"/> Permit <input type="radio"/> Default Signature Action	<span>Clear</span>

- 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

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.

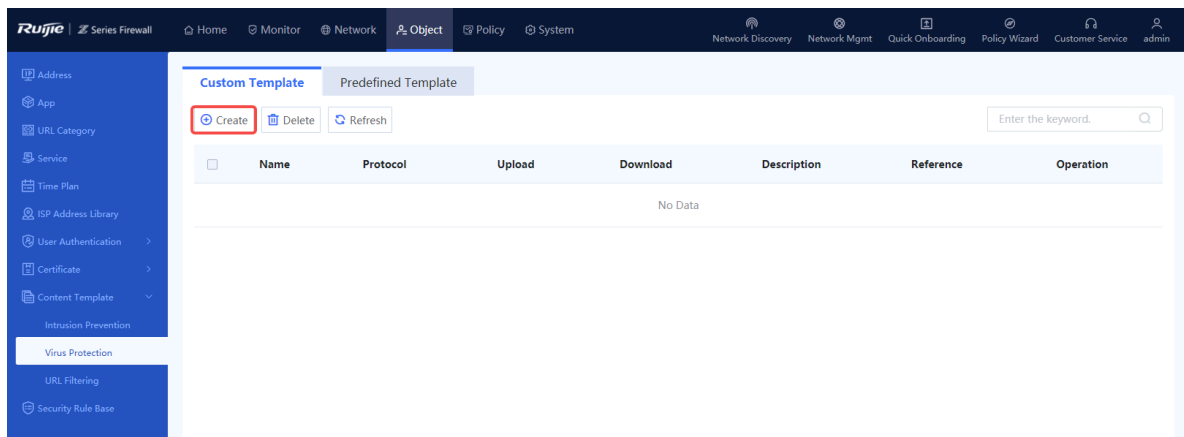
**Configuration Points**

- (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**.



[← Back](#)

## Add Virus Protection Template

**Basic Info**

\* Template Name

Description

---

**Scan Mode**

Scan Mode  Quick Scan  Deep Scan

Protocol

Protocol Type	Upload	Download
FTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HTTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
POP3	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SMTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>

---

[☰ Advanced Settings](#)

- **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  Action:  [+ Add Virus Protection Template](#)

URL Filtering  Enable  Not Enabled [+ Add URL Filtering](#)

## 7.2.5 ARP Attack Defense

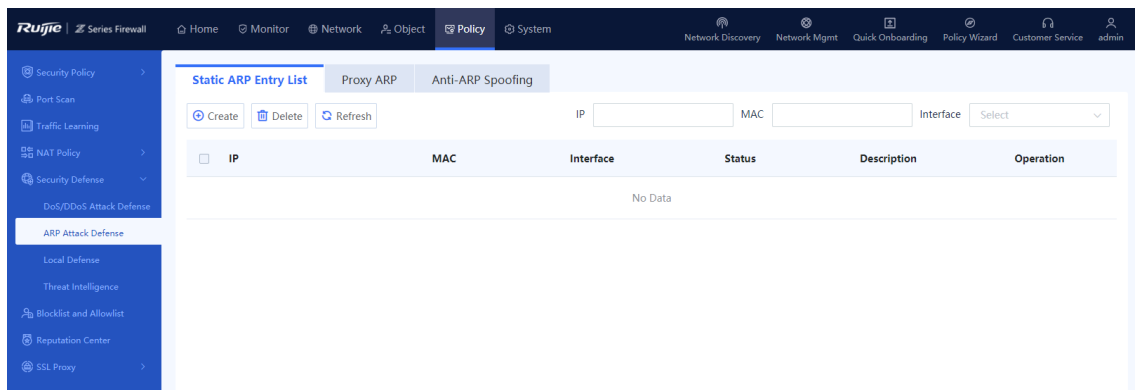
### 1. Configuring Static ARP

#### 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**.



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.

< Back Add ARP

\* IP

\* MAC

Auto MAC Obtaining

\* Interface

Auto Interface Discovery

Description

(3) Configure the basic information of the static ARP entry.

Item	Description	Remarks
IP	IP address to be bound to the static ARP entry.	<p>[Example]</p> <p>192.168.10.3</p>
MAC	MAC address to be bound to the static ARP entry.	<p>Two configuration methods are supported:</p> <ul style="list-style-type: none"> <li>● Fill in the information manually.</li> <li>● Click <b>Auto MAC Obtaining</b>. 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."</li> </ul> <p>[Example]</p> <p>11:22:33:44:55:66</p>
Interface	Physical interface to be bound.	<p>Two configuration methods are supported:</p> <ul style="list-style-type: none"> <li>● Fill in the information manually.</li> <li>● Click <b>Auto Interface Discovery</b>. 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."</li> </ul> <p>[Example]</p> <p>Ge0/1</p>



(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.

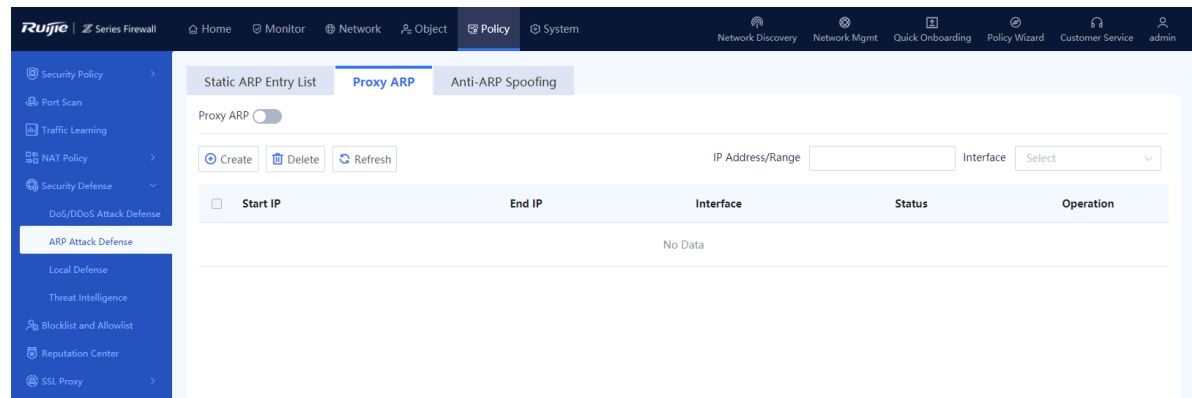
## 2. Configuring Proxy ARP

### 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**.



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**.



(3) Click **Create**.

The system displays the **Create Proxy ARP** page.

(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**.

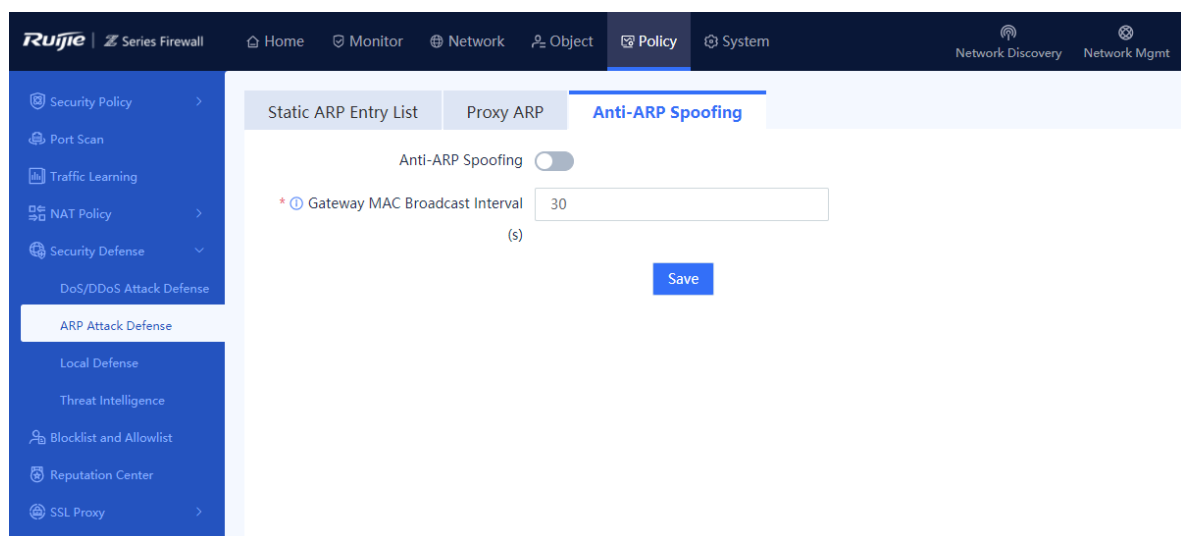
## 3. Configuring Anti-ARP Spoofing

### 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**.



(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

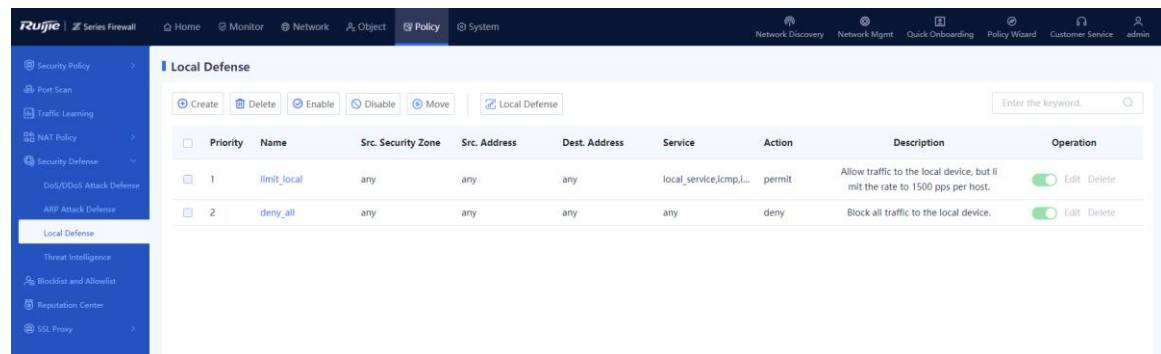
### Application Scenario

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.

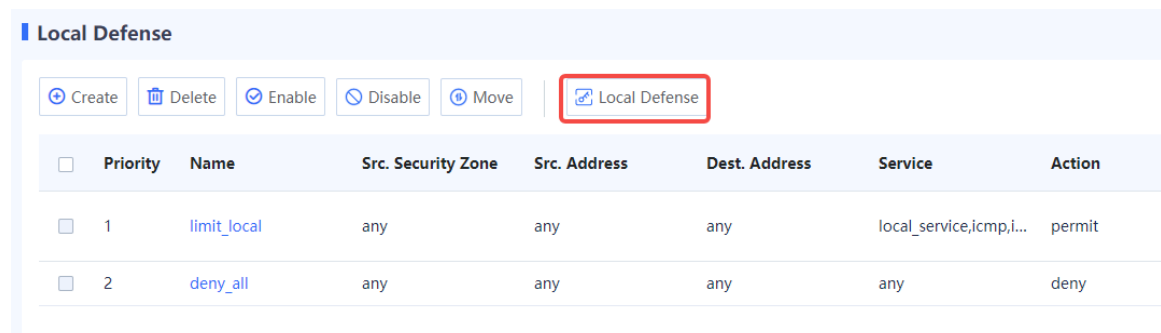
The local defense function has two default policies that cannot be modified to ensure that the device is protected from traffic attacks after this function is delivered.

### Procedure

- (1) Choose **Policy > Security Defense > Local Defense**.



- (2) Click **Local Defense**. Toggle on **Enable Local Defense** and click **Confirm**.



## Local Defense



**i** When local defense is disabled, access management cannot be configured, and existing configurations become invalid. Please operate with caution.

Enable Local Defense

Confirm

Cancel

(3) Click **Create** to enter the **Create Local Defense Policy** page.

[Back](#) **Create Local Defense Policy**

**Basic Info**

\* Name

Enabled State  Enable  Disable

Adjacent Policy

Description

---

**Src. and Dest.**

Src. Security Zone  [Add Security Zone](#)

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
- TrafficLearn... 172.20.37.114
- PortScan\_de... 172.20.37.54

[Add Address](#) [Add Address Group](#)

Selected (1) [Clear](#)

any [Remove](#)

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
- TrafficLearn... 172.20.37.114

[Add Address](#) [Add Address Group](#)

**Service**

**Service**

Service

To-be-selected (78)

Select

Service/Group Name	Protocol /Service	Dest. Port
<input checked="" type="checkbox"/> any		
<input type="checkbox"/> service_22_T...	TCP	22
<input type="checkbox"/> service_443_...	TCP	443
<input type="checkbox"/> service_2048...	TCP	2048
<input type="checkbox"/> service_2009...	TCP	20099

[Add Service](#) [Add Service Group](#)

Selected (1) [Clear](#)

any [✕](#)

**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.	<b>any</b> indicates traffic of all zones. [Example] any
Src. Address	The policy checks the traffic from this address set.	<b>any</b> indicates all addresses. [Example] any
Dest. Address	The policy checks the traffic to this address set.	<b>any</b> indicates all addresses. [Example] any

Service	The policy checks the traffic of this service.	<b>any</b> 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. <ul style="list-style-type: none"> <li>● <b>Disable</b>: not restricted</li> <li>● <b>Enable</b>: restricted. The <b>Packets Allowed to Pass Through Each Host (pps)</b> field needs to be set.</li> </ul>	[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.

---

#### **Note**

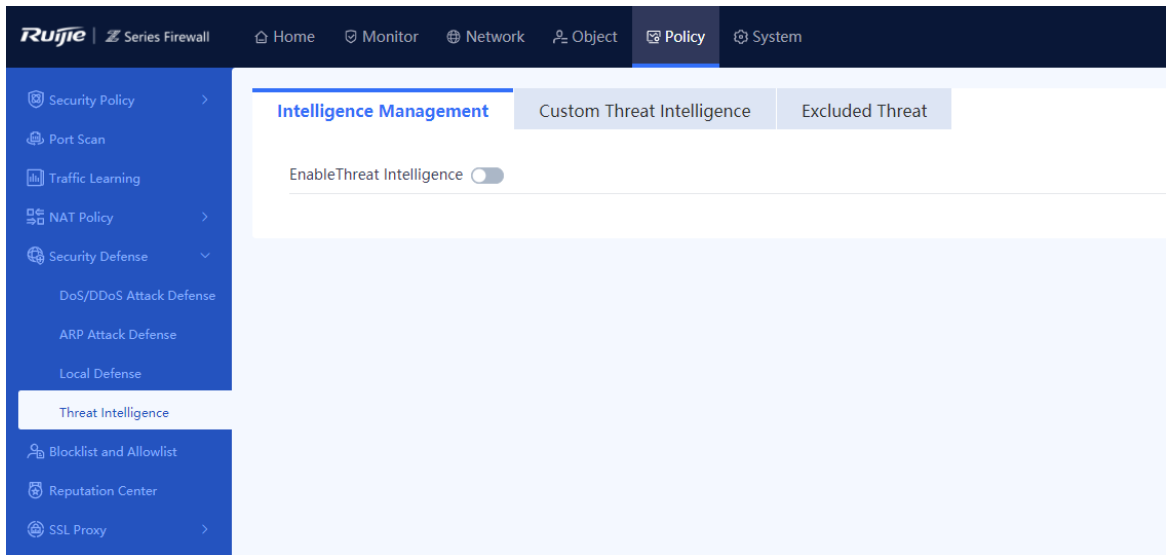
If the TI function is not authorized or authorization expires, the detection based on threat intelligence signature library is unavailable, and only the custom TI configured manually can be used. In this case, the threat intelligence signature library cannot be upgraded.

---

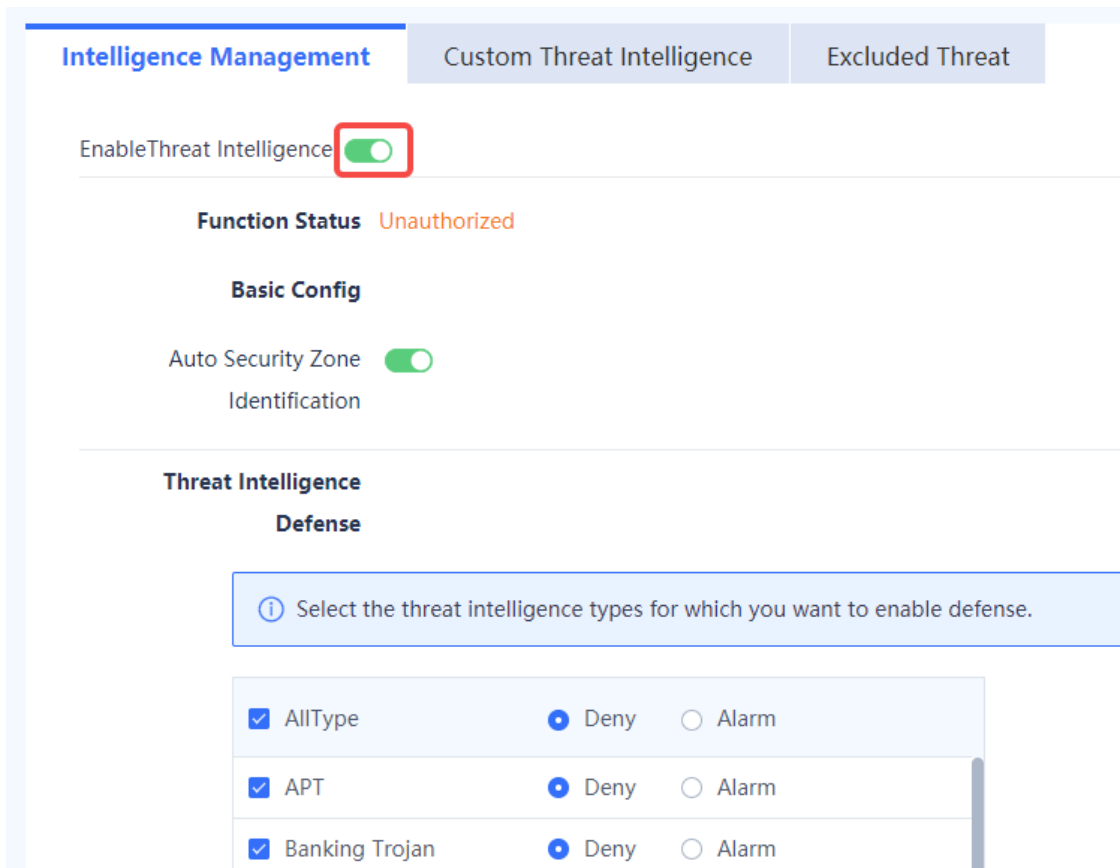
#### **Procedure**

(1) Choose **Policy > Security Defense > Threat Intelligence > Intelligence Management**.





(2) Click to enable the TI function.



(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.

<input checked="" type="checkbox"/> AllType	<input checked="" type="radio"/> Deny	<input type="radio"/> Alarm
<input checked="" type="checkbox"/> APT	<input checked="" type="radio"/> Deny	<input type="radio"/> Alarm
<input checked="" type="checkbox"/> Banking Trojan	<input checked="" type="radio"/> Deny	<input type="radio"/> Alarm
<input checked="" type="checkbox"/> Theft Trojan	<input checked="" type="radio"/> Deny	<input type="radio"/> Alarm
<input checked="" type="checkbox"/> Ransomware	<input checked="" type="radio"/> Deny	<input type="radio"/> Alarm
<input checked="" type="checkbox"/> Botnet	<input checked="" type="radio"/> Deny	<input type="radio"/> Alarm
<input checked="" type="checkbox"/> Mining Software	<input checked="" type="radio"/> Deny	<input type="radio"/> Alarm
<input checked="" type="checkbox"/> Regular Trojan	<input checked="" type="radio"/> Deny	<input type="radio"/> Alarm

Item	Description	Remarks
Function Status	<p>Current status of the TI function</p> <ul style="list-style-type: none"> <li>● <b>Unauthorized:</b> The TI function license is not activated, or online authorization fails.</li> <li>● <b>Normal:</b> The TI function license is activated. The function is available and the library can be updated.</li> <li>● <b>Server Error:</b> The TI function license is activated, but the secure cloud platform cannot connect to the threat intelligence signature library update server. The threat intelligence signature library cannot be updated.</li> </ul>	<p>The status is displayed automatically according to the current TI function status.</p> <p>[Example] Normal</p>

Item	Description	Remarks
<b>Basic Config</b>		
Auto Security Zone Identification	<p>Whether to identify the traffic inbound and outbound security zones automatically.</p> <ul style="list-style-type: none"> <li>● 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.</li> <li>● If this function is disabled, you can manually specify the effective security zones for TI.</li> </ul>	[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 <b>Auto Security Zone Identification</b> is disabled, this parameter needs to be configured. [Example] untrust
<b>Threat Intelligence Defense</b>		
Type	Select the TI type to defend against.	Select to enable defense. [Example] APT
Action	<p>Action to be taken on the traffic matching the TI:</p> <ul style="list-style-type: none"> <li>● <b>Deny:</b> Block traffic and record a security log.</li> <li>● <b>Alarm:</b> Not block traffic, but record a security log.</li> </ul>	[Example] Deny

(4) Click **Save** to complete the configuration.

### 3. Customizing Threat Intelligence

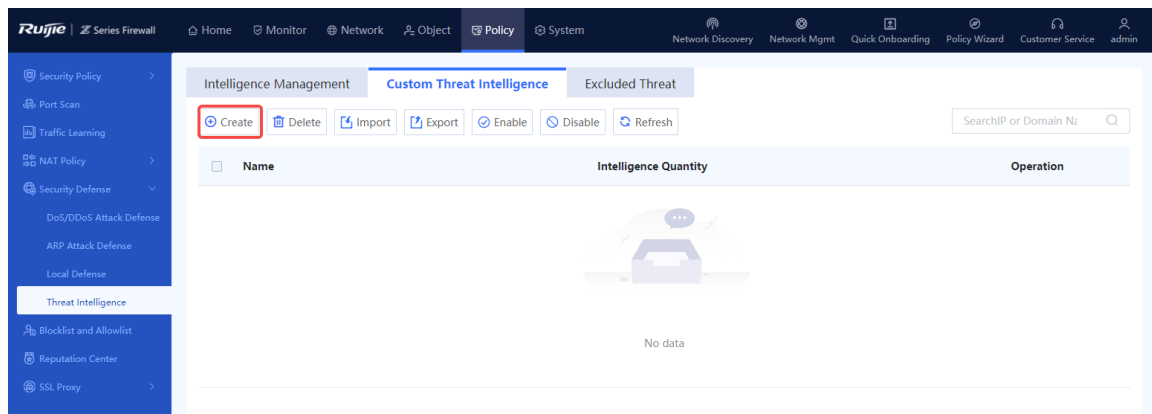
#### Application Scenario

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.

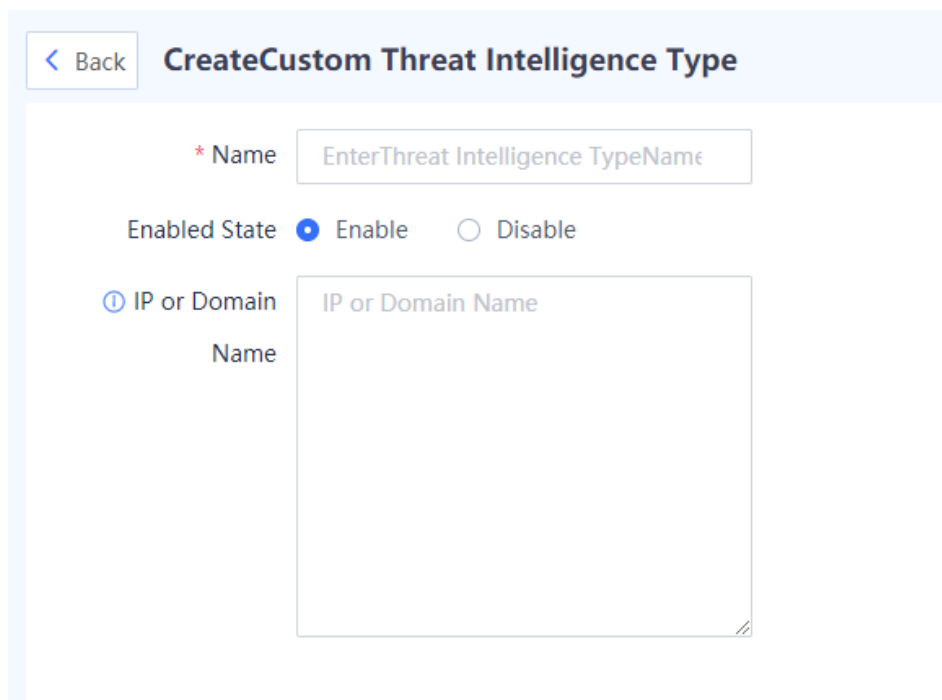
In the unauthorized state, custom threat intelligence can still be used for matching.

- 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.



(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.	<ul style="list-style-type: none"> <li>If multiple IP addresses or domain names need to be configured, enter one IP address or domain name per line, and press <b>Enter</b> to separate lines.</li> <li>The domain name matching rule is full match.</li> </ul> [Example] www.xxx.com

(4) Click **Save** to complete the configuration.

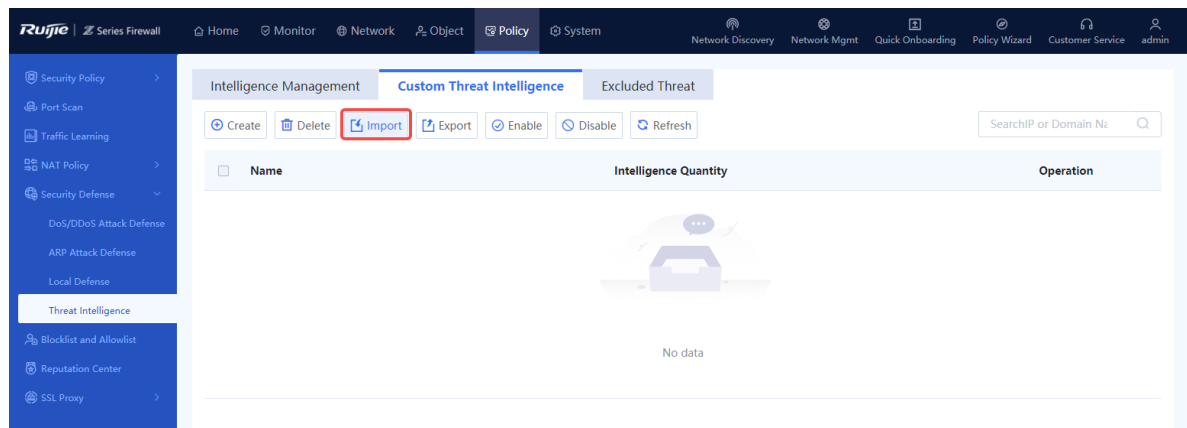
- Batch import custom TI.

### Application Scenario

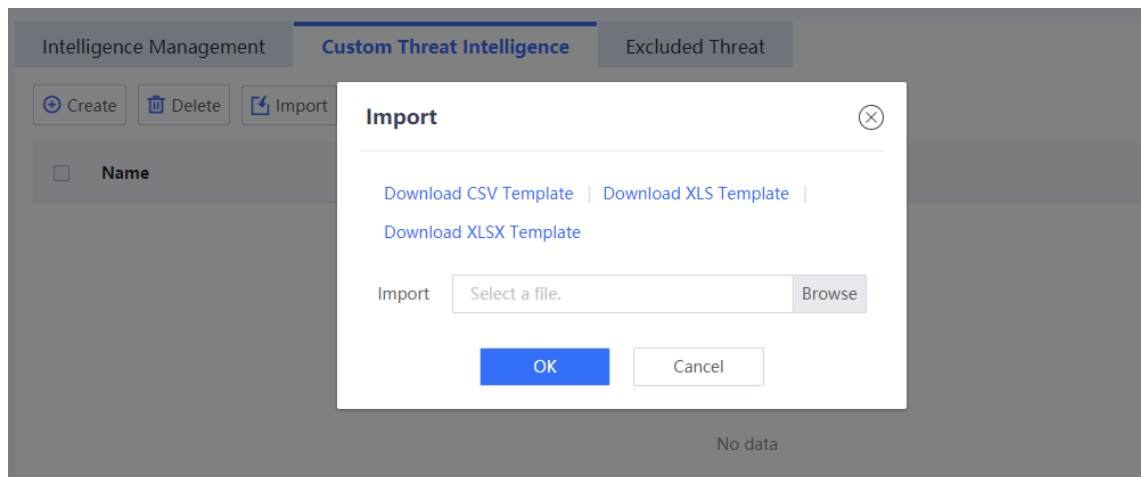
When you need to add a large number of TI types, you can fill in TI information in a template, and import them in a batch with one click.

### Procedure

(1) Choose **Policy > Security Defense > Threat Intelligence > Custom Threat Intelligence**.

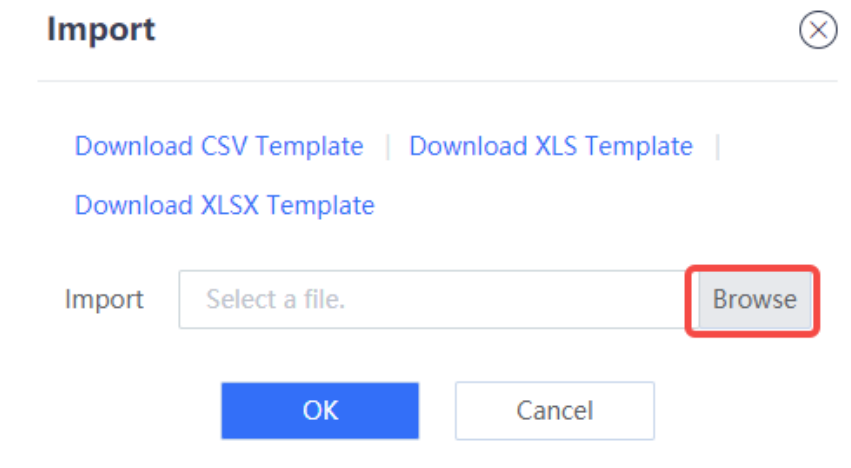


(2) Click **Import**. The **Import** dialog box is displayed.




(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.

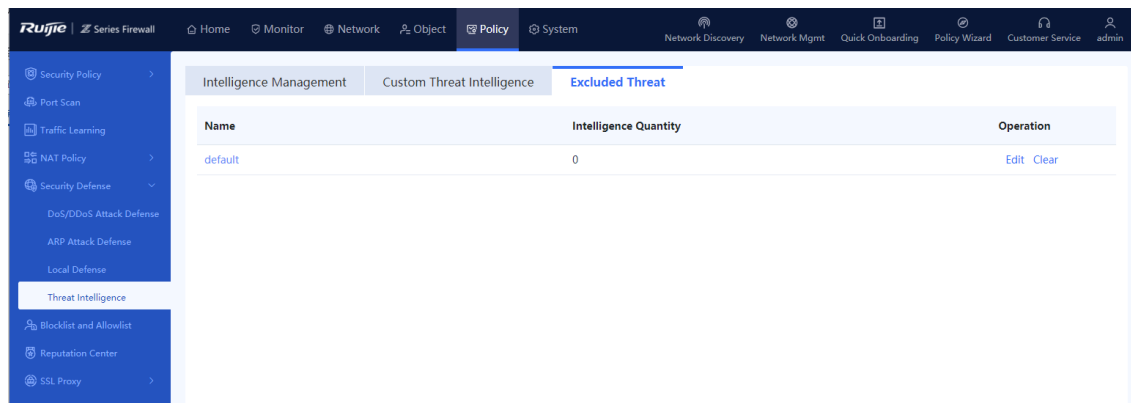
## 4. Configuring Excluded Threat

### 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**.



(2) Click **Edit** in the **Operation** column of the **default** entry.

**EditException Type**

\* Name:

① 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 <b>Enter</b> to separate lines. [Example] 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.

The screenshot shows the 'Security Log' interface with the following data:

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	<a href="#">View Details</a>
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	<a href="#">View Details</a>
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	<a href="#">View Details</a>
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	<a href="#">View Details</a>
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	<a href="#">View Details</a>
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	<a href="#">View Details</a>
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	<a href="#">View Details</a>
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	<a href="#">View Details</a>
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	<a href="#">View Details</a>
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	<a href="#">View Details</a>



(3) Click **View Details** to display attack log details.

### Security Log Details ⊗

[Exclude](#)

<p><b>Src.</b> <span style="color: red; font-weight: bold;">→</span> <span style="color: red; font-weight: bold;">Regular Trojan</span> <span style="color: red; font-weight: bold;">→</span> <b>Dest.</b></p> <p>Src. Security Zone: trust</p> <p>Src. IP: 192.168.6.36</p> <p>Src. Port: 17972</p> <p>MAC: f8:e4:3b:04:bd:5f</p>	<p>Dest. Security Zone: untrust</p> <p>Dest. IP: 101.201.78.55</p> <p>Dest. Port: 58468</p> <p>App:</p>
--	---

---

**Basic Info**

Time: 2023-03-08 17:36:35	Type: Regular Trojan
Security Event: Malware	Direction: LAN-to-WAN
Severity: <span style="color: red;">High</span>	Action: <span style="color: red;">Deny</span>
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.

#### i 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

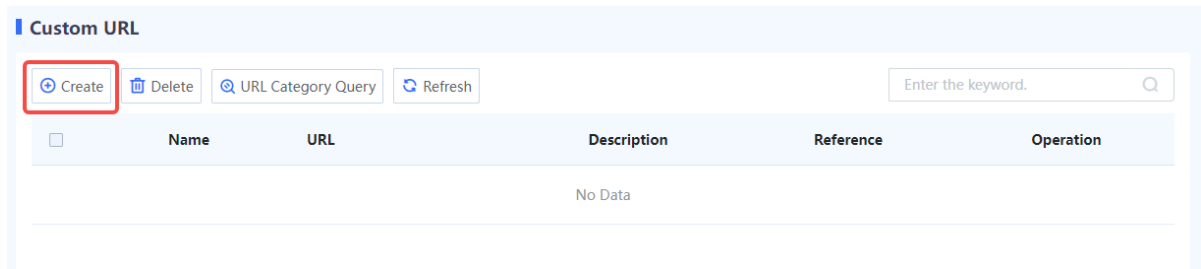
#### Application Scenario

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.

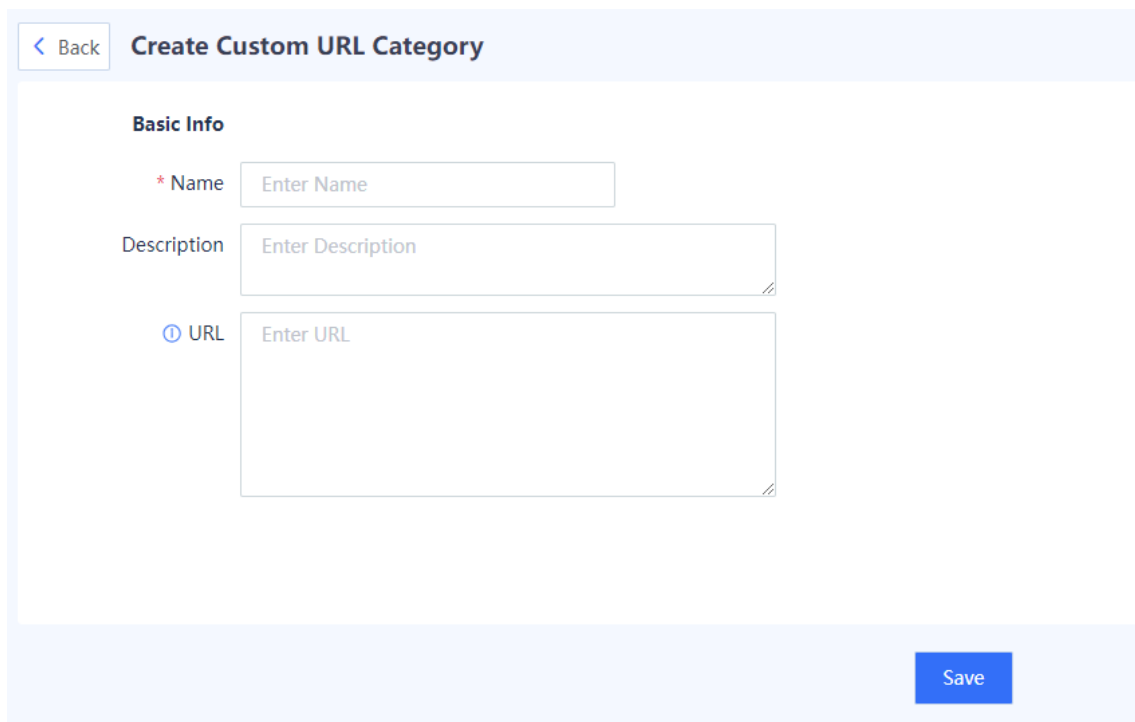
Configure a URL category to categorize web pages that intranet users can access to facilitate monitoring and management.

#### Procedure

- (1) Choose **Object > URL Category**.
- (2) Click **Create**.



- (3) Enter URL category information.



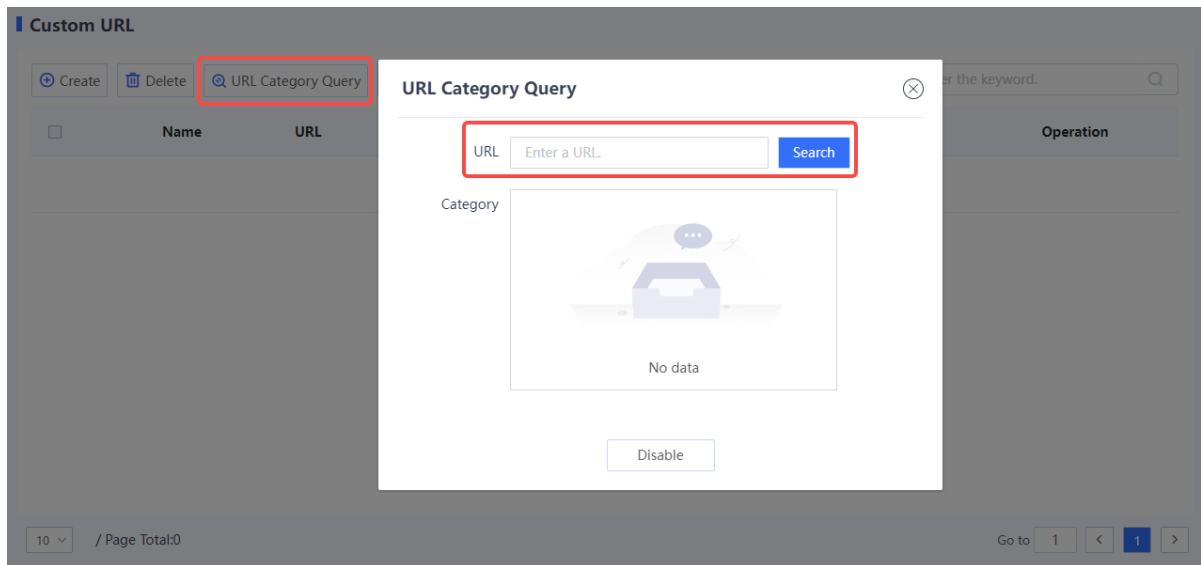
Item	Description	Remarks
<b>Basic Info</b>		
Name	URL category name.	[Example] category_1
Description	Description of the URL category.	N/A
URL	URLs in this category. A URL can contain the wildcard character (*). Enter one URL per line. Press <b>Enter</b> to separate	[Example] www.abc1.com

Item	Description	Remarks
	<p>lines.</p> <p>Note:</p> <ul style="list-style-type: none"> <li>● If a URL contains the pound sign (#), the sign and the string after the sign do not take effect for matching. For example, if <b>www.test.com/#123</b> is configured, all the domain names that start with <b>www.test.com/</b> will be matched.</li> <li>● If a URL contains the characters <b>http://</b> or <b>https://</b>, these characters will be automatically removed during matching.</li> <li>● If an IPv6 address is configured as a URL, the input format should be <i>[IPv6 address]</i>. For example, <b>[2001::1]</b>.</li> </ul>	<p>www.abc2.com</p>

(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](#).

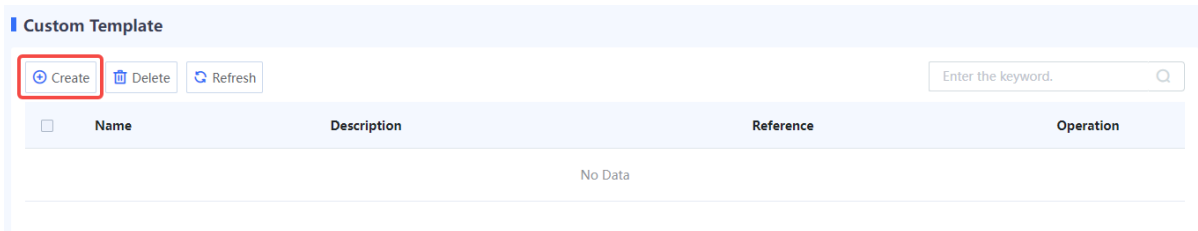
**Precautions**

- 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.

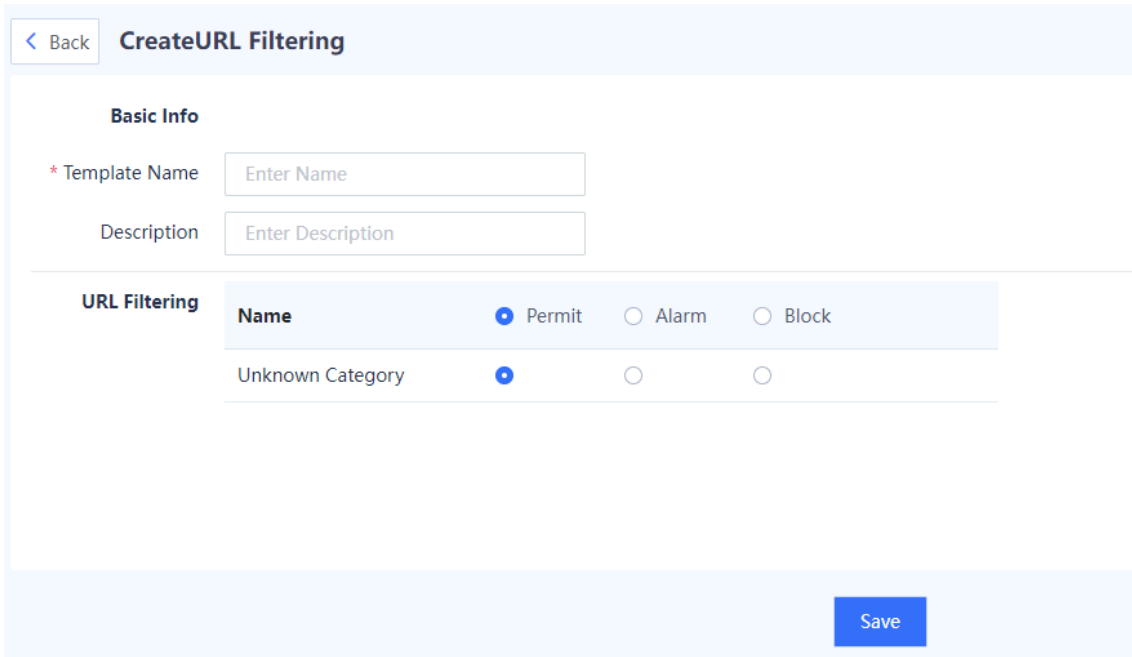
**2. Configuring a URL filtering template**

**Procedure**

- (1) Choose **Object > Content Template > URL Filtering**.
- (2) Click **Create**.



- (3) Enter URL filtering template information.



Item	Description	Remarks
<b>Basic Info</b>		
Template Name	Name of the URL filtering template.	[Example] Template_1
Description	Description of the URL filtering template.	N/A
<b>Blocklist and Allowlist</b>		
URL Allowlist	<p>After a URL is added to an allowlist, the device directly permits traffic that accesses the URL.</p> <p>URL allowlists take precedence over URL blocklists.</p> <p>Note:</p> <p>Multiple URLs can be entered. A URL can contain the wildcard character (*). Enter one URL per line. Press <b>Enter</b> to separate lines.</p> <p>If a URL contains the pound sign (#), the sign and the string after the sign do not take effect for matching. For example, if <b>www.test.com/#123</b> is configured, all the domain names that start with <b>www.test.com/</b> will be matched.</p> <p>If a URL contains the characters <b>http://</b> or <b>https://</b>, these characters will be automatically removed during matching.</p> <p>If an IPv6 address is configured as a URL, the input format should be <i>[IPv6 address]</i>. For example, <b>[2001::1]</b>.</p>	[Example] www.abc1.com
URL Blocklist	After a URL is added to a blocklist, the device directly blocks traffic that accesses the URL. The input format is the same as that for the URL allowlist.	[Example] www.abc2.com
<b>URL Filtering</b>		
URL Filtering	<p>Set processing actions for different URL categories:</p> <ul style="list-style-type: none"> <li>● <b>Permit:</b> Permit traffic that accesses the</li> </ul>	N/A

Item	Description	Remarks
	URLs of the specific categories. <ul style="list-style-type: none"> <li>● <b>Alarm:</b> Permit traffic that accesses the URLs of the specific categories and generate an alarm log.</li> <li>● <b>Block:</b> Block traffic that accesses the URLs of the specific categories and generate an alarm log.</li> </ul>	

(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.

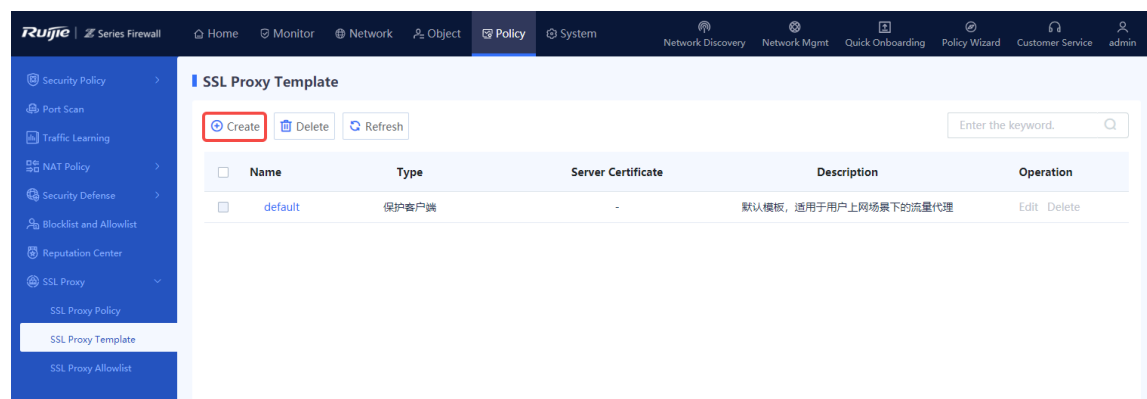
### Prerequisites

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.



- (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.

< Back

## Create SSL Proxy Template

\* Name

Description

Type  Protect Client  Protect Server

Item	Description	Remarks
Name	Name of the SSL proxy template.	Characters such as `~!#%^&*+\\{ };:'''/<>?` and spaces are not allowed. [Example] profile
Description	Proxy template description.	Characters such as `~!#%^&*+\\{ };:'''/<>?` are not allowed.
Type	The type can be <b>Protect Client</b> or <b>Protect Server</b> .	Select the type according to the actual networking scenario. [Example] Protect Client
Server Certificate	Used to establish the trust relationship between the device and client in the process of SSL proxy.	Required only when the template type is Protect Server. Imported server certificates can be selected.

### Follow-up Procedure

Create an SSL proxy policy and reference the SSL proxy template.

## 7.3.3 Importing Certificate

### 1. Importing SSL Proxy Certificate

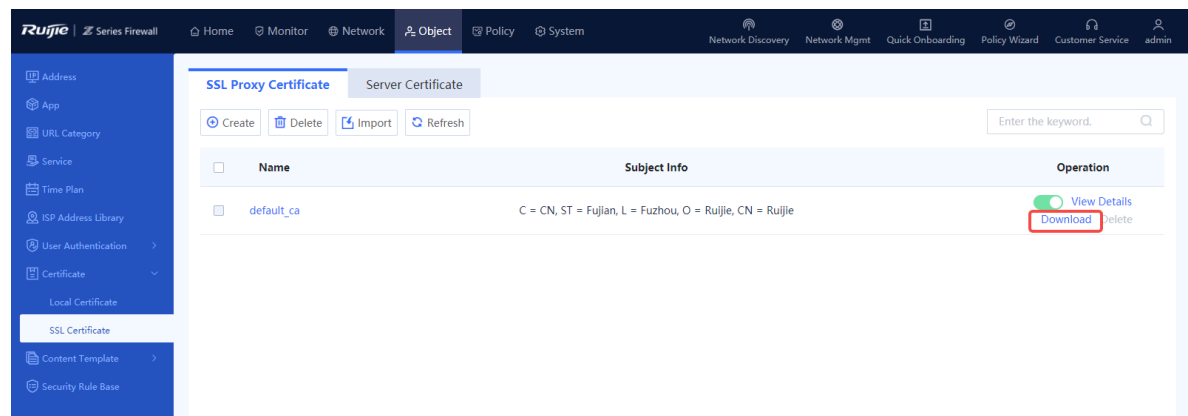
#### Application Scenario



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.

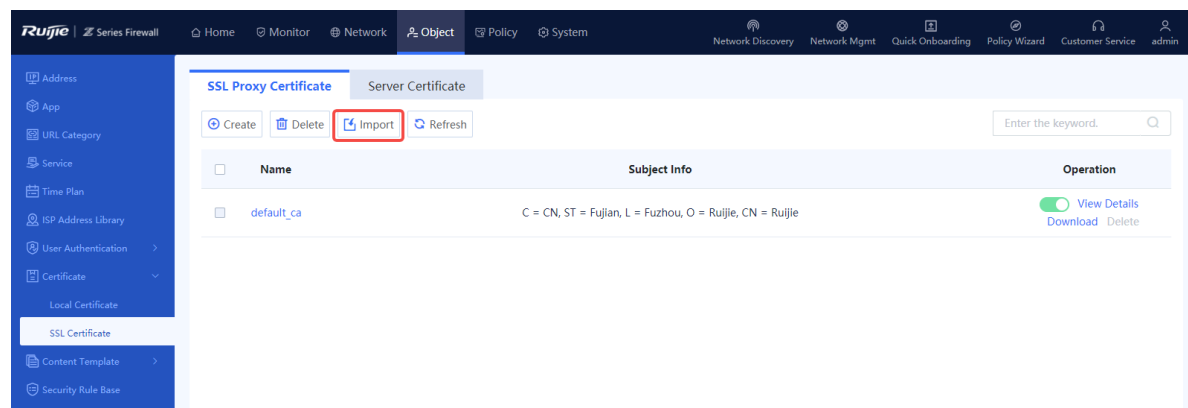
## Precautions

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.



## Procedure

- (1) Choose **Object > Certificate > SSL Certificate > SSL Proxy Certificate**.
- (2) Click **Import** to enter the **Import SSL Proxy Certificate** page.



### **i** 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


\* Certificate    
 File

\* 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.	<ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul> <p>[Example] P12</p>
Certificate File	Imported SSL proxy certificate file.	Click <b>Browse</b> 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.	<ul style="list-style-type: none"> <li>● Certificate with the p12 or pem suffix: You need to specify the password of the certificate when importing the certificate.</li> <li>● Certificate with the crt suffix: When you import the certificate, specify the key file and password of the key file.</li> </ul>

### 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.



- 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.

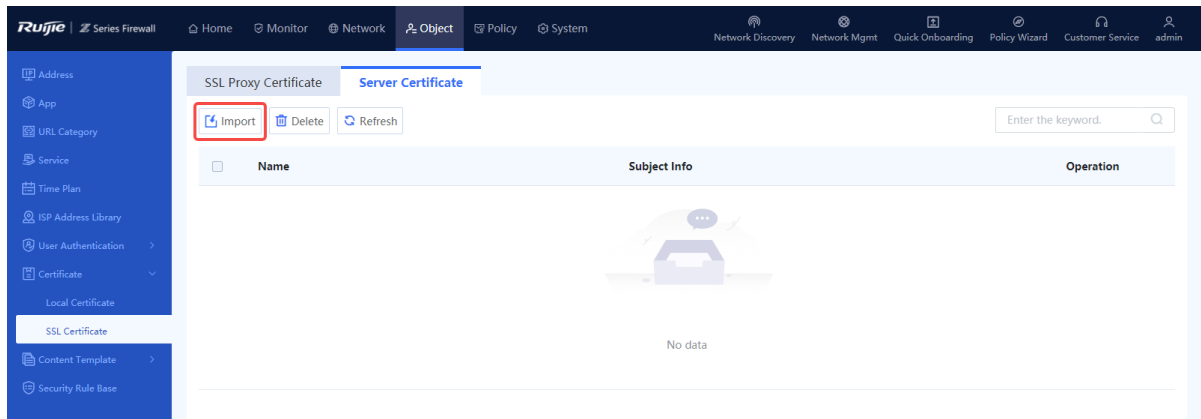
## 2. Importing Server Certificate

### 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**.

### Import Server Certificate ⊗

---

\* Certificate Format

\* Certificate File

\* Password

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, P12, or CRT format.	<ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul> <p>[Example]</p>

Item	Description	Remarks
		P12
Certificate File	Imported server certificate file.	Click <b>Browse</b> 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.	<ul style="list-style-type: none"> <li>● Certificate with the p12 or pem suffix: You need to specify the password of the certificate when importing the certificate.</li> <li>● Certificate with the crt suffix: When you import the certificate, specify the key file and password of the key file.</li> </ul>

### 7.3.4 Configuring an SSL Proxy Policy

#### Application Scenario

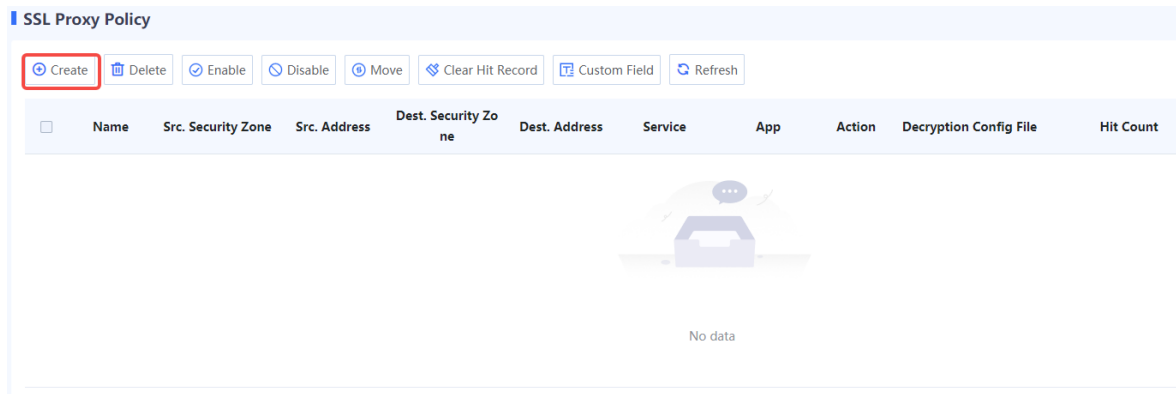
Configure this function if you need to perform virus protection detection or IPS detection for HTTPS encrypted traffic.

#### 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.



(3) Configure the SSL proxy policy according to the following table.

< Back

### Create SSL Proxy Policy

**Basic Info**

\* Name

Enabled State  Enable  Disable

Description

---

**Src. and Dest.**

\* Src. Security Zone

\* Src. Address

\* Dest. Security Zone

\* Dest. Address

---

**Service**

Service

---

**App**

App

---

**Decryption Settings**

Action Option  Decrypt  Not Decrypt

Item	Description	Remarks
Basic Info		

Item	Description	Remarks
Name	Name of the SSL proxy policy.	Characters such as `~!#%^&*+V0:/"<>? 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 <b>To-be-selected</b> area. The selected address is automatically added to the <b>Selected</b> area. [Example] Any
Dest. Security Zone	Destination security zone of the target data connection.	[Example] trust
Dest. Address	Destination address of the target data connection.	Click the drop-down list, and select a destination address in the <b>To-be-selected</b> area. The selected address is automatically added to the <b>Selected</b> area. [Example]

Item	Description	Remarks
		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 <b>Decrypt</b> 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

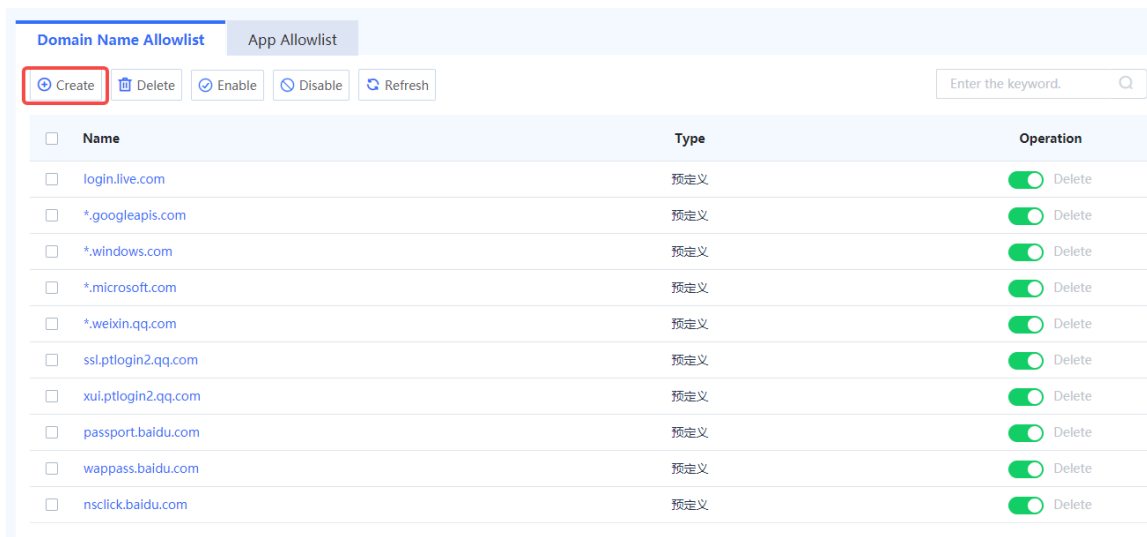
#### Application Scenario

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.

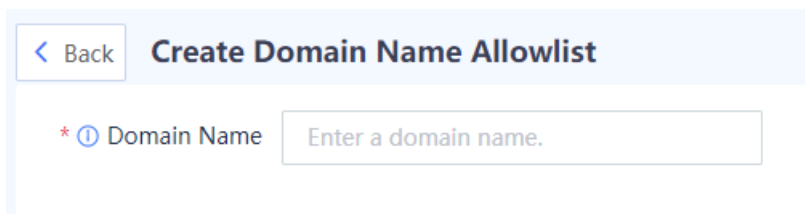
#### Procedure

- (1) Choose **Policy > SSL Proxy > SSL Proxy Allowlist > Domain Name Allowlist**.
- (2) Click **Create** to enter the **Create Domain Name Allowlist** page.





(3) Enter the domain name and click **Save**.



## 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.

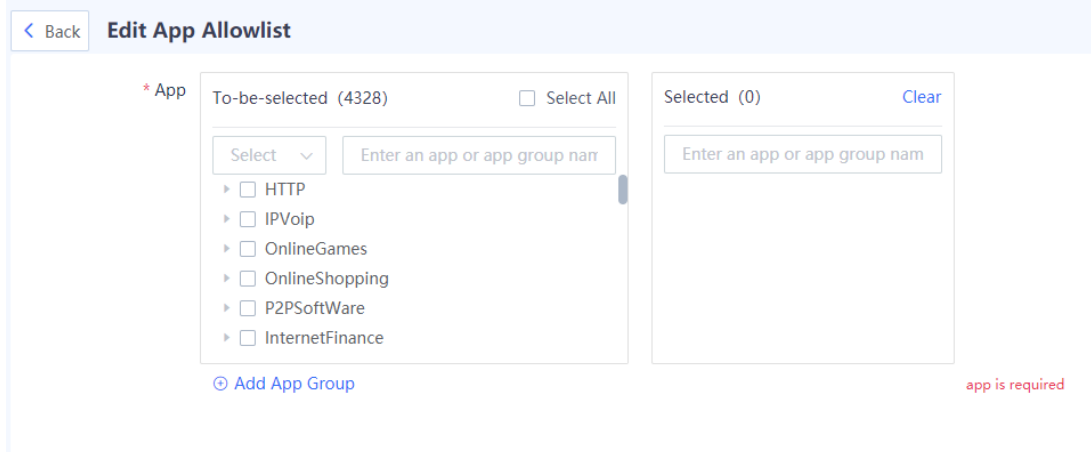
The preconfigured application allowlist of SSL proxy includes the commonly used applications, the applications that do not need to be or cannot be accessed by SSL proxy. You can add applications to the predefined application allowlist.

### Procedure

- (1) Choose **Policy > SSL Proxy > SSL Proxy Allowlist > App Allowlist**.
- (2) Click **Edit** to enter the **Edit App Allowlist** page.



(3) Select the applications or application group to be added to the allowlist, and click **Save**.



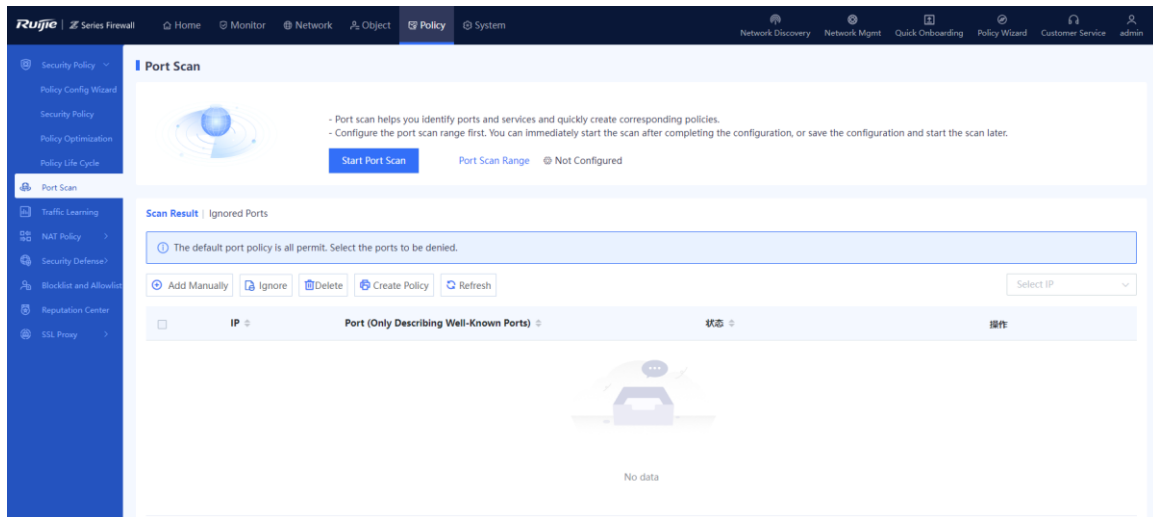
## 7.4 Port Scan

### 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

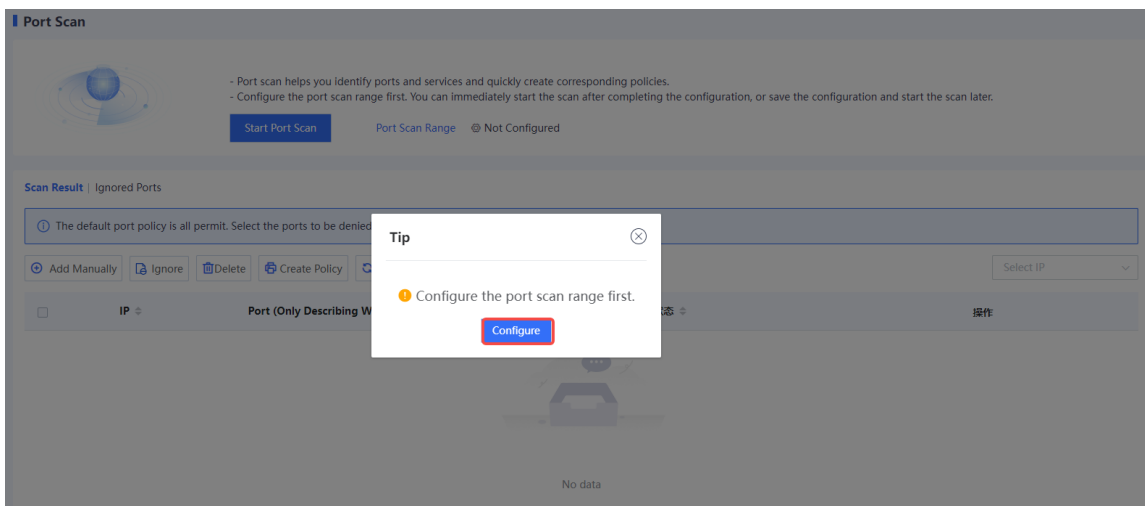
(1) Choose **Policy > Port Scan**.



(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**.



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

IP Address/Range

No Data

---

**Select or Add Ports for Scan**

UDP Scan  Yes  No

Select Ports  All Ports  Custom Ports

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

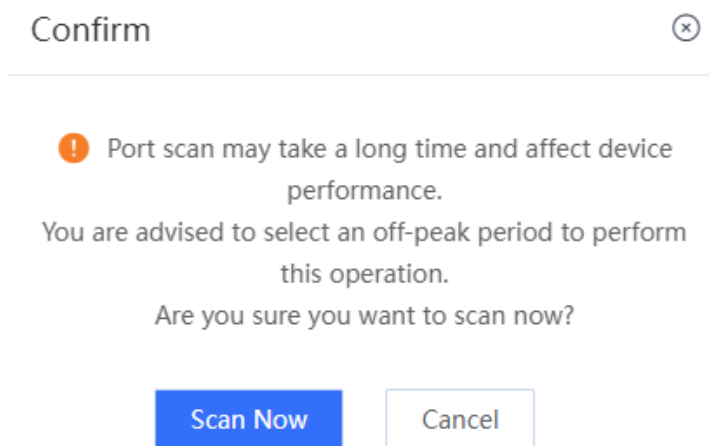
Add Custom Port Range

Item	Description	Remarks
UDP Scan	Whether to perform UDP scan.	[Example]

Item	Description	Remarks
		Yes
Select Ports	Select the port to be scanned: <ul style="list-style-type: none"> <li>● <b>All Ports:</b> Scan all ports.</li> <li>● <b>Custom Ports:</b> Customize the ports to be scanned.</li> <li>● Select <b>Common Ports</b> to add common service ports. You can click <b>Select Common Ports</b> to select common service ports.</li> <li>● Select <b>Custom Ports</b> to add the ports to be scanned.</li> </ul>	[Example] All Ports

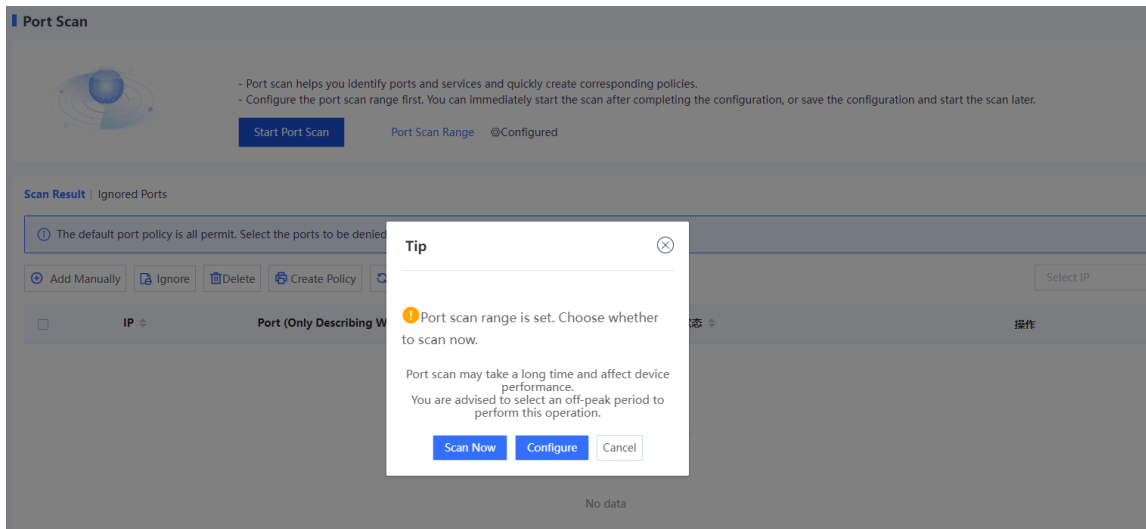
- d Choose whether to start port scan immediately according to service situation.
- o When services are busy, click **Save** to save the port scan configuration. You can start port scan when services are idle.
- o When services are idle, click **Save and Scan Now** to save the port scan configuration and start port scan immediately.

Confirm the system prompt and click **Scan Now**.

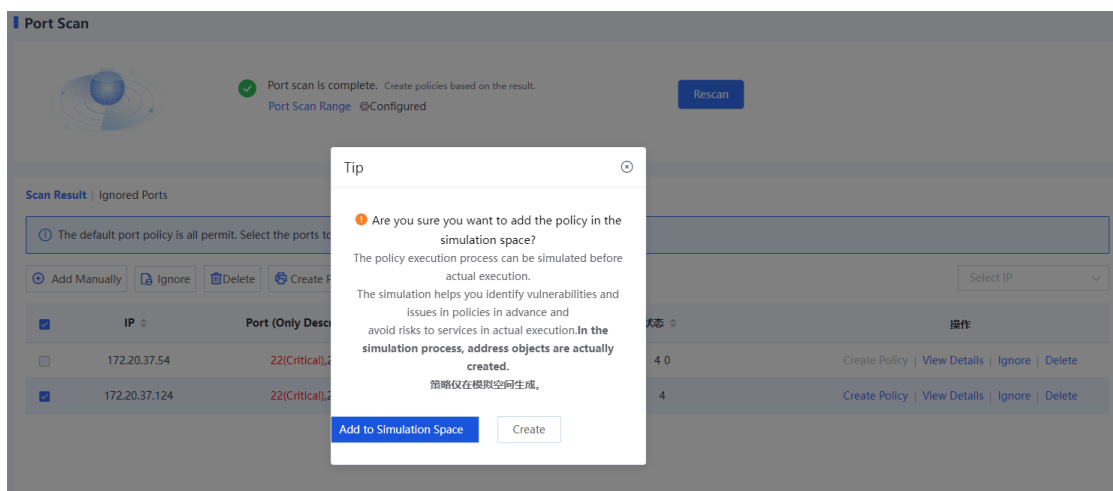
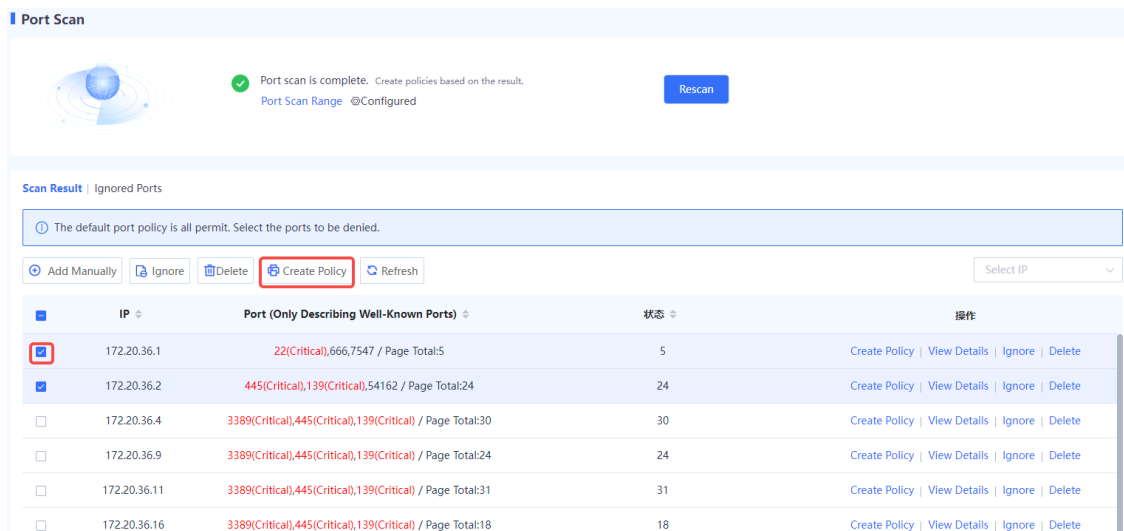


(3) (Optional) If port scan policy has been configured:

- a Click **Start Port Scan**.
- b Click **Scan Now** to start port scan.



(4) When port scan is finished, select the scan result and click **Create Policy**.



- o Click **Create** to add the generated security policy to the security policy list.

**Insert it to the specified location.** ⊗

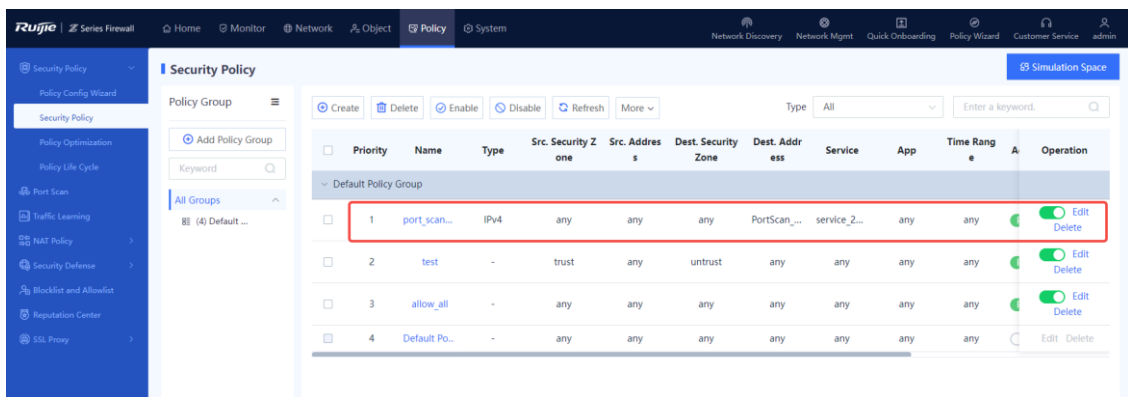
---

\* Policy Name   
Prefix

\* Policy Group  ▼

Policy  ▼

Before/After  ▼  
the Adjacent  
Policy



- o 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



- 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.

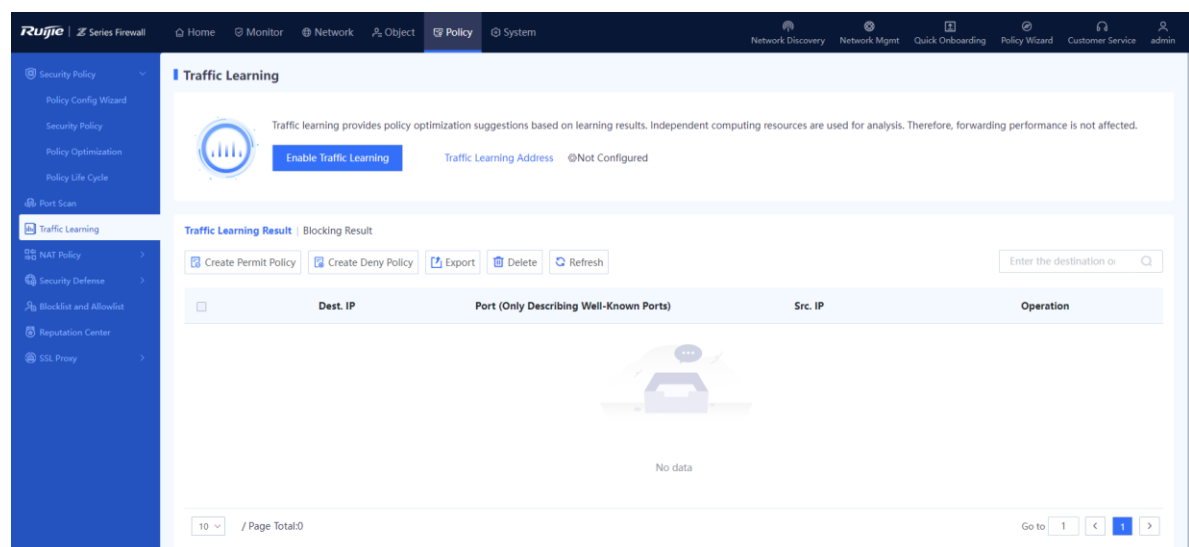
## 7.5 Traffic Learning

### 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

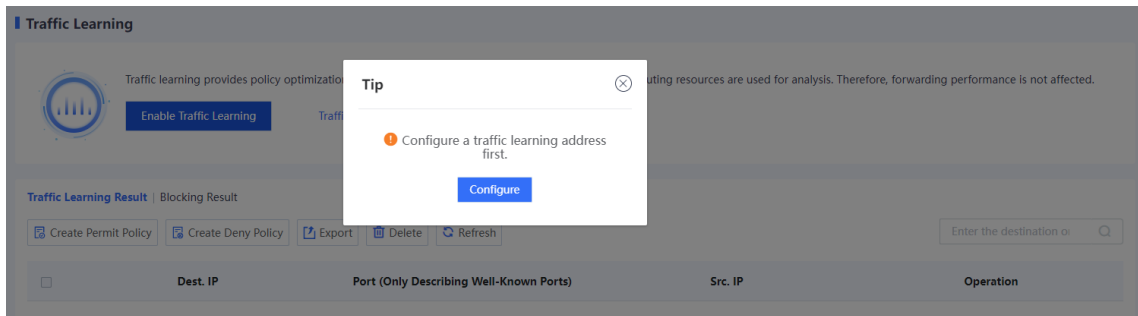
(1) Choose **Policy > Traffic Learning**.



(2) (Optional) If the traffic learning address is not configured, configure it first.

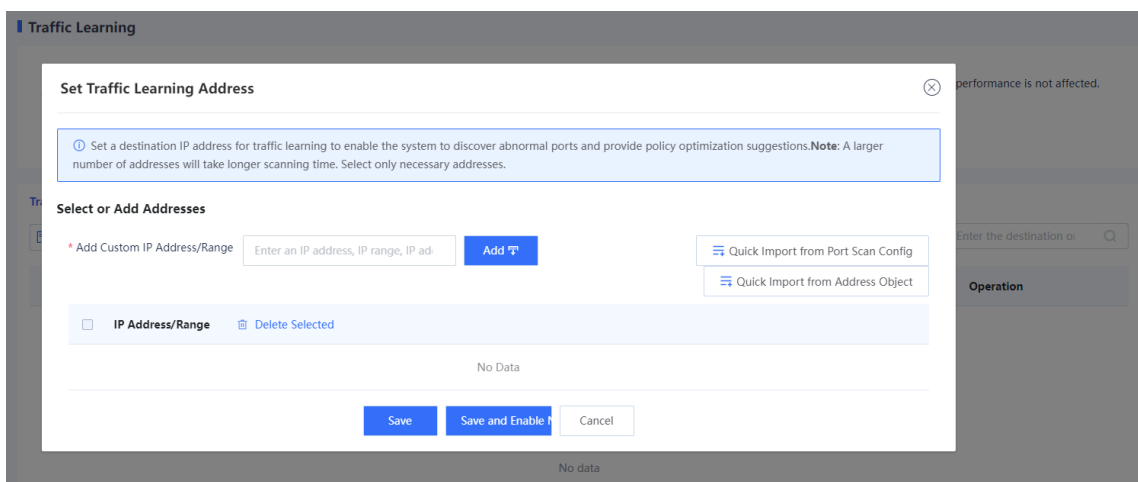
- Click **Enable Traffic Learning** and click **Configure** in the prompt box to configure the traffic learning address.





b Select or add the IP address to be learned.

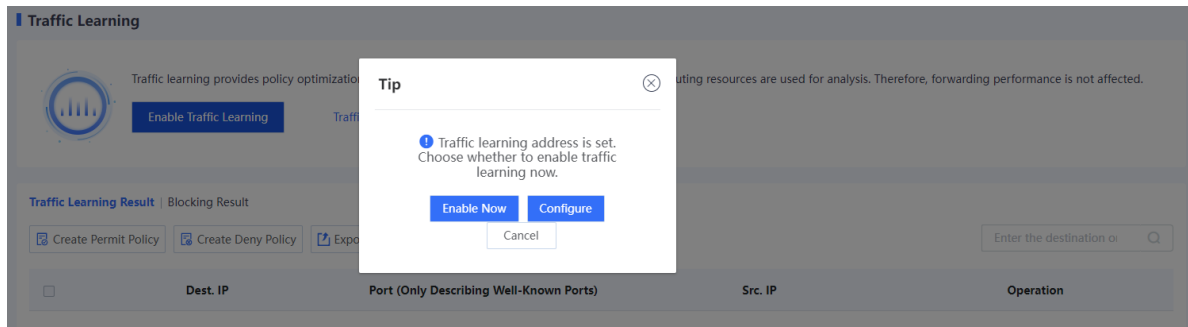
Enter the IP address or range to be learned in the **Add Custom IP Address/Range** input box, and click **Add** to add it to the **IP Address/Range** area.



### 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.
  - o When services are busy, click **Save** to save the traffic learning address configuration. You can enable traffic learning when services are idle.
  - o 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.



**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**.

Traffic Learning Result | Blocking Result

Create Permit Policy Create Deny Policy Export Delete Refresh

Enter the destination or

	Dest. IP	Port (Only Describing Well-Known Ports)	Src. IP	Operation
<input type="checkbox"/>	172.20.37.124	443	172.25.22.250 1	Create Permit Policy Create Deny Policy <b>View Details</b> Delete
<input type="checkbox"/>	172.20.37.124	445(Critical)	172.18.162.108 1	Create Permit Policy Create Deny Policy View Details Delete

10 / Page Total:2

Go to 1 < 1 >

- You can choose to generate a deny policy or a permit policy for a specific traffic learning result.
  - On the traffic learning result page, click **Create Deny Policy** or **Create Permit Policy**.

172.20.37.124445

Create Permit Policy Create Deny Policy Delete Refresh

Enter the source IP add

	Src. IP	协议类型	Status	Operation
<input type="checkbox"/>	172.18.162.108	TCP	Unhandled	<b>Create Permit Policy</b> <b>Create Deny Policy</b> Delete

10 / Page Total:1

Go to 1 < 1 >

- 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.**

**Add to Simulation Space**    Create

**Insert it to the specified location.** ⓧ

---

\* Policy Name   
Prefix

\* Policy Group   
Policy

Before/After   
the Adjacent Policy

**OK**    Cancel

- c After confirming that the policy is appropriate in the simulation space, add it to the security policy list.

Priority	Name	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count	Hit Session	Operation
1	LnDeny_44	TrafficLear...	any	any	any	Deny		0	Clear	View Details.. Edit Delete
2	port_scan...	PortScan_...	service_2...	any	any	Permit		0	Clear	View Details.. Edit Delete
3	test	any	any	any	any	Permit		0	Clear	View Details.. Edit Delete
4	allow_all	any	any	any	any	Permit		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 provides policy optimization suggestions based on learning results. Independent computing resources are used for analysis. Therefore, forwarding performance is not affected.

Traffic Learning Result | **Blocking Result**

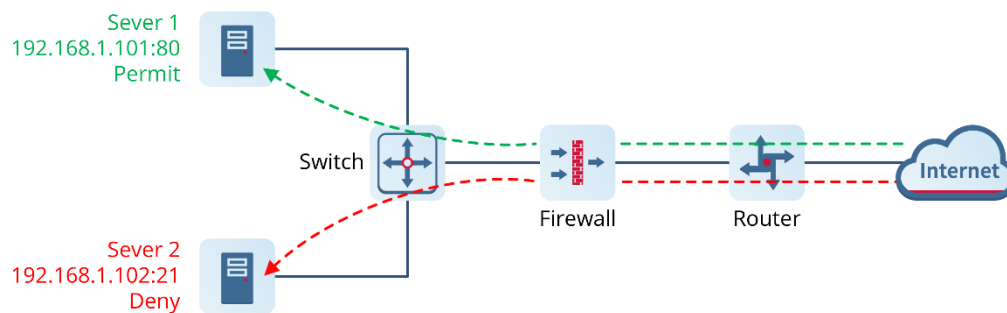
Dest. IP	Port (Only Describing Well-Known Ports)	Src. IP	Operation
No data			

## 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

描述

\*生效范围  全年  指定时间范围

---

**周期时间表**

<input type="checkbox"/>	周期	时间段	操作
<input type="checkbox"/>	周一,周二,周三,周四,周五	09:00:00-18:00:00	<a href="#">编辑</a> <a href="#">删除</a>

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.

App Custom App App Group

App Type

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
MeituxiuxiuorMeyan	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

App Type List:

- HTTP
- IPVoip
- OnlineGames
- OnlineShopping
- P2PSoftWare
- InternetFinance
- InstantMessenger
- InstantMessaging-APP
- VideoCategory
- VideoStreamingMediaSoftware
- HttpVideos
- Videos-APP
- VideoLIVE
- MusicRoAudio
- InternetFileTransfer
- ProtocolClass
- InternetofThings
- RemoteControl

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.

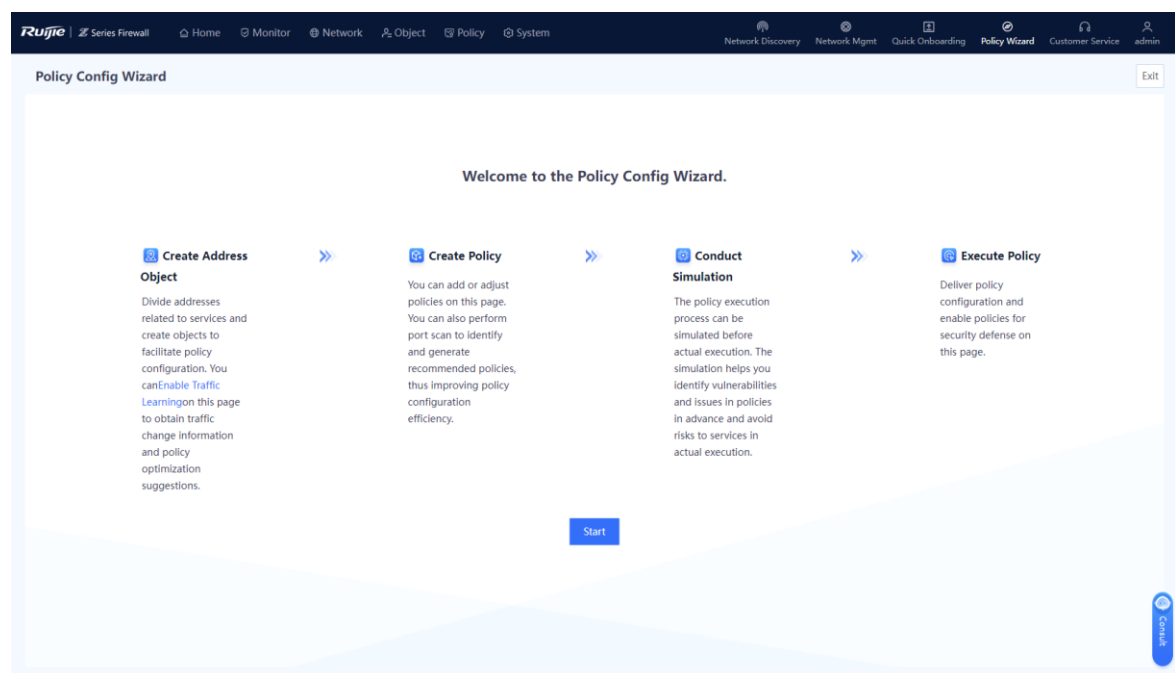
By default, the device is configured with a security policy that blocks all packets, and the default policy cannot be deleted or modified.

## 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.



### 1. Creating an Address Object

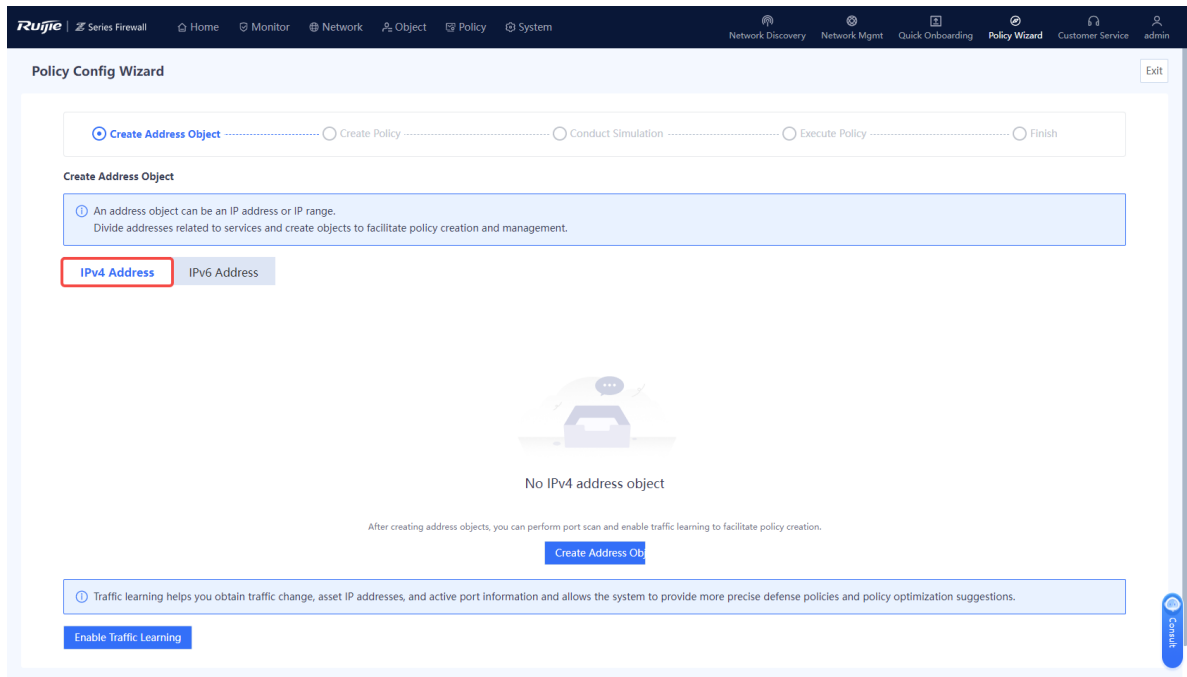
#### Application Scenario

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.

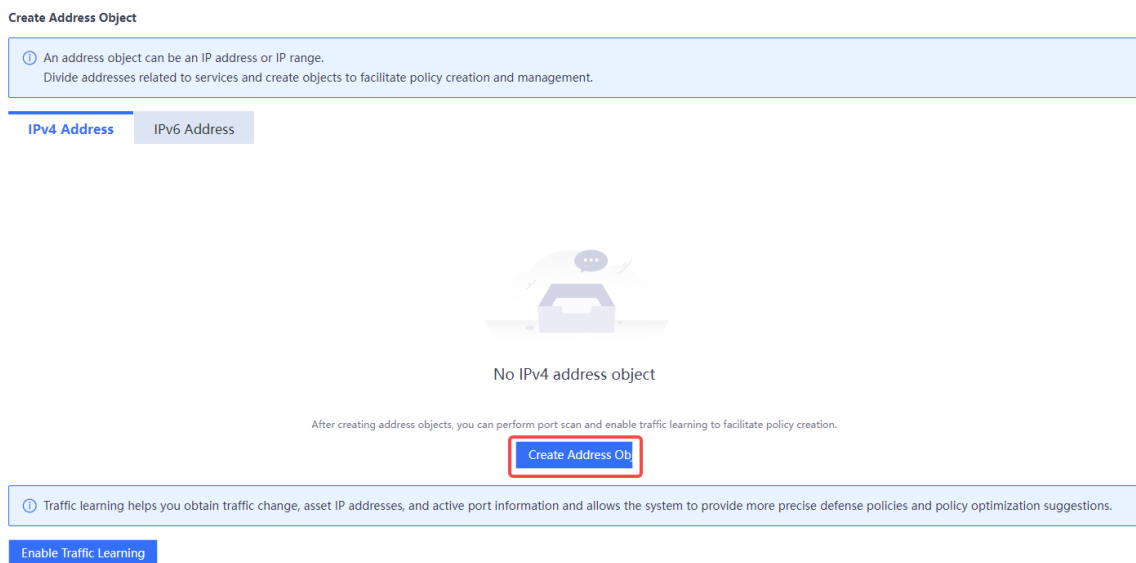
#### Procedure

- (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**.

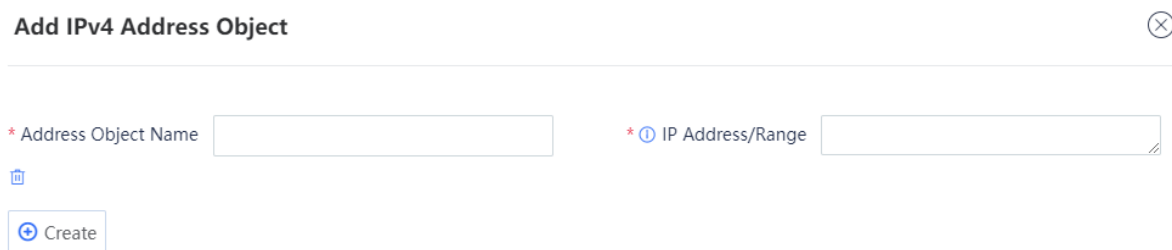




(2) Click **Create Address Object**.



(3) Fill the names and IP addresses/ranges in the **Add IPv4 Address Object** or **Add IPv6 Address Object** page.



## Add IPv6 Address Object



\* Address Object Name

\* IP Address/Range



Create

Item	Description	Remarks
Address Object Name	Name of the IP address object.	[Example] Addr1
IP Address/Range	IP address or range.	<p>Three configuration methods are supported:</p> <ul style="list-style-type: none"> <li>● IP address: One or multiple IP addresses. Input an IP address per line. Press <b>Enter</b> to separate lines. <ul style="list-style-type: none"> <li>○ Example 1: 192.168.20.3</li> <li>○ Example 2: 1234::100</li> </ul> </li> <li>● IP address range: A contiguous range of addresses. Connect the start IP address and end IP address with a hyphen (-). <ul style="list-style-type: none"> <li>○ Example 1: 192.168.20.1-192.168.20.3</li> <li>○ Example 2: 1234::100-2345::100</li> </ul> </li> <li>● Network segment: IP address network segment <ul style="list-style-type: none"> <li>○ Example 1: 192.168.1.0/24 or 192.168.1.0/255.255.255.0</li> <li>○ Example 2: 1234::100/100</li> </ul> </li> </ul>

**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.

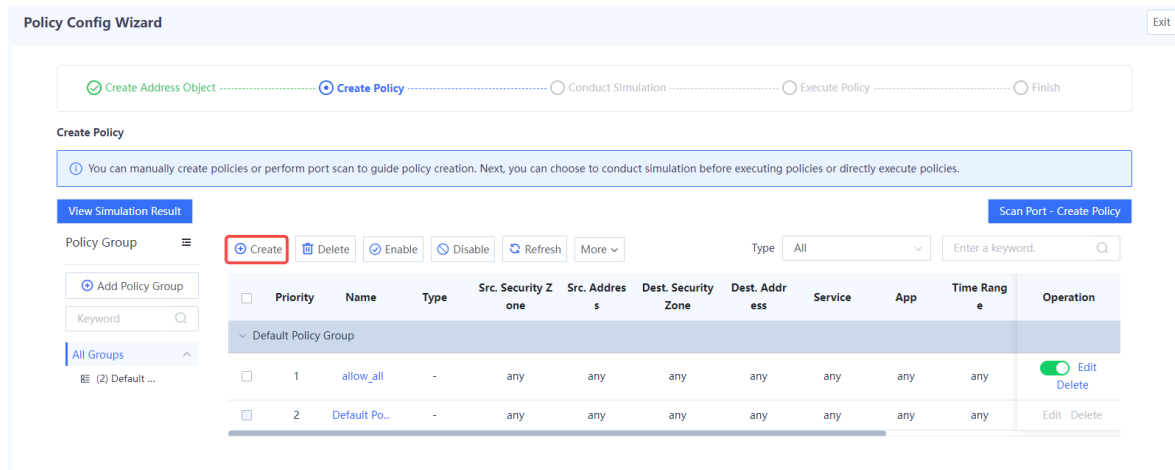
The security policy verifies the traffic passing the firewall. Only the traffic matching the security policy with the permit action can be forwarded. The security policy function provides security defense. For example, a firewall can be located at the boundary between an intranet and the Internet. A 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**.



- (2) Set parameters related to security policy.
  - a Configure basic information about security policy.

### Create Security Policy

**Basic Info**

\* Name

Enabled State  Enable  Disable

\* Policy Group  [⊕ Add Group](#)

\* Adjacent Policy

Description

- b Configure the source and destination security zones and addresses of the target data connection.

**Src. and Dest.**

\* Src. Security Zone

\* Src. Address

\* Dest. Security Zone

\* Dest. Address

Item	Description	Remarks
Src. Security Zone	Security zone initiating the target data connection.	Select from the drop-down list. [Example] untrust
Src. Address	Source address that initiates the target data connection.	Select a source address in the <b>To-be-selected</b> area. The selected address is automatically added to the <b>Selected</b> area.

Item	Description	Remarks
		[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 <b>To-be-selected</b> area. The selected address is automatically added to the <b>Selected</b> area. [Example] Any

- c (Optional) Select the service and application of the target data connection request.

**Service**

Service  ▾

**App**

App  ▾

- d (Optional) Select the time range in which the policy is effective.

**Time Range**

Time Range  ▾ [⊕ 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	<p>If the action is set to <b>Permit</b>, the device performs check according to whether content security check is enabled:</p> <p>Content security check is not enabled: Directly permit the traffic.</p> <p>Content security check is enabled: Process the traffic according to the content check policy.</p>
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 ⓘ

Select the duration. ▼

h Click **Save**.

### 3. Simulation Run

#### Application Scenario

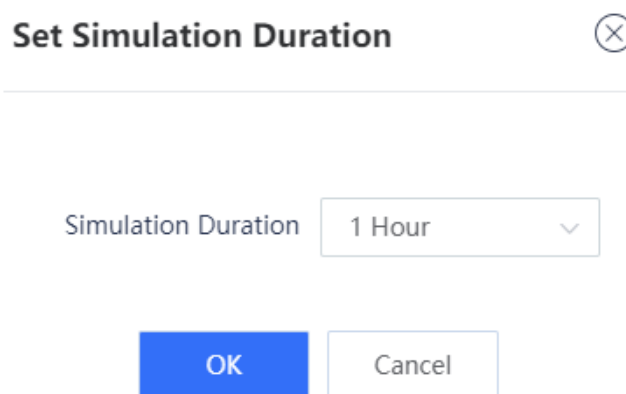
After you create a security policy, you can conduct simulation run to discover vulnerabilities or problems of the policy in advance to avoid risks to services in actual implementation.

#### Procedure

(1) On the **Create Policy** page, select the policy for which simulation run will be performed, and click **Start Simulation**.

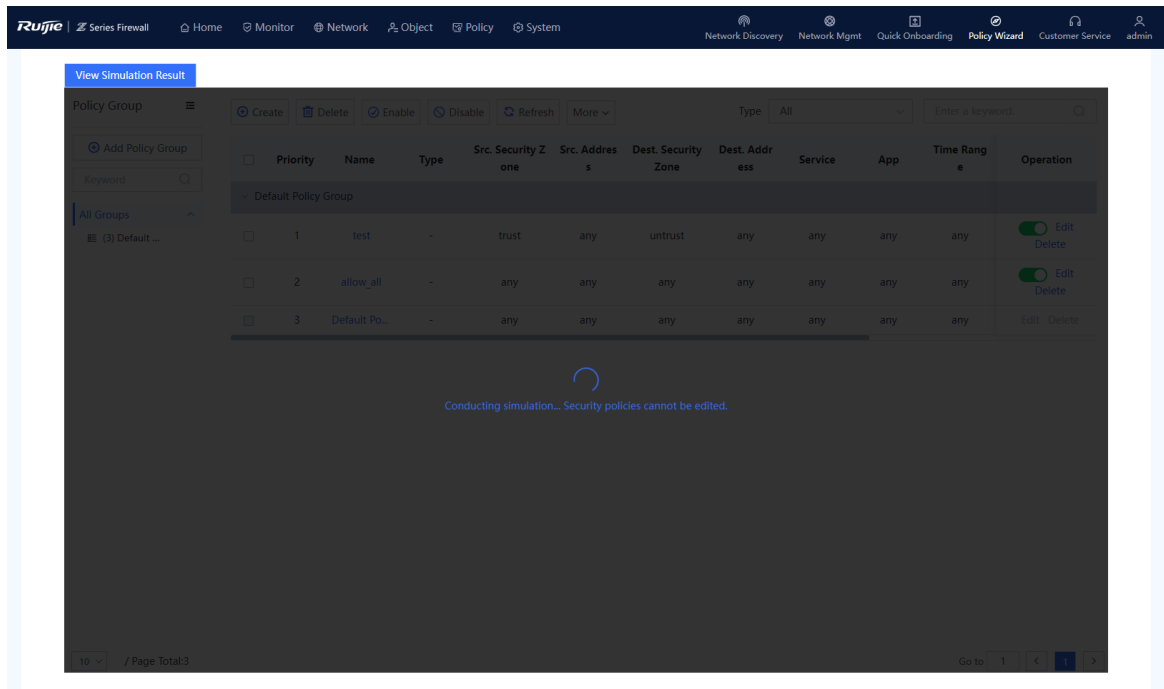


(2) In the **Set Simulation Duration** dialog box, set the duration of simulation run.



(3) Click **OK**.

The system automatically performs simulation run for the selected policies.



(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:


- o The number of times traffic is permitted in the real policy but blocked in the simulated policy.
- o 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** ⊗

① Due to capacity limitations, only the details about the first 100,000 simulation results are recorded.

Refresh Clear Result

Src. Address	Actual Execution Result	Simulation Result	Hit Count in Actual Execution	Hit Count in Simulation	Details
 <p style="color: red; font-weight: bold;">The actual execution result is the same as the simulation result.</p>					

10 / Page Total:0 Go to: 1 < 1 >

(6) If the simulation results are as expected, click **Apply to Real Network** to make the policy effective.



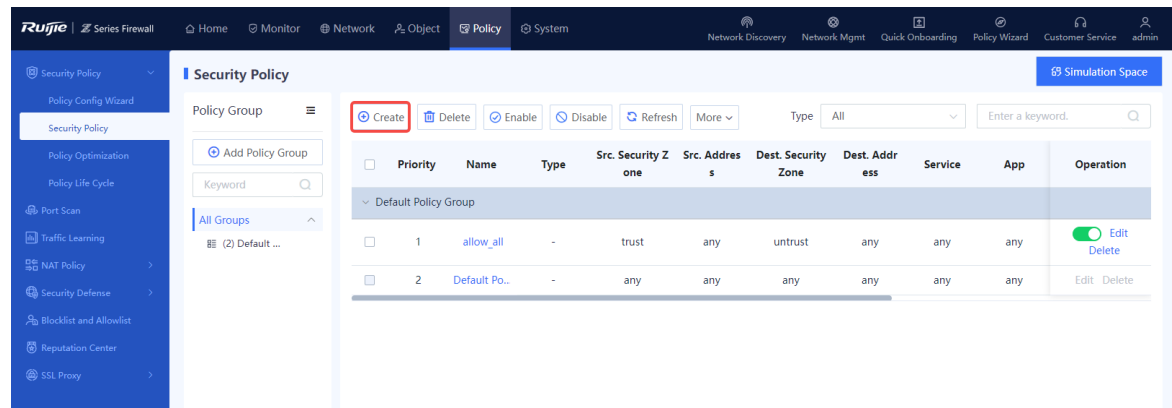
## 7.6.3 Configuring Security Policy (Manual)

### 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**.



(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.

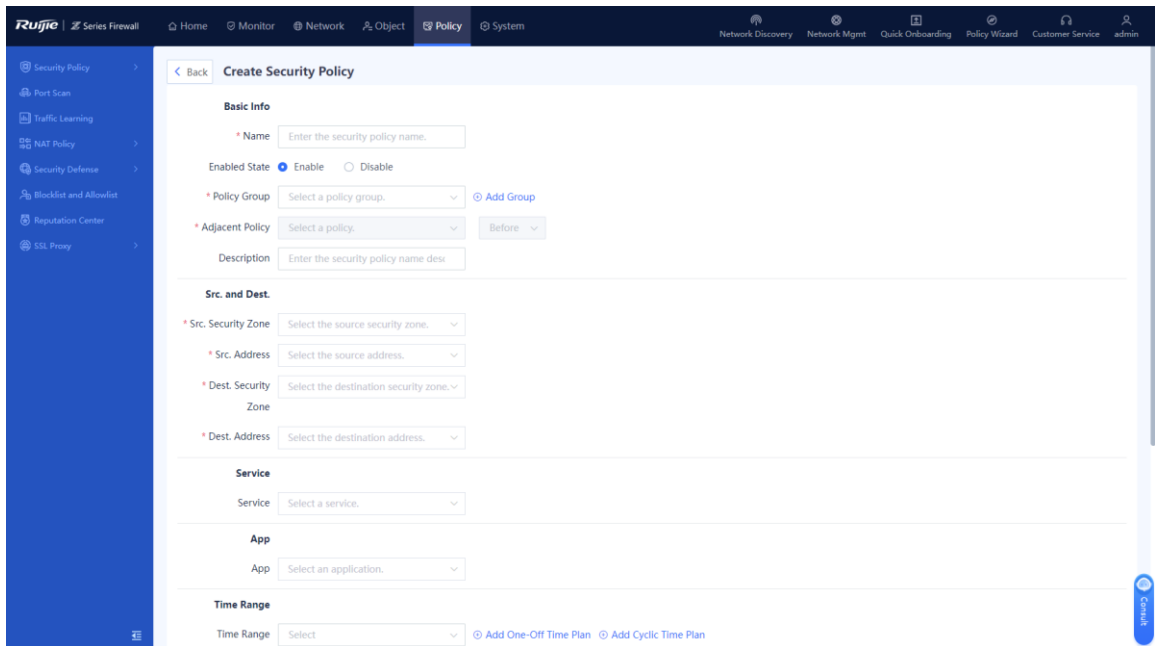
Do Not Show This Again

Simulation Space

Create

(3) Click **Create**.

The system displays the **Create Security Policy** page.



(4) Set parameters of security policy.

Item	Description	Remarks
Basic Info		
Name	Security policy name.	<p>Characters such as `~!#%^&amp;*+\/0:."/&lt;&gt;? and spaces are not allowed.</p> <p>[Example]</p> <p>Trust_to_untrust</p>
Enabled State	Whether to enable the new security policy.	<p>[Example]</p> <p>Enable</p>
Policy Group	Policy group to which the new security policy belongs.	<ul style="list-style-type: none"> <li>● Select from the drop-down list.</li> <li>● Click <b>Add Group</b> to add a custom policy group.</li> </ul> <p>[Example]</p> <p>Default policy group.</p>
Adjacent Policy	Move the new security policy before or after the specified policy. The	-

Item	Description	Remarks
	closer a policy is to the front, the higher its priority is in matching.	
Description	Security policy description.	Characters such as `~!#%&*+ \{ } ; : " / < > ?` are not allowed. [Example] Perform virus detection for the HTTP traffic from security zone 1 to security zone 2.
Src. and Dest.		
Src. Security Zone	Source security zone initiating the target data.	<ul style="list-style-type: none"> <li>● Click the drop-down list, and select a source security zone in the <b>To-be-selected</b> area. The selected zone is automatically added to the <b>Selected</b> area.</li> <li>● Click <b>Add Security Zone</b> to add a custom security zone.</li> </ul> [Example] trust
Src. Address	Source address that initiates the target data connection.	Click the drop-down list, and select a source address in the <b>To-be-selected</b> area. The selected address is automatically added to the <b>Selected</b> area. [Example] Any
Dest. Security Zone	Destination security zone of the target data connection.	<ul style="list-style-type: none"> <li>● Click the drop-down list, and select a destination security zone in the <b>To-be-selected</b> area. The selected zone is automatically added to the <b>Selected</b> area.</li> <li>● Click <b>Add Security Zone</b> to add a custom security zone.</li> </ul>

Item	Description	Remarks
		[Example] trust
Dest. Address	Destination address of the target data connection.	Click the drop-down list, and select a destination address in the <b>To-be-selected</b> area. The selected address is automatically added to the <b>Selected</b> 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
User/User group	The traffic of specified users or user groups matches the policy.	<ul style="list-style-type: none"> <li>● Click the drop-down list, and select a user or user group in the <b>To-be-selected</b> area. The selected user or user group is automatically added to the <b>Selected</b> area.</li> <li>● To add a user, click <b>Add User</b>.</li> </ul> [Example] UserGroup_1
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.	<ul style="list-style-type: none"> <li>● To add a one-off time plan, click <b>Add One-Off Time Plan</b>.</li> <li>● To add a cyclic time plan, click <b>Add Cyclic Time Plan</b>.</li> </ul> [Example] Any
Action Option	Action taken by the security policy to permit or deny the target data connection.	[Example] Permit

Item	Description	Remarks
Content Security	<p>Whether intrusion prevention and virus detection are enabled for the target data connection.</p> <p>If you want to enable content security check, you must specify the intrusion prevention and virus protection templates, and configure the actions.</p>	<p>The configuration of content security takes effect on only IPv4 traffic.</p> <p>[Example]</p> <ul style="list-style-type: none"> <li>● Intrusion Prevention: Enable</li> <li>● Virus Protection: Enable</li> <li>● URL Filtering: Not Enabled</li> </ul>
Advanced	<p>Advanced settings of the security policy, including:</p> <p><b>Long-Lived Connection:</b> applies to the special servers that require long-lived connections. After this function is enabled, the server's connection request is not restricted by the connection timeout setting of the firewall. The connection duration needs to be set.</p>	<p>Click <b>Settings</b>, and set parameters on the displayed <b>Advanced Option</b> page.</p> <p>[Example]</p> <p>Select <b>Long-Lived Connection</b>.</p>

(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.

<input type="checkbox"/>	Priority	Name	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count	Hit Session	Operation
▼ Default Policy Group													
<input type="checkbox"/>	1	allow_all	any	any	any	any	any	any	Perm		2600 Clear	View Details..	Edit Delete
<input type="checkbox"/>	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.

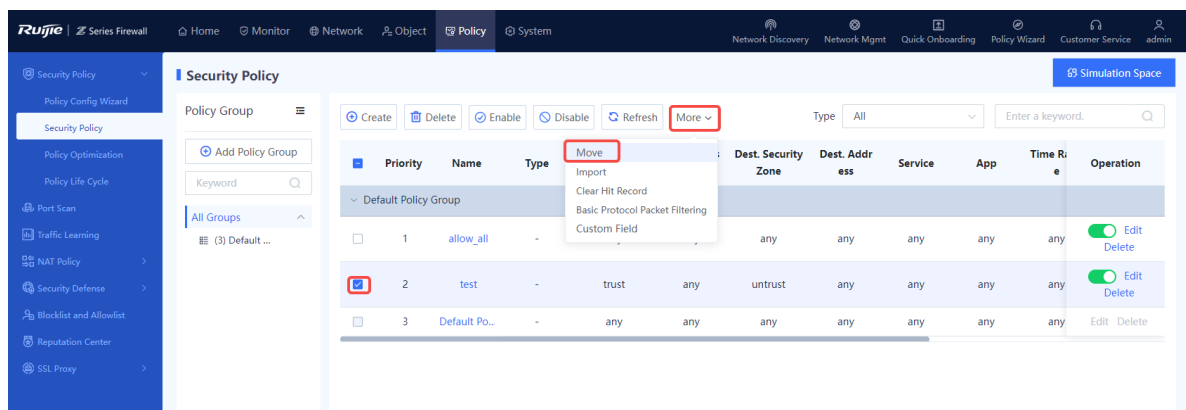
### **Note**

- 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.

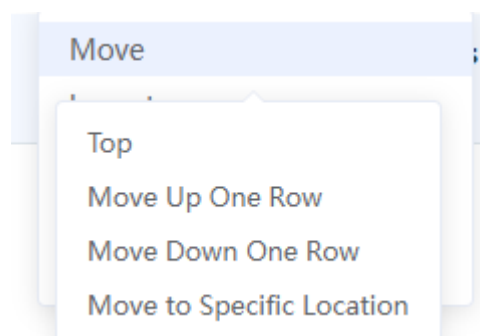
## Procedure

(1) Choose **Policy > Security Policy**.

(2) Select the policy of which the priority needs to be adjusted.



(3) Click **More** and select **Move**. Select the required operation from the shortcut menu to move the selected policy.



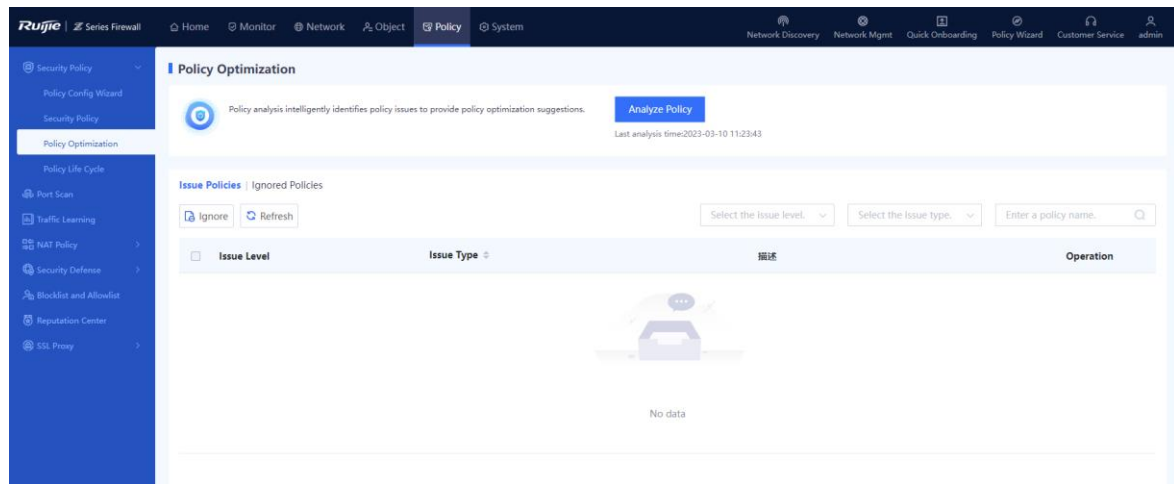
## 7.6.5 Optimizing Policy

### Application Scenario

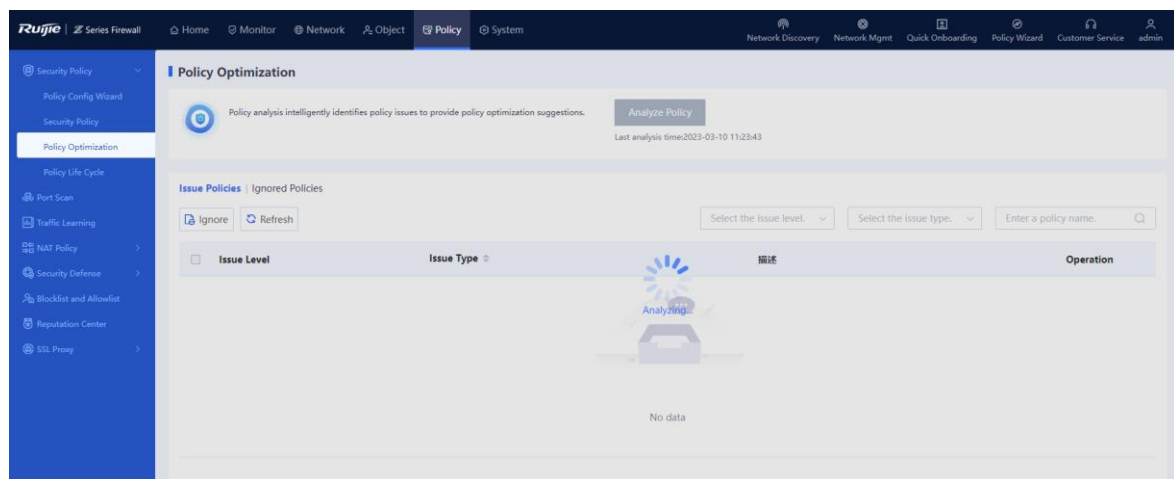
Affected by factors such as service accumulation and change of O&M personnel, the configuration complexity of security policies becomes increasingly high during the routine security policy O&M process. The policy optimization function of Z-S series firewalls can intelligently compare and analyze the 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**.



### (2) Click **Analyze Policy** to analyze the security policy.



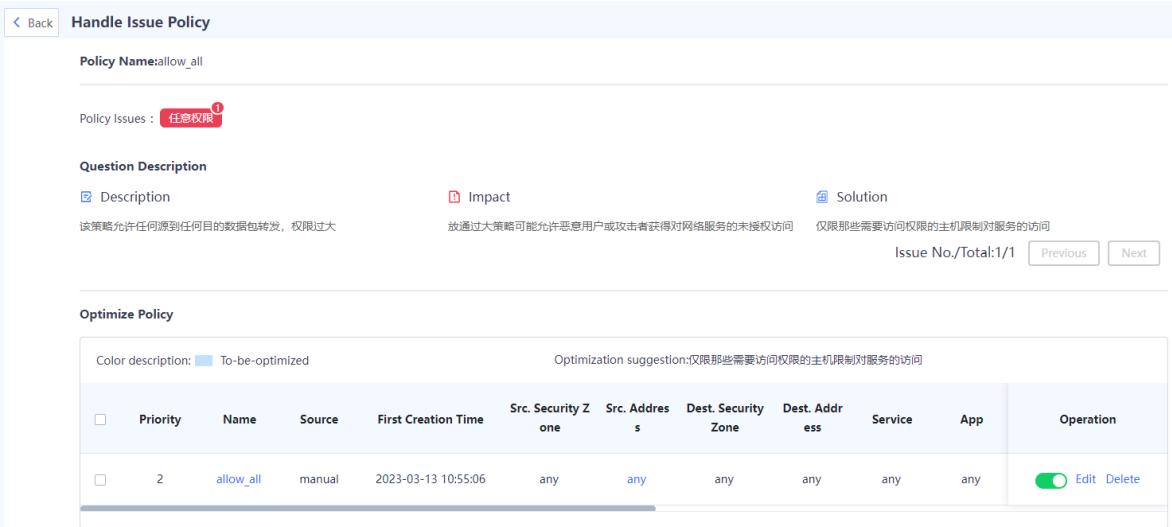
After analysis is completed, the system displays the issue policy list.



### 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.



**Handle Issue Policy**

Policy Name: allow\_all

Policy Issues : 任意权限<sup>1</sup>

**Question Description**

Description     Impact     Solution

该策略允许任何源到任何目的的数据包转发, 权限过大    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    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

<input type="checkbox"/>	Priority	Name	Source	First Creation Time	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Operation
<input type="checkbox"/>	2	allow_all	manual	2023-03-13 10:55:06	any	any	any	any	any	any	<input checked="" type="checkbox"/> 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

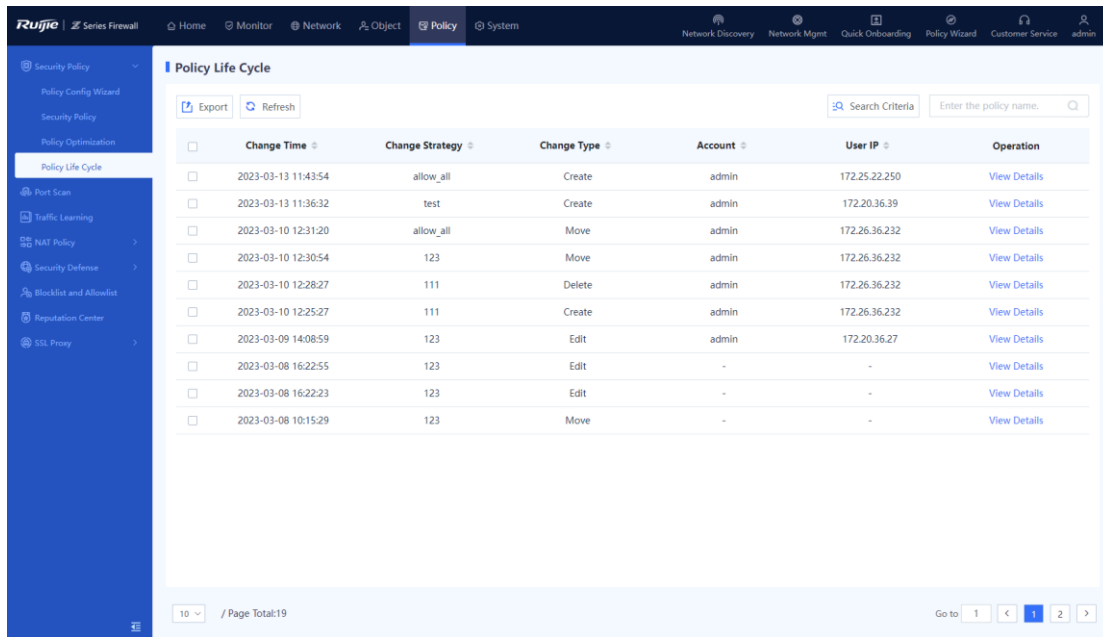
### Application Scenario

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.

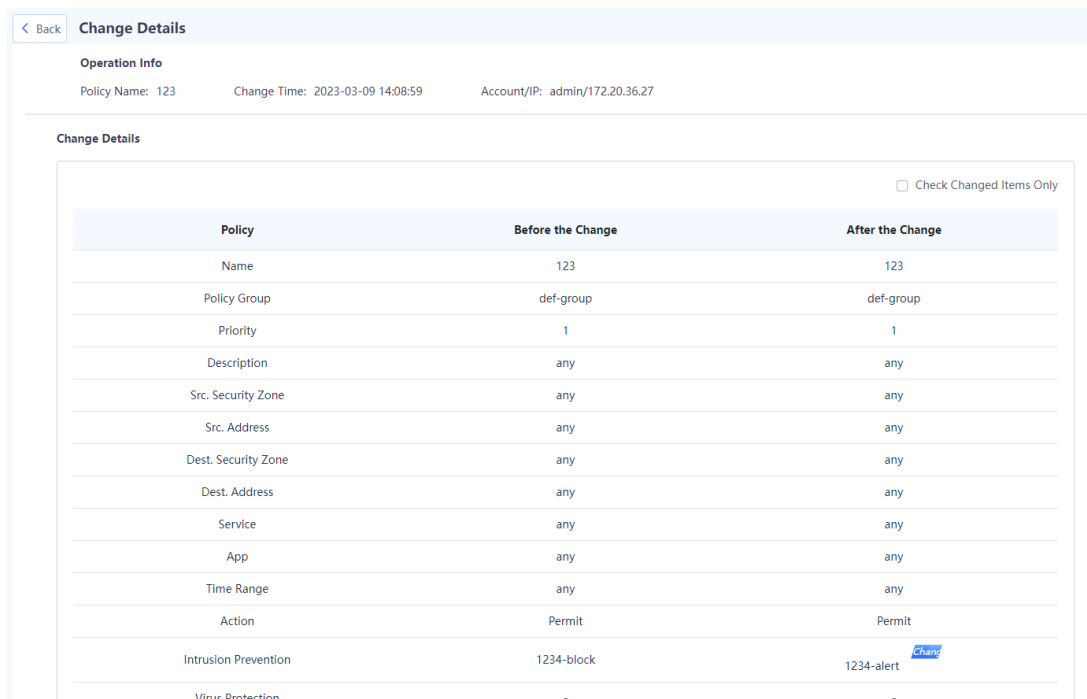
### Procedure

- (1) Choose **Policy > Security Policy > Policy Life Cycle**.





(2) Select the security policy you want to view. Click **View Details** in the **Operation** column.



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

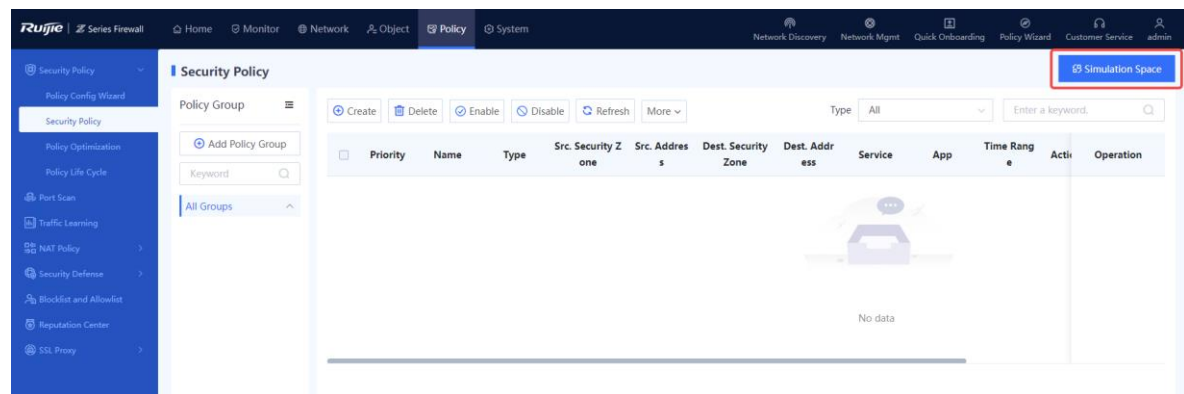
Affected by factors such as service accumulation and change of O&M personnel, the configuration complexity of security policies becomes increasingly high during the routine security policy O&M process. In the middle and late stages of O&M, if the security policy is modified improperly, the risk of service 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.

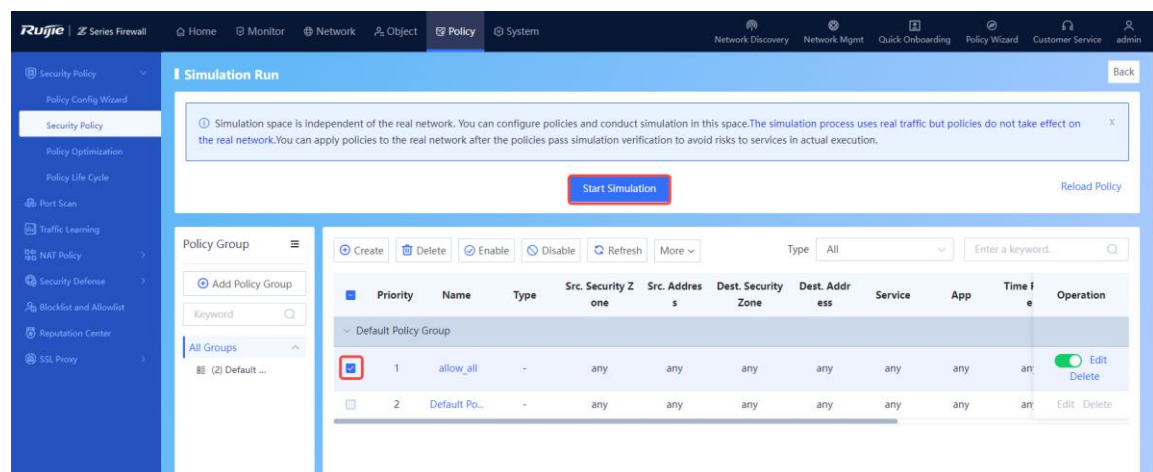
This function solves the problems such as service interruption caused by improper configuration in O&M, and provides O&M personnel with a test and verification environment, thus reducing O&M difficulty and risk, and lowering O&M costs.

## 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**.



- (4) In the **Set Simulation Duration** dialog box, set the duration of simulation run.

## Set Simulation Duration



Simulation Duration 1 Hour

Start Simulation

Cancel

(5) Click **Start Simulation**.

The system automatically performs simulation run for the selected policies.

The screenshot shows the 'Simulation Run' interface in the Ruijie Series Firewall management console. The main content area displays the following information:

- Simulation Run** (Back)
- Information: 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.
- Status: Running 32 Minute (planned duration: 1 hour)
- Buttons: Stop Simulation, Reload Policy, Apply to Real Network
- Message: You can leave this page temporarily and perform operations after the execution result is generated.

Below the simulation status, a table lists the policies being simulated:

Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Co-Unit	Operation
Default Policy Group												
1	test	-	trust	any	untrust	any	any	any	any	Deny		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	Deny		Edit, Delete

At the bottom of the table, a message indicates: 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:


- o The number of times traffic is permitted in the real policy but blocked in the simulated policy.
- o 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** ⊗

① Due to capacity limitations, only the details about the first 100,000 simulation results are recorded.

Refresh Clear Result

Src. Address	Actual Execution Result	Simulation Result	Hit Count in Actual Execution	Hit Count in Simulation	Details
 <p style="color: red; font-weight: bold;">No data</p>					

(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

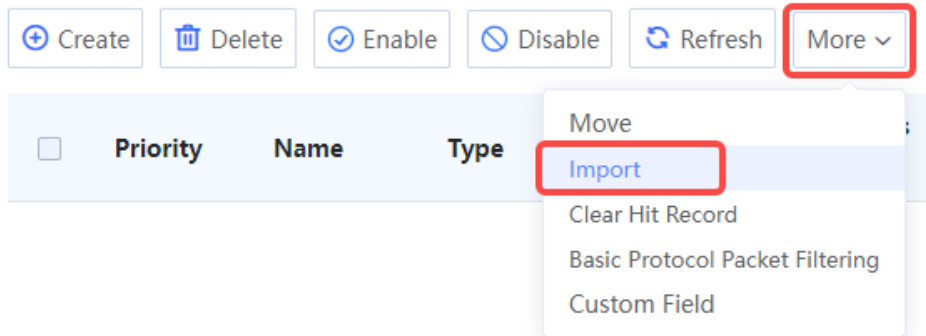
The security policies containing IPv6 addresses cannot be imported in a batch.

### 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** ⊗

① 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

OKCancel

- (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.

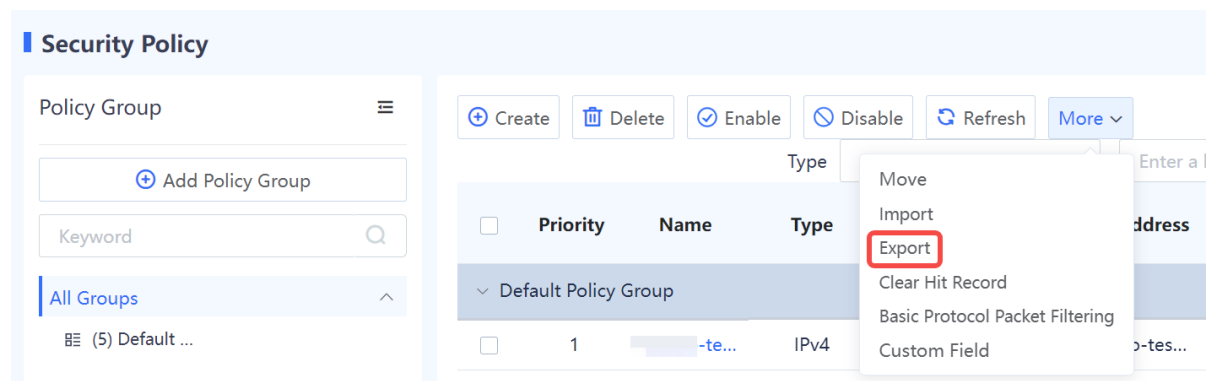
## 7.6.9 Exporting Security Policies

### Application Scenario

On the Z-S series firewall, you can export configured security policies. To configure security policies quickly, you can batch export the security policies, modify them, and then import them.

### Procedure

- (1) Choose **Policy > Security Policy > Security Policy**.
- (2) Click **More**. In the drop-down list, select **Export** to export all security policies on the device except the default policy.



## 7.6.10 Enabling Basic Protocol Packet Control

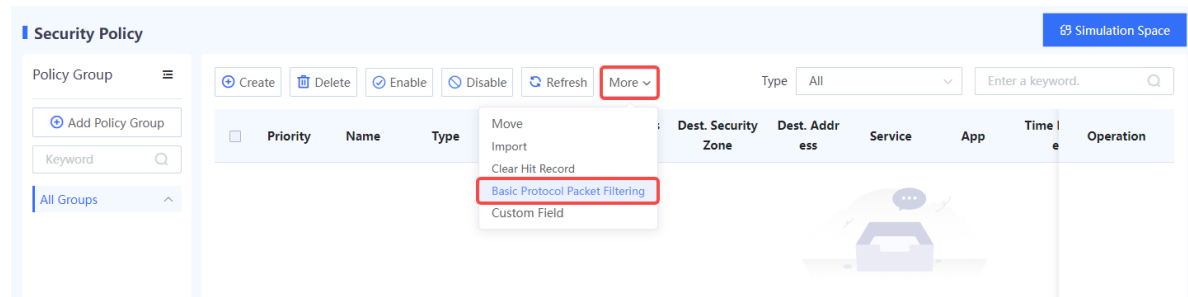
### Application Scenario

You can enable or disable the basic protocol packet control function of security policies.

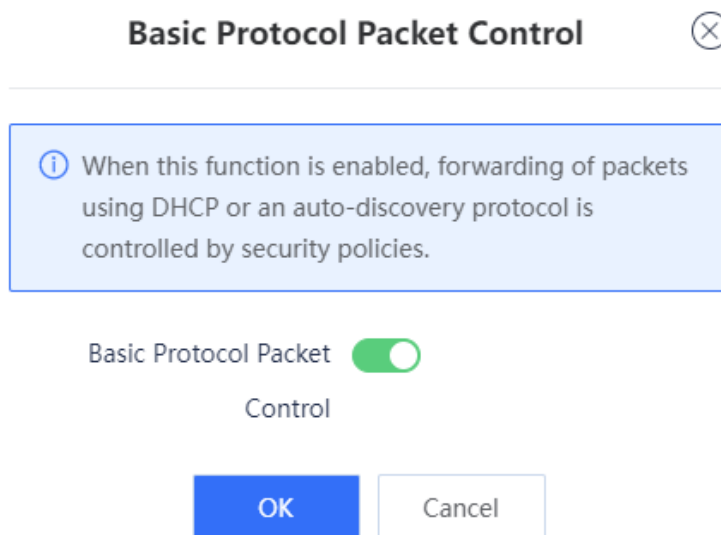
By default, the firewall does not perform security control on the network basic protocol packets (such as DHCP packets and auto-discovery protocol packets). It directly forwards these packets if no additional configurations are performed so that the device can quickly access the network. If you want 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**.



- (4) Click **OK**.

## 7.7 Traffic Control Policy

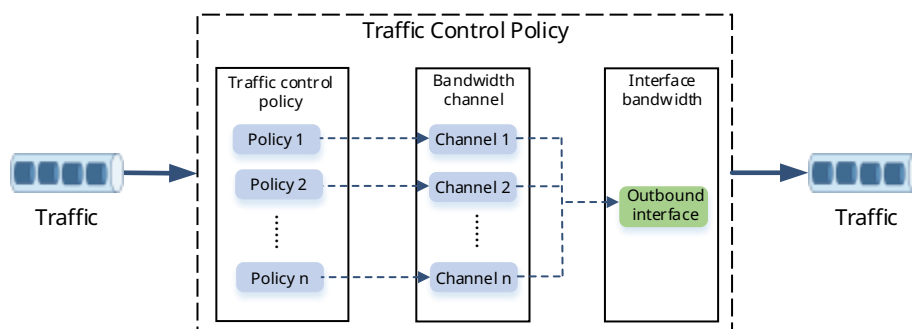
### 7.7.1 Overview

Traffic control enables a device to accurately manage and control user traffic based on source and destination addresses, services, applications, users and user groups. Different traffic control policies can be applied to different services to allocate egress bandwidth properly, thereby ensuring the normal running of key services.

As shown in the following figure, the device implements traffic control through traffic control policies, bandwidth channels, and line bandwidth (interface bandwidth).

- Traffic control policy: defines the matching conditions and processing actions for traffic, and references bandwidth channels.
- Bandwidth channel: specifies the uplink and downlink bandwidth resources to be referenced by traffic control policies.
- Line bandwidth: specifies the uplink and downlink bandwidth of the outbound interface.

The processing procedure of traffic control policies is as follows:



- (1) After a device receives traffic, the device matches the traffic against traffic control policies in the configured order until one policy is matched. If the traffic matches no policy, no traffic control action is performed.
- (2) The closer a policy is to the front, the higher its priority in matching. You can adjust the priority of a policy by moving its position.
- (3) If the traffic matches a policy, the device forwards the traffic based on the rate of the bandwidth channel referenced by the policy. If the actual traffic exceeds the maximum bandwidth set for the bandwidth channel, the excessive traffic is discarded.
- (4) When the traffic is sent out through the outbound interface, it is limited by the egress bandwidth. When traffic from multiple bandwidth channels is simultaneously forwarded by an interface and the actual traffic exceeds the interface bandwidth, the device forwards packets with higher priority first, such as packets configured with bandwidth guarantee. The device stores packets

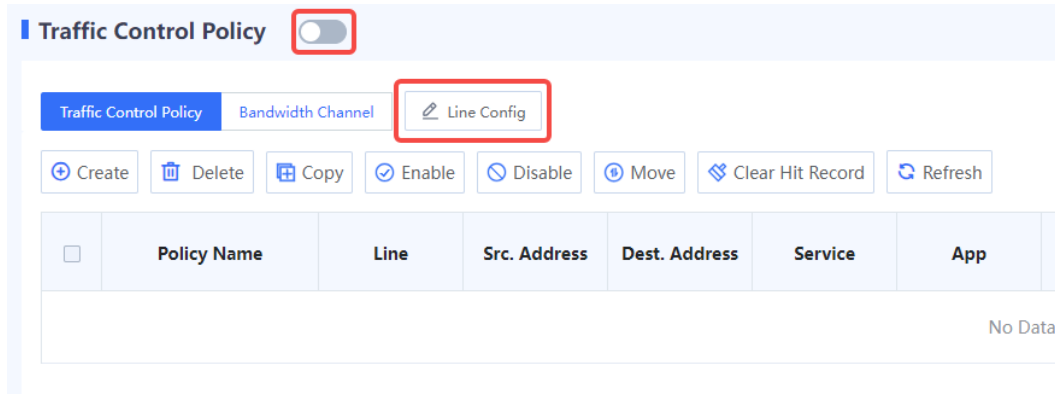


with lower priority in the buffer and sends them when the traffic is lower than the interface bandwidth limit. When the buffer is full, subsequent packets are discarded.

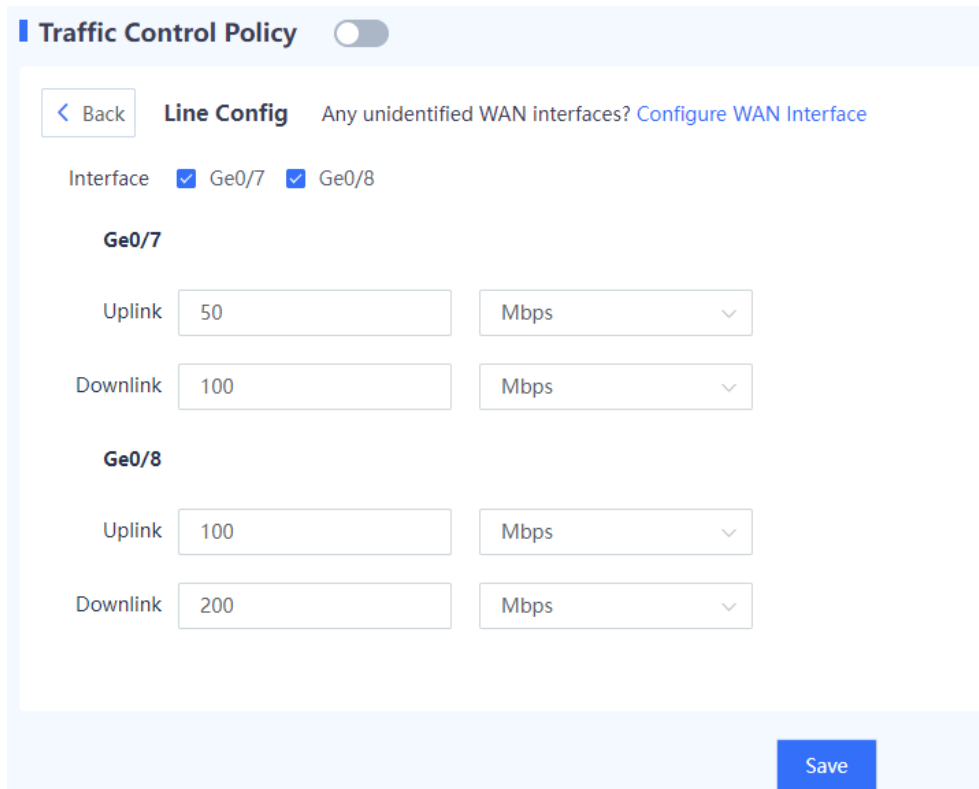
## 7.7.2 Configuring Traffic Control Policies

### 1. Configuring Egress Bandwidth

- (1) Choose **Policy > Traffic Control Policy**.
- (2) Toggle on  to enable traffic control.



- (3) Select an outbound interface and configure uplink and downlink bandwidth limits.



**Note**

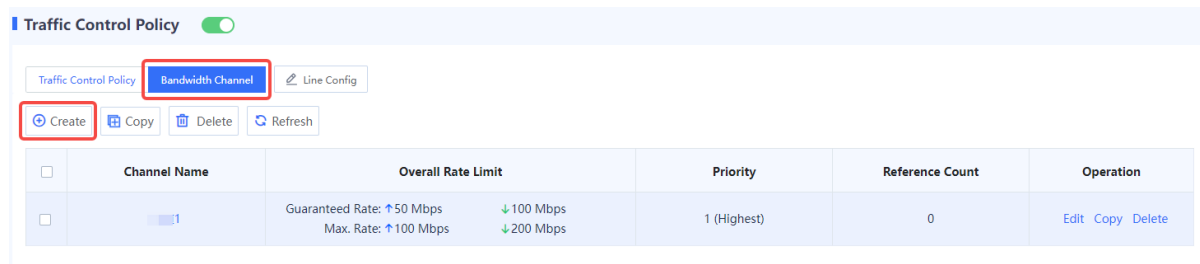
The outbound interface must be a WAN interface.

(4) Click **Save**.

## 2. Configuring Bandwidth Channels

(1) Choose **Policy > Traffic Control Policy**.

(2) Click the Bandwidth Channel. Click Create.



(3) Enter bandwidth channel name, uplink and downlink bandwidth limits and channel priority.

< Back

### Add Bandwidth Channel

**Basic Info**

\* Name

---

**Overall Rate Limit** ⓘ

Max. Uplink Rate  Mbps ▼

Guaranteed Uplink Rate  Mbps ▼

Max. Downlink Rate  Mbps ▼

Guaranteed Downlink Rate  Mbps ▼

Priority 4 (Medium) ▼

Save

Item	Description	Remarks
<b>Basic Info</b>		

Item	Description	Remarks
Name	Bandwidth channel name.	[Example] Channel 1
<b>Overall Rate Limit</b>		
Max. Uplink Rate	The maximum bandwidth resource available to the traffic transmitted over the channel. The excessive traffic is discarded. If the parameter is not specified, the traffic is not limited.	[Example] 10 Mbps
Guaranteed Uplink Rate	The minimum bandwidth resource available to the traffic transmitted over the channel. If the parameter is not specified, no bandwidth resource is guaranteed.	[Example] 10 Mbps
Max. Downlink Rate	The maximum bandwidth resource available to the traffic transmitted over the channel. The excessive traffic is discarded. If the parameter is not specified, the traffic is not limited.	[Example] 10 Mbps
Guaranteed Downlink Rate	The minimum bandwidth resource available to the traffic transmitted over the channel. If the parameter is not specified, no bandwidth resource is guaranteed.	[Example] 10 Mbps
Priority	Bandwidth channel priority. When traffic from multiple bandwidth channels is simultaneously forwarded by an interface and traffic congestion occurs on the interface, the device forwards traffic from channels with higher priority first.	[Example] 1

(4) Click **Save**.

### 3. Configuring Traffic Control Policies

(1) Choose **Policy > Traffic Control Policy**.

(2) Click **Traffic Control Policy**. Click **Create**.

**Traffic Control Policy** ●

Traffic Control Policy Bandwidth Channel Line Config

<input type="checkbox"/>	Policy Name	Line	Src. Address	Dest. Address	Service	App
No Data						

(3) Configure the following information for a traffic control policy.

[Back](#) **Add Traffic Control Policy**

**Basic Info**

\* Name

Enabled State  Enable  Disable

---

**Line**

Line

---

**Src. and Dest.**

Src. Address

Dest. Address

---

**Services and Apps**

Service

App

**User/User Group**

User/User Group

---

**Action Execution**

Action  Limit  No Rate Limit  Block

\* Bandwidth  [Add Bandwidth Channel](#)

Channel

**Time Range**

Time Range  [Add One-Off Time Plan](#) [Add Cyclic Time Plan](#)

[Save](#)

Item	Description	Remarks
<b>Basic Info</b>		
Name	Name of the traffic control policy	[Example] Policy_1
Enabled State	Whether to enable the new traffic control policy	[Example] Enable
Line	Select the outbound interface to forward the traffic matching the policy.	[Example] Ge0/7
Policy position	Move the new policy above or below the specified policy. The closer a policy is to the front, the higher its priority in matching.	-
<b>Src. and Dest.</b>		
Src. Address	The packets with specified source IP addresses match the policy.	[Example] Any
Dest. Address	The packets with specified destination IP addresses match the policy.	[Example] Any
<b>Services and Apps</b>		

Item	Description	Remarks
Service	The traffic of specified services matches the policy.	[Example] Any
App	The traffic of specified applications matches the policy.	[Example] Any
<b>User/User Group</b>		
User/ User Group	The traffic of specified users or user groups matches the policy.	[Example] UserGroup_1
<b>Action Execution</b>		
Action	<p>The action the device performs for the traffic matching the policy.</p> <ul style="list-style-type: none"> <li>● Limit: The device forwards the packets based on the bandwidth limits configured for the selected bandwidth channel.</li> <li>● No Rate Limit: The device does not limit the traffic and forwards the packets.</li> <li>● Block: The device discards packets to block the service traffic.</li> </ul>	-
<b>Time Range</b>		
Time Range	Effective time range.	[Example] Any

(4) Click **Save**.

## 7.8 DHCP Management

### 7.8.1 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.

## 7.8.2 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**.

[Back](#) **Create DHCP Service**

Protocol Type  Ipv4  Ipv6

**Basic Info**

\* Interface

\*  IP Assignment Range

\* Subnet

\* Default Gateway

\* Primary DNS Server  [Use System DNS Settings](#)

Secondary DNS Server

[Advanced](#)

☰ **Advanced**

\* Lease Time  Day  Hour  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.	<ul style="list-style-type: none"> <li>● Enter an IP address range per line.</li> <li>● Connect the start IP address and end IP address with a hyphen (-).</li> </ul> [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 service to the terminals, which obtain IP addresses.	[Example] 255.255.255.0



Item	Description	Remarks
Primary DNS Server	Preferred DNS server used by the DHCP service.	Click <b>Use System DNS Settings</b> . 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
<b>Advanced</b>		
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.	<ul style="list-style-type: none"> <li>● The lease period ranges from 3 minutes to 365 days.</li> <li>● The default lease period is 1 hour.</li> </ul> [Example] 1 hour
Reserved IP Address/Range	Reserved IP addresses in the <b>IP Assignment Range</b> .	[Example] 192.168.1.2
Binding Host MAC	Static bindings between the pre-assigned IP addresses specified by <b>IP Assignment Range</b> and the MAC addresses of the clients.  When receiving a request	The value is in the format of IP address/MAC address, where the IP address should be a pre-assigned address in the <b>IP Assignment Range</b> . Enter one binding entry per line.  [Example]

Item	Description	Remarks
	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.	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**.

**Create DHCP Service**

Protocol Type  Ipv4  Ipv6

**Basic Info**

\*  Select an interface.

\* Primary DNS Server  Enter the DNS server address.

Secondary DNS Server

\* Lease Time  Day  Hour  Minute

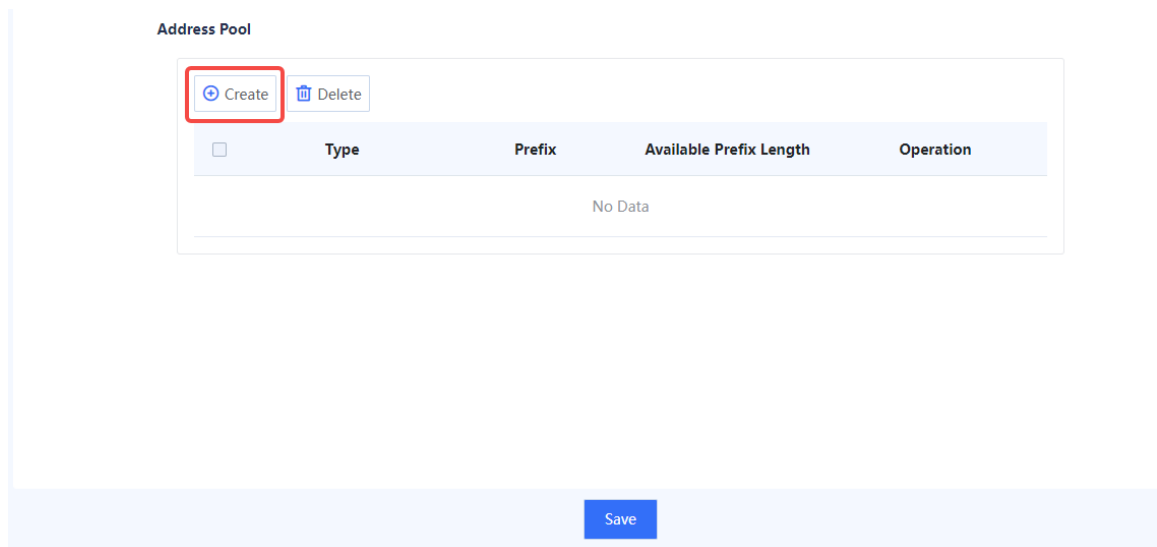
**Address Pool**

<input type="checkbox"/>	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 instability, the IP addresses are reclaimed after the lease expires. When the terminal devices recover connectivity, they will request the addresses again.	[Example] 1 hour

c In the **Address Pool** area, click **Create**.



d Select the address type and enter an available address prefix and length, and click **OK**.

### Create Address Pool ⊗

---

\* Type  Network Address  Prefix

\* Prefix

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.

### 7.8.3 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.

## 7.9 Blocklist and Allowlist

### 7.9.1 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.

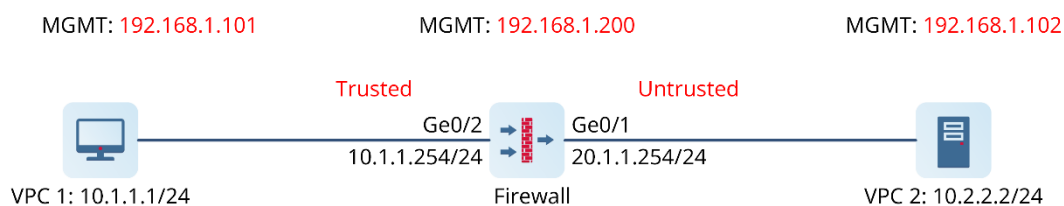
---

- 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.

### 7.9.2 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.)

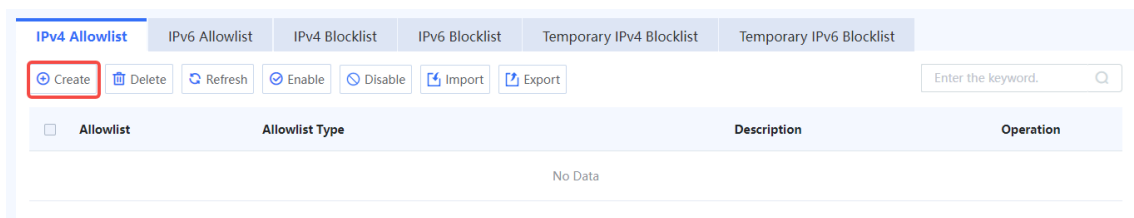
### 7.9.3 Creating an IPv4 Allowlist

#### Application Scenario

Configure an IPv4 allowlist on the web UI.

#### Procedure

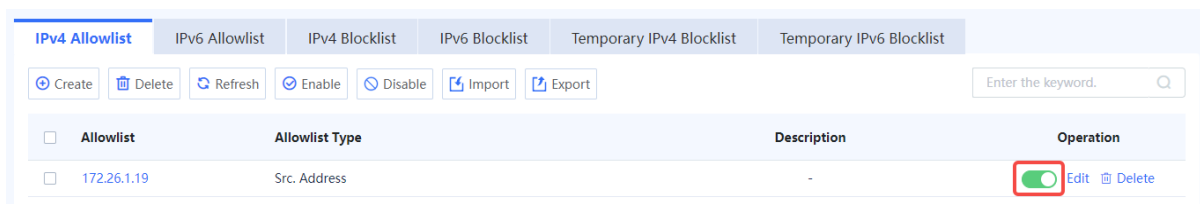
- (1) Access the **Add Allowlist** page.
  - a Choose **Policy > Blocklist and Allowlist > IPv4 Allowlist**.
  - b Above the operation area, click **Create**.



- (2) Set parameters for the allowlist policy and click **Save**.

Item	Description	Remarks
Allowlist Type	Type of the allowlist: <ul style="list-style-type: none"> <li>● <b>Src. Address:</b> Permit packets sent from this address.</li> <li>● <b>Dest. Address:</b> Permit packets sent to this address.</li> </ul>	[Example] Src. Address
IP Address/Range	Allowlist IP address/range.	The following two formats are supported: <ul style="list-style-type: none"> <li>● Single IP address: 192.168.1.1</li> <li>● IP address range: 192.168.1.1-192.168.1.10</li> </ul>

(3) Toggle on the switch in the **Operation** column to enable the allowlist.



### 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.

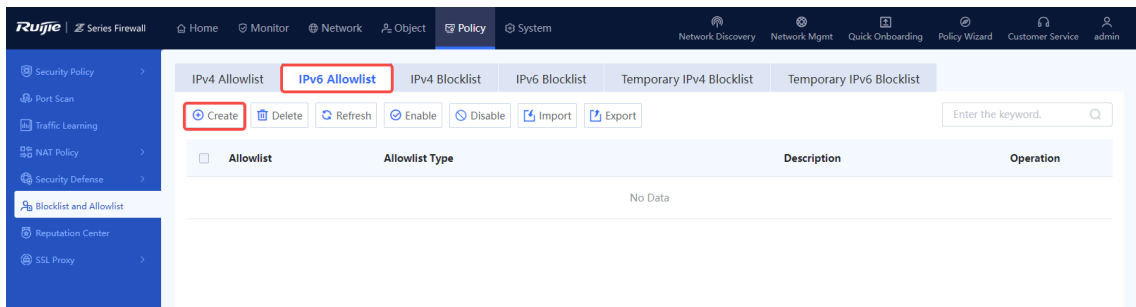
## 7.9.4 Creating an IPv6 Allowlist

### 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**.



- (2) Set parameters for the allowlist policy and click **Save**.

**Add Allowlist**

IP Type IPv6

Allowlist Type  Src. Address  Dest. Address

\*

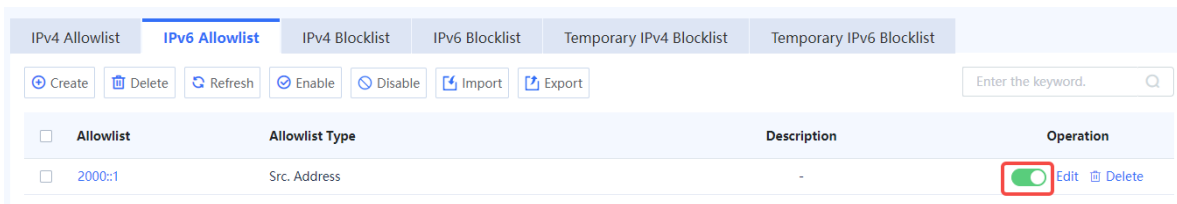
Description

Item	Description	Remarks
Allowlist Type	Type of the allowlist: <ul style="list-style-type: none"> <li>● <b>Src. Address:</b> Permit packets sent from this address.</li> <li>● <b>Dest. Address:</b> Permit packets sent to this address.</li> </ul>	[Example] Src. Address
IP Address/Range	Allowlist IP	The following two formats are



Item	Description	Remarks
	address/range.	supported: <ul style="list-style-type: none"> <li>● Single IP address: 1234::100</li> <li>● IP address range: 1234::100-2345::100</li> </ul>

(3) Toggle on the switch in the **Operation** column to enable the allowlist.



**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.

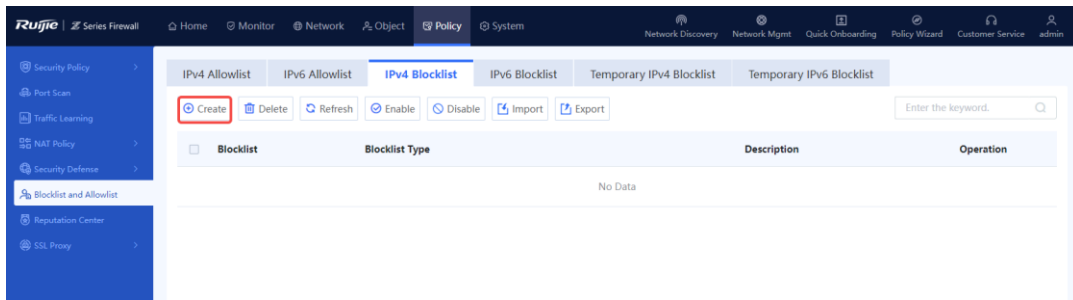
**7.9.5 Creating an IPv4 Blocklist**

**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**.



(2) Set parameters for the blocklist policy and click **Save**.

[Back](#) **Add Blocklist**

IP Type IPv4

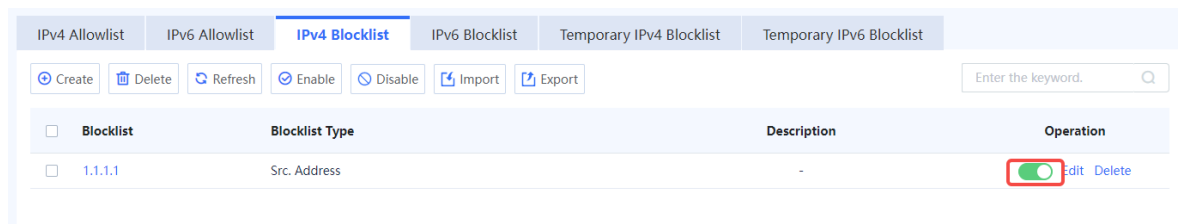
Blocklist Type  Src. Address  Dest. Address

\*  IP Address/Range

Description

Item	Description	Remarks
Blocklist Type	Type of the blocklist: <ul style="list-style-type: none"> <li>● <b>Src. Address:</b> Block packets sent from this address.</li> <li>● <b>Dest. Address:</b> Block packets sent to this address.</li> </ul>	[Example] Src. Address
IP Address/Range	Blocklist IP address/range.	The following two formats are supported: <ul style="list-style-type: none"> <li>● Single IP address: 192.168.1.1</li> <li>● IP address range: 192.168.1.1-192.168.1.10</li> </ul>

(3) Toggle on the switch in the **Operation** column to enable the blocklist.



### 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.

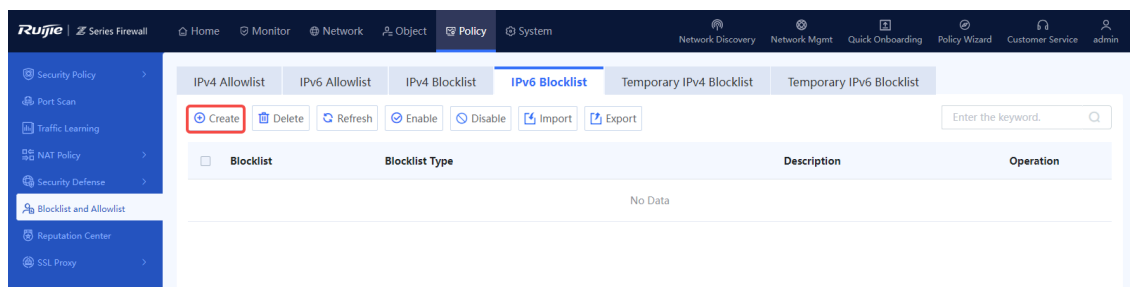
## 7.9.6 Creating an IPv6 Blocklist

### 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**.

[< Back](#)

## Add Blocklist

IP Type IPv6

Blocklist Type  Src. Address  Dest. Address

\* ⓘ IP Address/Range

Description

Item	Description	Remarks
Blocklist Type	Type of the blocklist: <ul style="list-style-type: none"> <li>● <b>Src. Address:</b> Block packets sent from this address.</li> <li>● <b>Dest. Address:</b> Block packets sent to this address.</li> </ul>	[Example] Src. Address
IP Address/Range	Blocklist IP address/range.	The following two formats are supported: <ul style="list-style-type: none"> <li>● Single IP address: 1234::100</li> <li>● IP address range: 1234::100-2345::100</li> </ul>

(3) Toggle on the switch in the **Operation** column to enable the blocklist.

IPv4 Allowlist
IPv6 Allowlist
IPv4 Blocklist
IPv6 Blocklist
Temporary IPv4 Blocklist
Temporary IPv6 Blocklist

[Create](#)
[Delete](#)
[Refresh](#)
[Enable](#)
[Disable](#)
[Import](#)
[Export](#)
Enter the keyword. Q

	Blocklist	Blocklist Type	Description	Operation
<input type="checkbox"/>	2003::1	Src. Address	-	<input checked="" type="checkbox"/> <a href="#">Edit</a> <a href="#">Delete</a>

### 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.

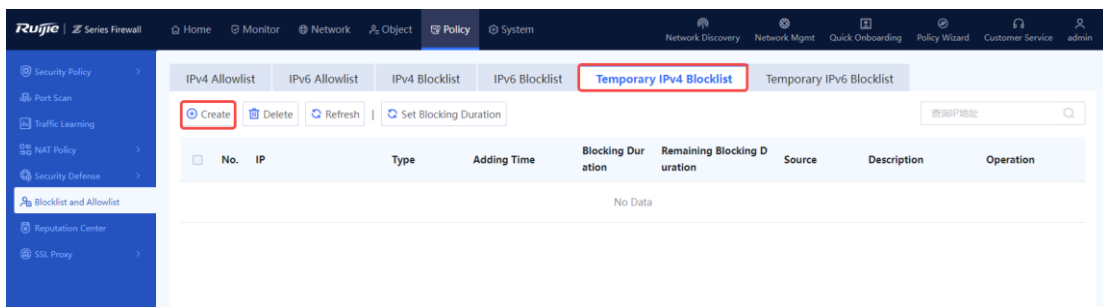
## 7.9.7 Creating a Temporary IPv4 Blocklist

### 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**.



- (2) Set parameters for the blocklist policy and click **Save**.

< Back

### Add Temporary Blocklist

IP Type  IPv4

Blocklist Type  Src. Address  Dest. Address

\*

Blocking Duration   (Range: 3 min to 15 days)

Description

Item	Description	Remarks
Blocklist Type	Type of the temporary blocklist: <ul style="list-style-type: none"> <li>● <b>Src. Address:</b> Block packets sent from this address.</li> <li>● <b>Dest. Address:</b> Block packets sent to this address.</li> </ul>	[Example] Src. Address
IP Address/Range	Temporary blocklist IP address/range.	The following two formats are supported: <ul style="list-style-type: none"> <li>● Single IP address: 192.168.1.1</li> <li>● IP address range: 192.168.1.1-192.168.1.10</li> </ul>
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**.

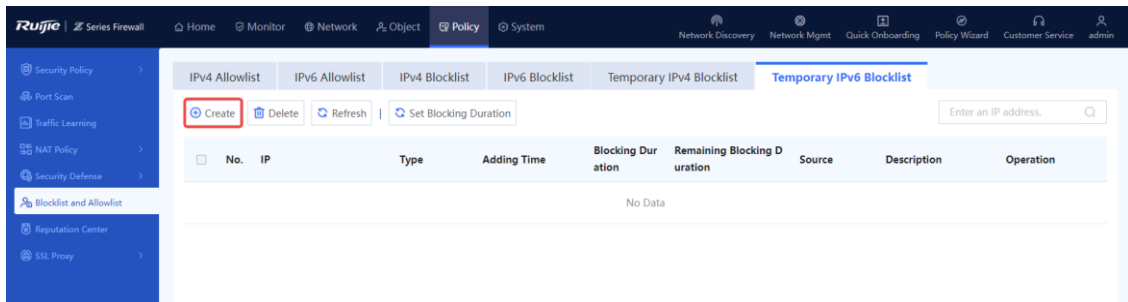
## 7.9.8 Creating a Temporary IPv6 Blocklist

### 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  Minute (Range: 3 min to 15 days)

Description

Item	Description	Remarks
Blocklist Type	Type of the temporary blocklist: <ul style="list-style-type: none"> <li>● <b>Src. Address:</b> Block packets sent from this address.</li> <li>● <b>Dest. Address:</b> Block packets sent to this address.</li> </ul>	[Example] Src. Address
IP Address/Range	Temporary blocklist IP address/range.	The following two formats are supported: <ul style="list-style-type: none"> <li>● Single IP address: 1234::100</li> <li>● IP address range: 1234::100-2345::100</li> </ul>

Item	Description	Remarks
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**.

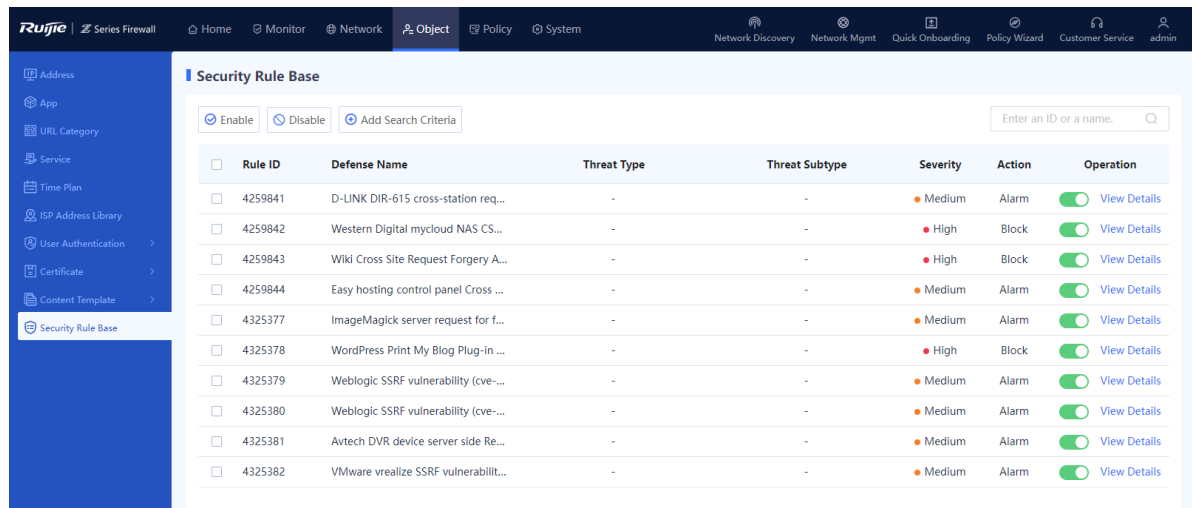
## 7.10 Security Rule Base Management

**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**.





(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.

## 7.11 Connecting to Ruijie Cloud

### 7.11.1 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.

---

### 7.11.2 Connecting to Ruijie Cloud

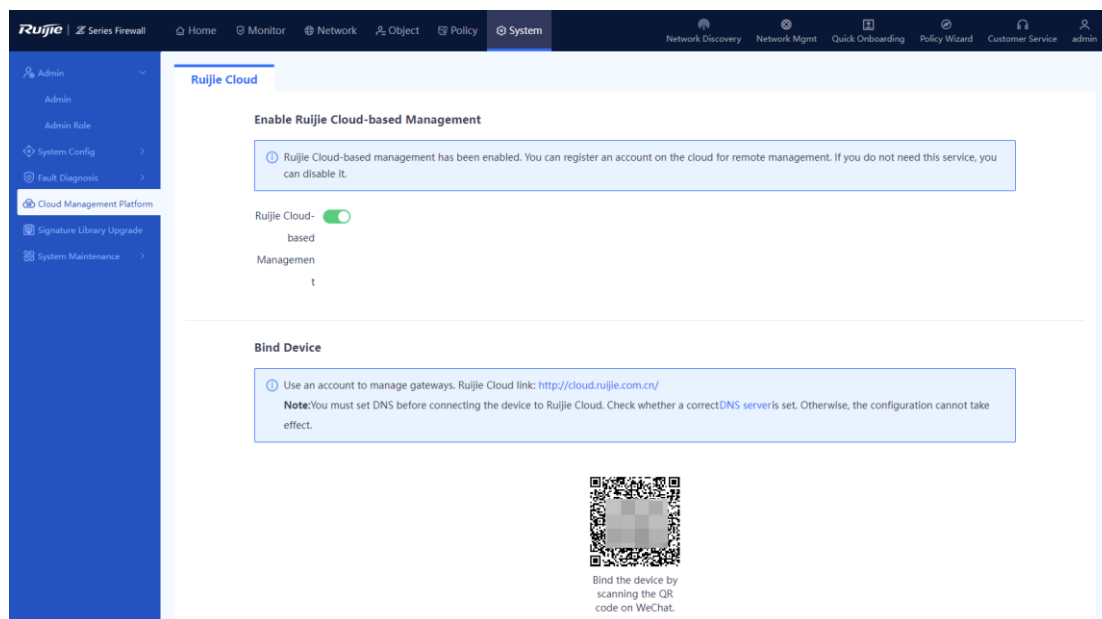
#### 1. Enabling Ruijie Cloud

##### 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.



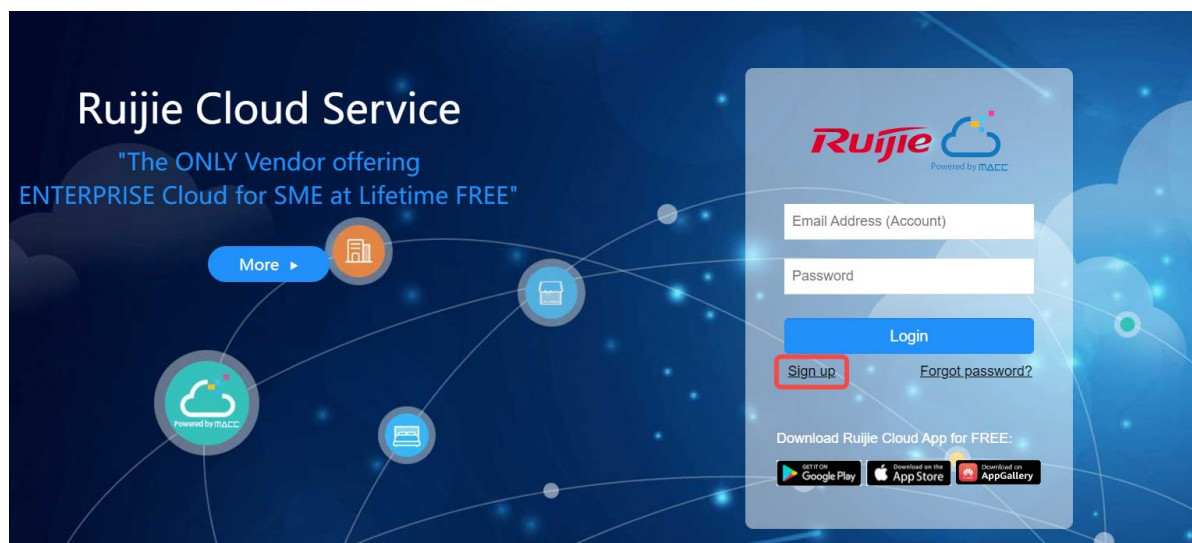
## 2. Binding Devices

### 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****Follow-up Procedure**

After the firewall is bound, the web page prompts you that the firewall has been bound to the related account.



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](#)

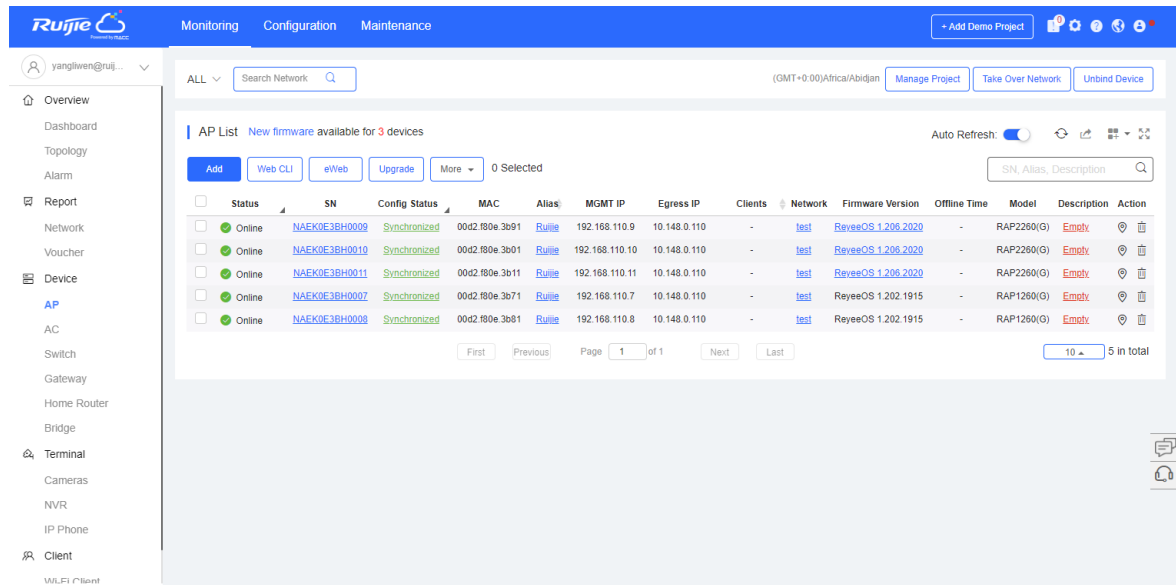
**7.11.3 Operations on Ruijie Cloud****1. Viewing Device Information****Application Scenario**

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**

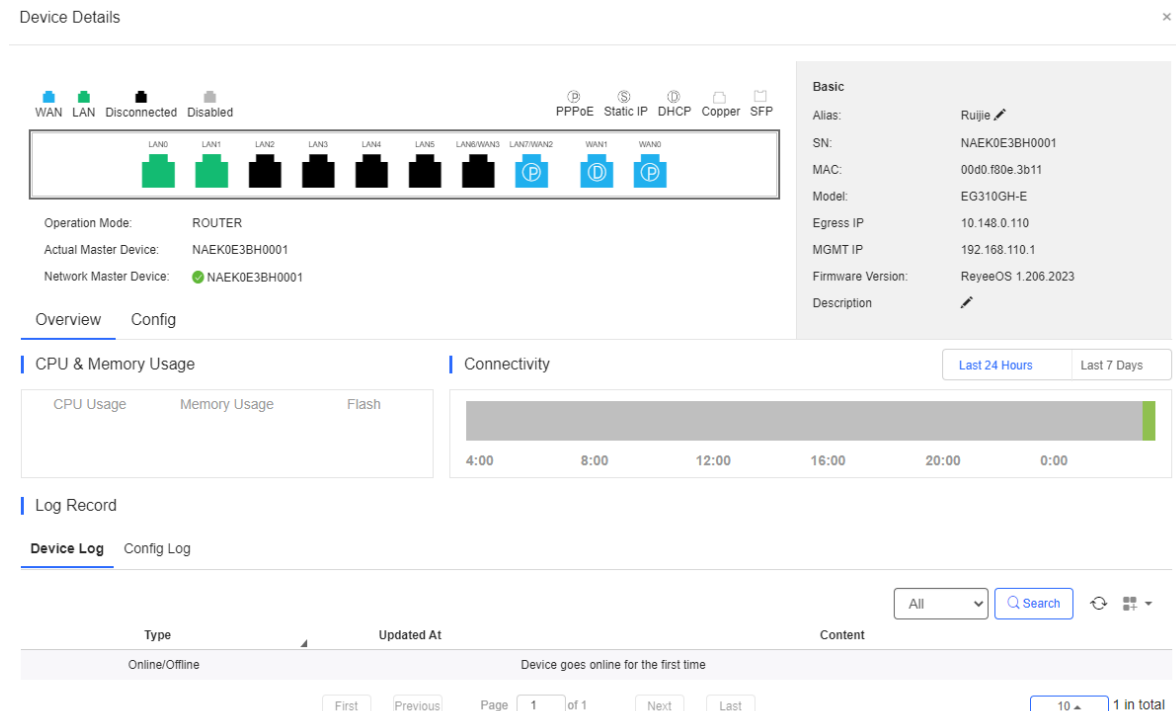
- (1) Choose **Monitoring > Device > Firewall** to open the device list.
- (2) View device details.

Figure 7-6 Firewall Details



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.



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

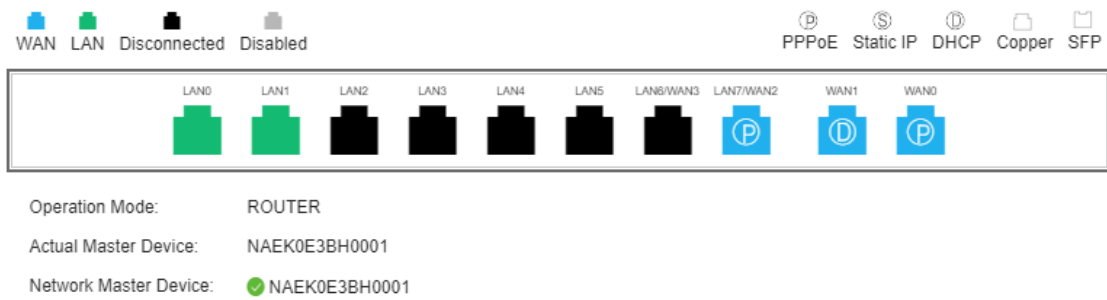
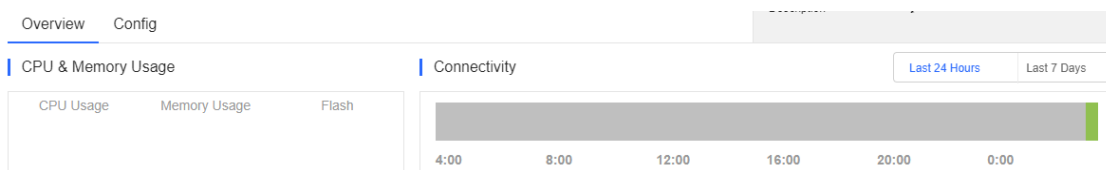


Figure 7-8 Basic Information



Figure 7-9 Status Information



**Figure 7-10 Interface Information**



## 2. Managing Tunnels

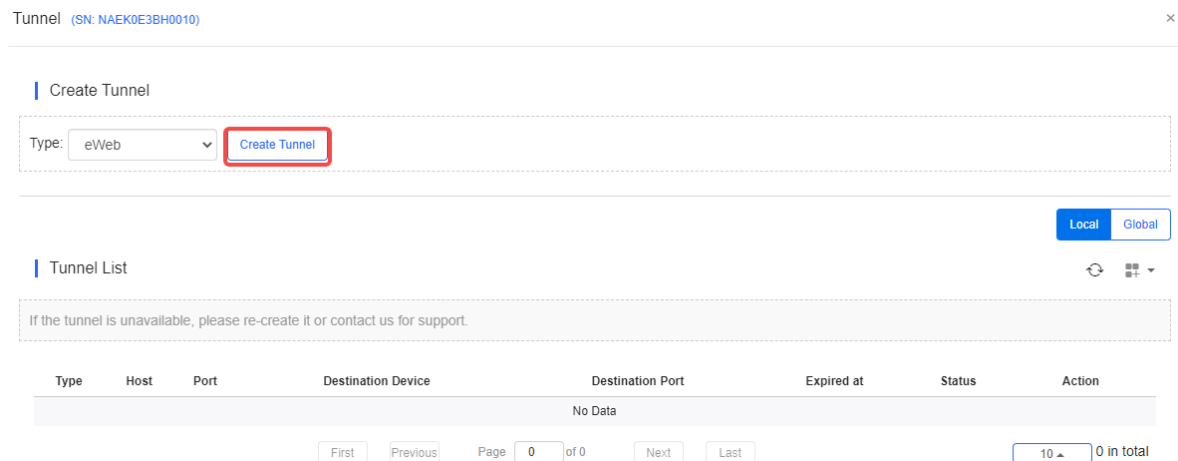
(1) Click **Tunnel** or **eWeb** to access the EWEB page of the device.

**Figure 7-11 Tunnel Management**



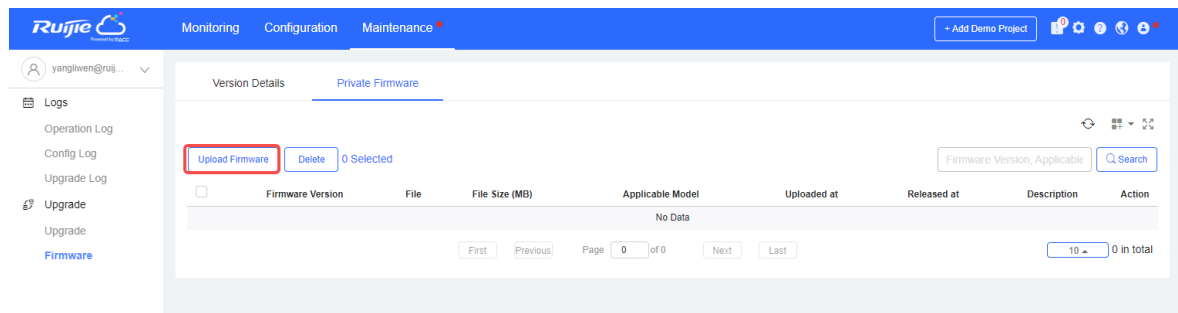
(2) To add a tunnel, click **Create Tunnel**.

**Figure 7-12 Creating a Tunnel**

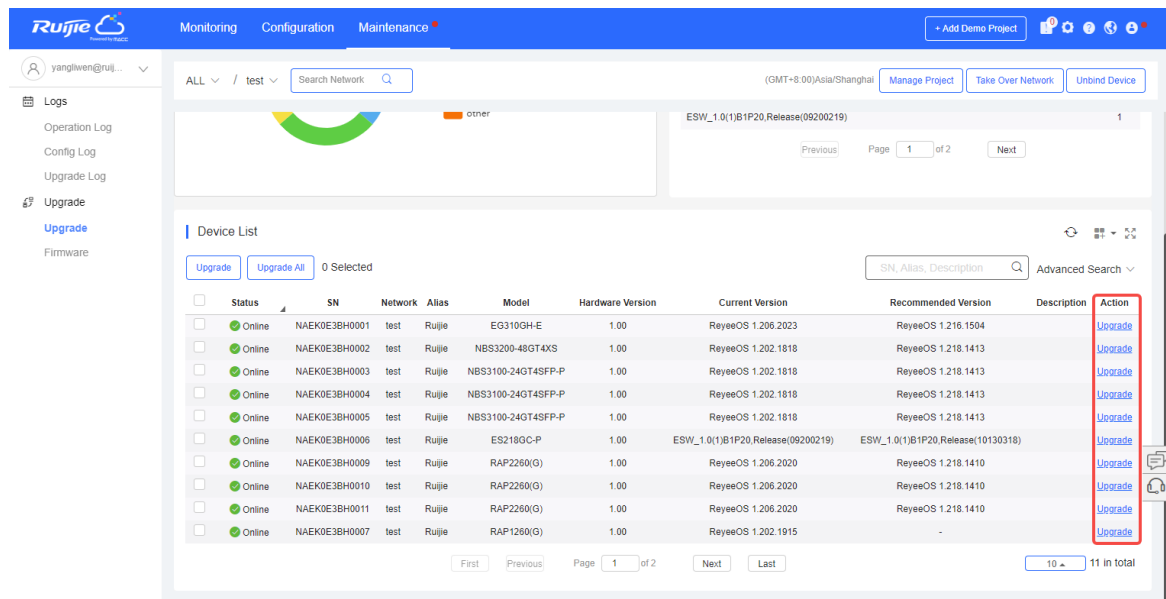


### 3. Upgrading Device Software/Firmware

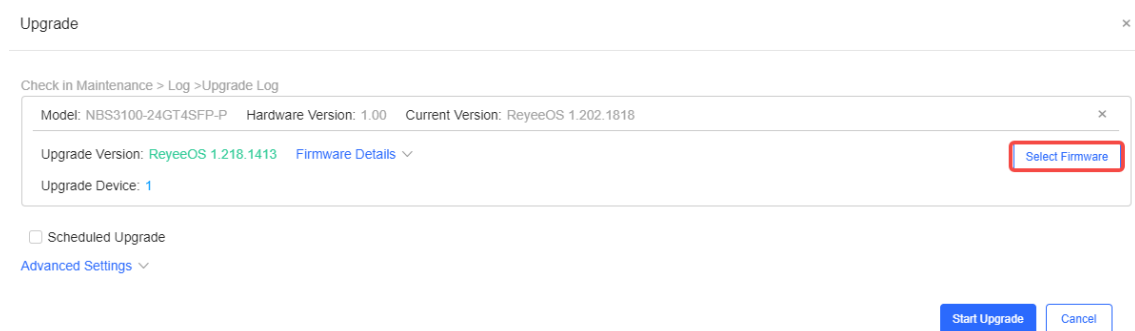
- (1) Choose **Maintenance > Upgrade > Firmware > Private Firmware**.
- (2) Click **Upload Firmware** to upload the software version/firmware version.



- (3) Choose **Maintenance > Upgrade > Upgrade**, find out the device to be upgraded in **Device List**, and click **Upgrade**.



(4) Click **Select Firmware** to select the upgrade package file to be uploaded.

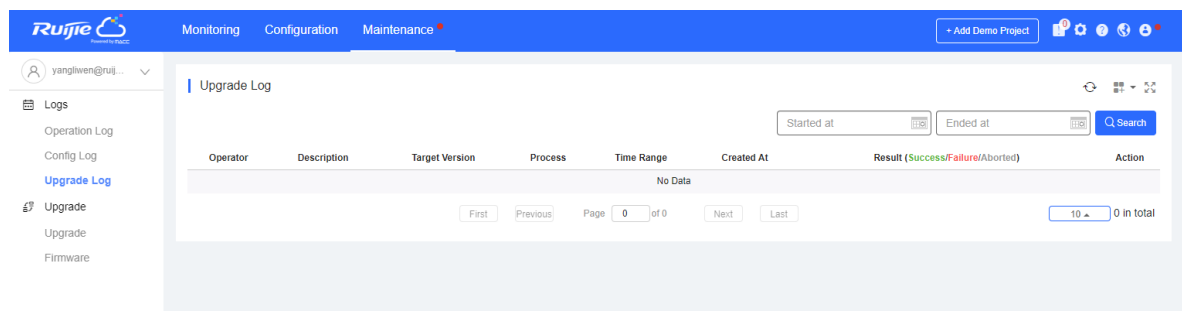


(5) Click **Start Upgrade** to start the upgrade.

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**





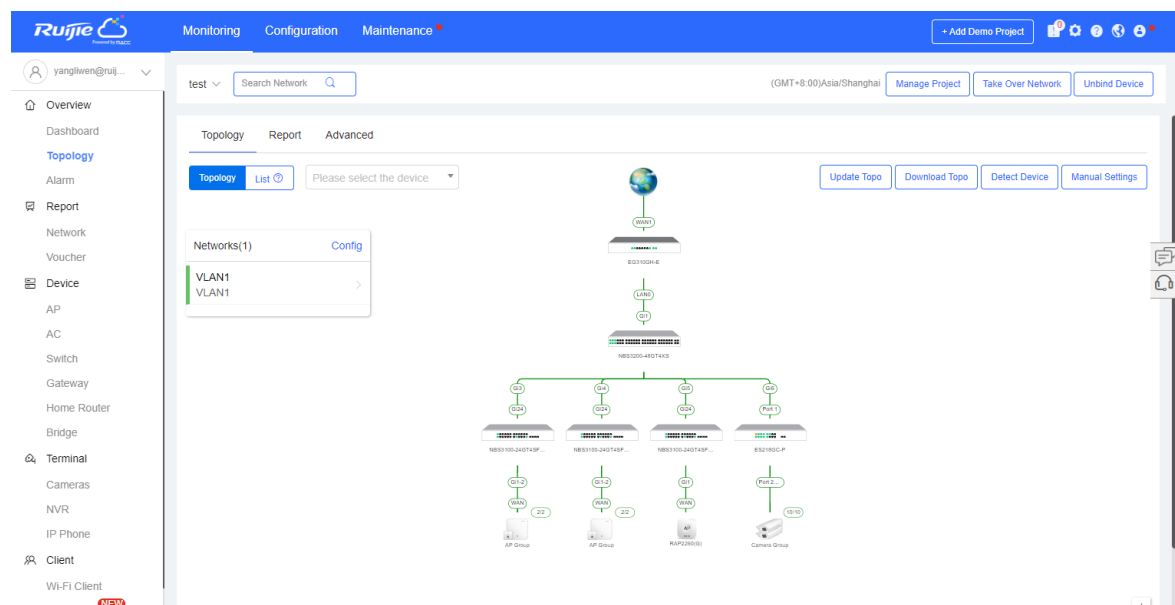
## 4. Viewing Network Topology

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**.

## 7.12 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.

## 7.13 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.

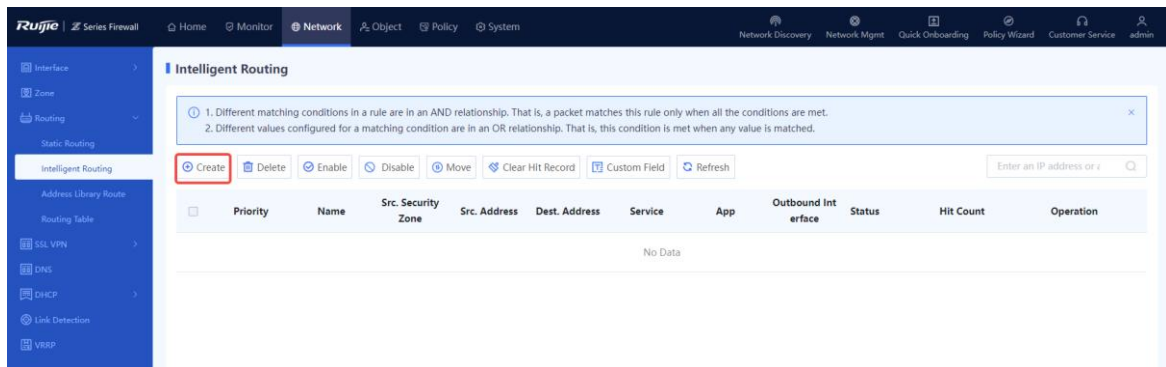
In a multi-path scenario where no routing rules are configured, if the device is connected to different service networks through different paths, the traffic will be evenly routed over the paths. In this situation, the access data to service networks may be incorrectly sent to other networks, causing 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.



- (3) Set parameters of intelligent routing.

**Create Intelligent Routing**

**Basic Info**

\* Name

Enabled State  Enable  Disable

Adjacent Policy

Description

---

**Matching Conditions**

\* Src. Security Zone

\* Src. Address

\* Dest. Address

\* Service

\* App

\* Time Range   Add One-Off Time Plan  Add Cyclic Time Plan Select a time range.

---

**Action Settings**

Action Option  Forwarding  No Intelligent Routing

\* Outbound Interface

Next-Hop Address

Link Detection

**Save**

Item	Description	Remarks
Basic Info		
Name	Name of intelligent routing.	Characters such as `~!#%^&*+V0:."/<>? 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 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.	<ul style="list-style-type: none"> <li>● Click the drop-down list, and select a source security zone in the <b>To-be-selected</b> area. The selected zone is automatically added to the <b>Selected</b> area.</li> <li>● Click <b>Add Security Zone</b> to add a custom security zone.</li> </ul> [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 <b>To-be-selected</b> area. The selected address is automatically added to the <b>Selected</b> area. [Example]

Item	Description	Remarks
		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 <b>To-be-selected</b> area. The selected address is automatically added to the <b>Selected</b> area.  [Example]  Any
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 <b>Outbound Interface</b> and <b>Next-Hop Address</b> .	[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 <a href="#">7.16 Link Detection</a> .

(4) Click **Save**.

## 7.14 Address Library Routing (ISP-based Routing)

### 7.14.1 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.

### 7.14.2 Configuring an ISP Address Library

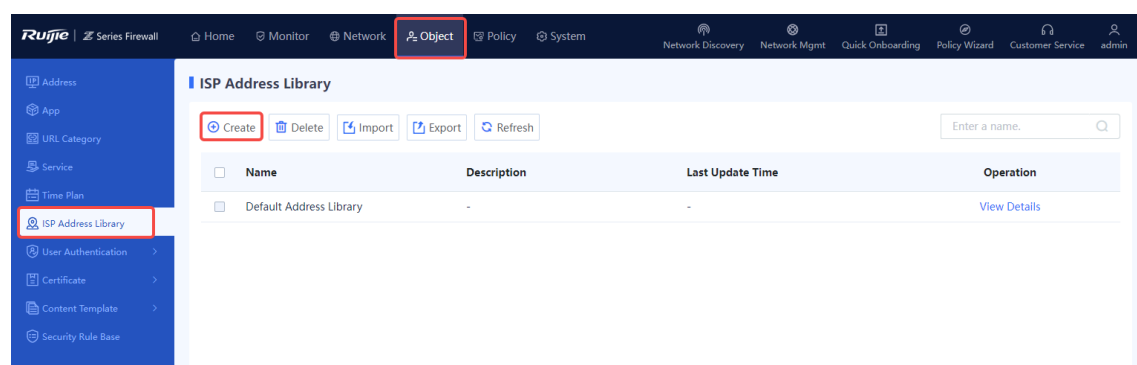
#### 1. Creating an ISP Address Library Manually

##### 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**.



- (2) Set parameters of the ISP address library.

< Back
**Create ISP Address Library**

\* Name

Description

---

\* ISP Address List

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 <b>Create</b> to enter a single IP address or an IP address range. Three configuration methods are supported: <ul style="list-style-type: none"> <li>● IP address: One or multiple IP addresses. Input an IP address per line. Press <b>Enter</b> to separate lines. Example: 192.168.20.3</li> <li>● IP address range: A contiguous range of addresses. Connect the start IP address and end IP address with a hyphen (-). Example: 192.168.20.1-192.168.20.3.</li> <li>● Network segment: IP address network segment. Example:</li> </ul>

Item	Description	Remarks
		192.168.1.0/24 or 192.168.1.0/255.255.255.0

(3) Click **Save**.

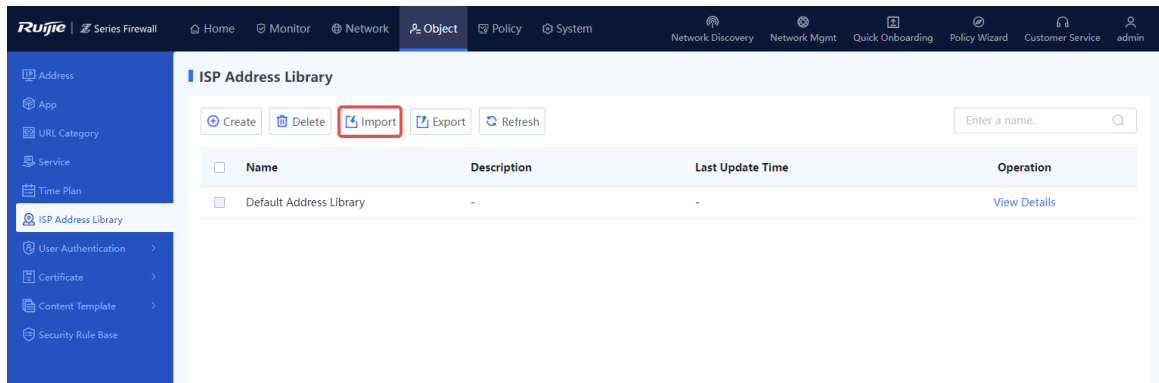
## 2. Importing an Address File to an ISP Address Library

### 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.



(2) Click **Download CSV Template** to download the template of the ISP address library file and enter IP addresses in the template.



## Import ⊗

---

[Download CSV Template](#)

\* Name

e

\* File

(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.

The screenshot shows the 'Library Upgrade' page in the Ruijie management interface. It features a navigation bar with 'Library Upgrade' selected. Below the navigation, there are filter tabs for various library types, with 'ISP Address Library' currently active. A set of filters includes 'Product Type', 'Product Series', 'Model', and 'Software Version', each with a dropdown menu and a 'Reset' button. The main content is a table with the following columns: No., File Name, Version Number, Version Description, Model, Software Version, Release Date, File Size (MB), MD5, and Operation. Two rows of data are visible, each with a 'Download' link in the 'Operation' column.

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...	<a href="#">Download</a>
2	isp_20221030.1000...	20221030.1000	isp_20221030.1000	Z5100,Z5100-S,Z3...	Universal	2022-10-30	0.01	0ABAF66F14A49F...	<a href="#">Download</a>

(2) Open the **Signature Library Upgrade** page.

Open the web page on the device, and choose **System > Signature Library Upgrade**.

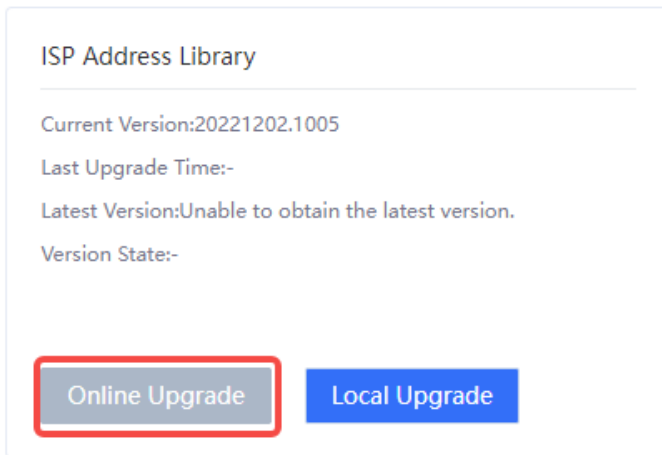
The screenshot displays the 'Signature Library Upgrade' configuration page. The left sidebar shows the navigation menu with 'System' selected and 'Signature Library Upgrade' highlighted. The main content area includes an 'Enable Auto Upgrade' section with a frequency of 'Daily' (6) and a time of '4' minutes. Below this, there are checkboxes for various signature libraries, all of which are checked: 'App Identification Signature Library', 'Intrusion Prevention Signature Library', 'Virus Protection Signature Library (Deep Scan)', 'Virus Protection Signature Library (Quick Scan)', 'ISP Address Library', and 'Threat Intelligence Signature Library'. A 'Save' button is present. The 'Signature Library Type' section shows a radio button for 'Upgrade All' (selected), with a note: '(Upgrade all signature libraries online simultaneously)'. There are three panels for individual library configurations: 'App Identification Signature Library', 'Virus Protection Signature Library (Deep Scan)', and 'Virus Protection Signature Library (Quick Scan)'. Each panel shows 'Current Version', 'Last Upgrade Time', 'Latest Version', 'Version State', and 'Activation State'. The 'Deep Scan' panel has a warning: 'The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded'. Each panel has 'Online Upgrade' and 'Local Upgrade' buttons. A 'system.versionRollback' button is also visible at the bottom.

(3) Find out **ISP Address Library**, and select **Online Upgrade** or **Local Upgrade** according to actual situation.

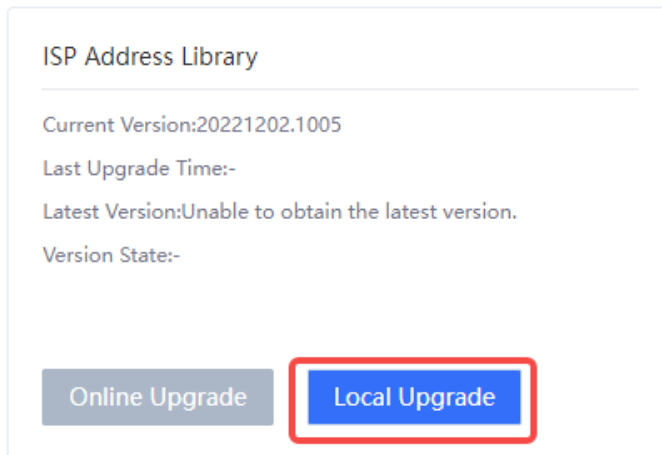
- Online Upgrade: When the current version information about the firewall exists on the cloud platform and a new version is available, online upgrade of the device system can be performed on the firewall.

**⚠ Caution**

The firewall must be connected to the Internet.



- o Local Upgrade
- a Click **Local Upgrade**.



- b Upload the version file that is downloaded from the cloud platform and click **Upgrade Now**.

**Local Upgrade** ⊗

① 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>

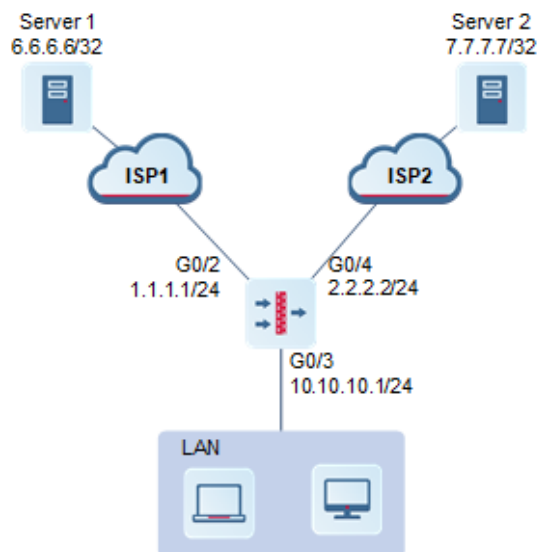
Import

## 7.14.3 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.

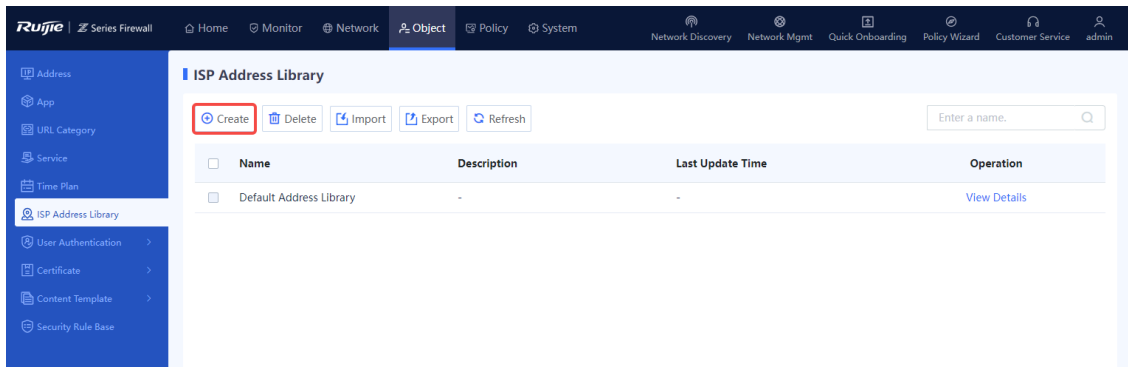
Configure the interface IP address, security zones, and gateway. For details, see [0](#)

[Routing](#) Mode.

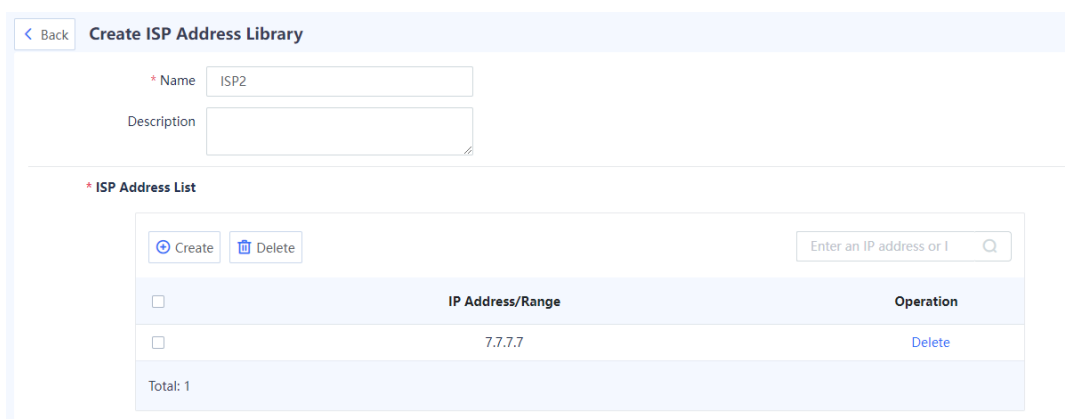
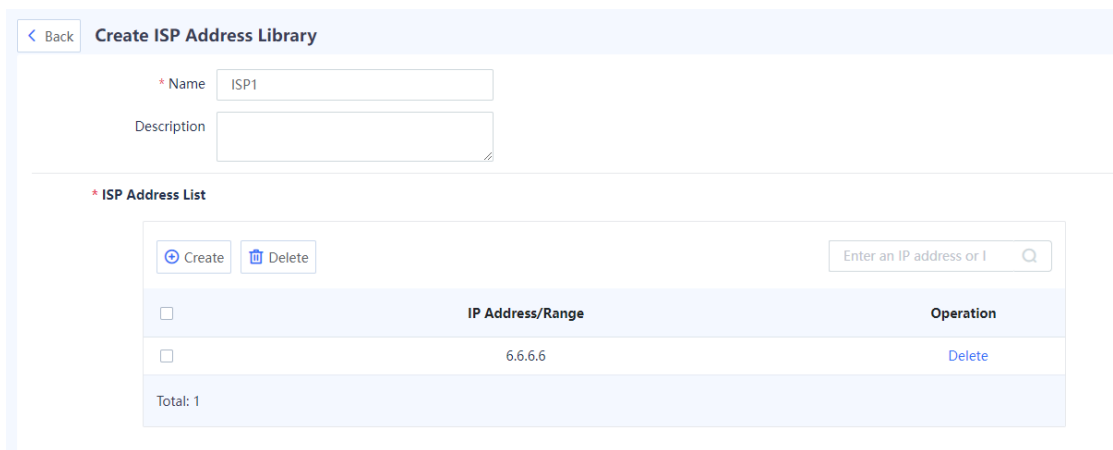
<input type="checkbox"/>	Ge0/2	-		Routing	untrust	IPv4: Static IP	1.1.1.1/24	-	1500		<a href="#">Edit</a>
<input type="checkbox"/>	Ge0/3	-		Routing	trust	IPv4: Static IP	10.10.10.1/24	-	1500		<a href="#">Edit</a>
<input type="checkbox"/>	Ge0/4	-		Routing	untrust	IPv4: Static IP	2.2.2.2/24	-	1500		<a href="#">Edit</a>

- (2) Configure ISP address library.

- a Choose **Object > ISP Address Library** and click **Create**.



- 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.



- (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

ⓘ MTU

MAC  [Restore Default MAC](#)

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**.

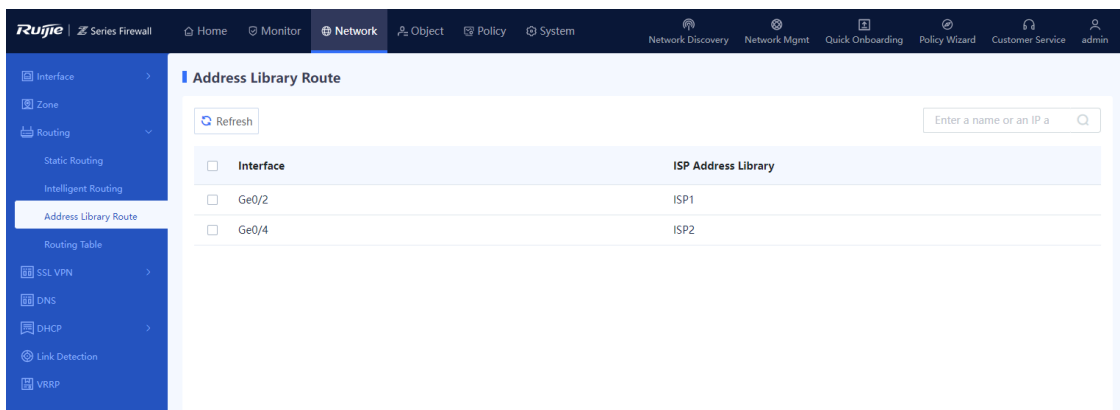
**Advanced**

ISP Address Library

ⓘ MTU

MAC  [Restore Default MAC](#)

Link Detection



- (4) Configure the security policy: forward the traffic from Trust zone to Untrust zone.

[< Back](#) **Create Security Policy**

**Basic Info**

\* Name

Enabled State  Enable  Disable

\* Policy Group  [+ Add Group](#)

\* Adjacent Policy

Description

---

**Src. and Dest.**

\* Src. Security Zone

\* Src. Address

\* Dest. Security Zone

\* Dest. Address

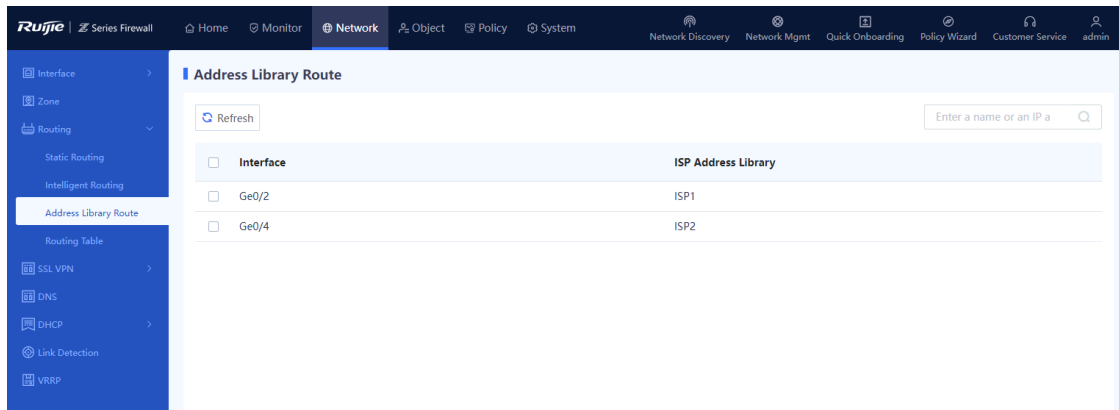
## 7.14.4 Viewing the Routing Table of Address Library

### 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.



## 7.15 Aggregate Interface

### Application Scenario

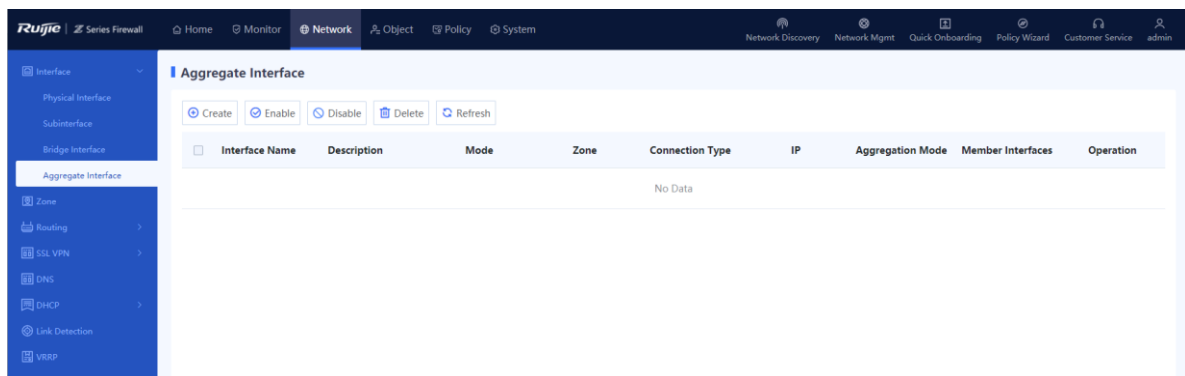
An aggregate interface binds multiple physical interfaces together to form a logical interface for link bandwidth expansion, which provides higher connection reliability.

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  $\times$   $n$ .
- 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**.





(2) Click **Create**.

The system opens the **Add Aggregate Interface** page.

[Back](#) **Add Aggregate Interface**

**Basic Info**

\* Interface Name

Connection Status  Enable  Disable

Mode  Routing Mode  Transparent Mode  Off-Path Mode

Zone  [Add Security Zone](#)

Interface Type  WAN Interface  LAN Interface

Description

**Member Interface**

To-be-selected (0)  Select All

- Ge0/0
- Ge0/1
- Ge0/2
- Ge0/3
- Ge0/4

Selected (0) [Clear](#)

**Address**

\* Connection Type  Static Address  DHCP

\* IP/Mask

\* Next-Hop Address

Default Route

**Line Bandwidth**

Uplink

Downlink

**Access Management**

Permit  HTTPS  PING  SSH

**Advanced Settings**

Aggregation Mode

ISP Address Library

① MTU

① MAC

Link Detection

(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. <ul style="list-style-type: none"> <li>● <b>Routing Mode:</b> forwards traffic based on IP addresses.</li> <li>● <b>Transparent Mode:</b> forwards traffic based on MAC addresses.</li> <li>● <b>Off-Path Mode:</b> only receives mirrored traffic, but does not forward traffic.</li> </ul>	[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 allowed. [Example] Expand egress bandwidth.

Item	Description	Remarks
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 <b>Routing Mode</b> is used. [Example] Static Address
IP/Mask	IPv4 address and mask of the interface.	This parameter is available when <b>Connection Type</b> is set to <b>Static Address</b> . [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 <b>Connection Type</b> is set to <b>Static Address</b> . [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 bandwidth.	Enter the bandwidth value and select a unit. 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.

Item	Description	Remarks
		[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 <b>HTTPS</b> .
Advanced Settings		
Aggregation Mode	For the manually configured aggregate interface, the aggregation mode is displayed as <b>Static Aggregation</b> .	Only the <b>Static Aggregation</b> 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 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.	An integer ranging from 64 to 1600.  [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	For details about link detection, see <a href="#">7.16 Link Detection</a> .


Item	Description	Remarks
	detect the network connectivity between the interface and the next hop in real time.	

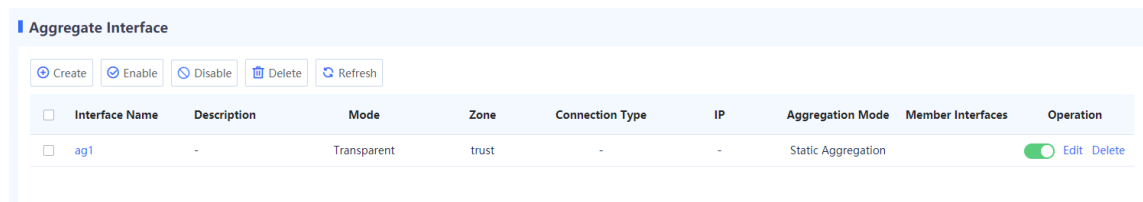
### Caution

- 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**.



## 7.16 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

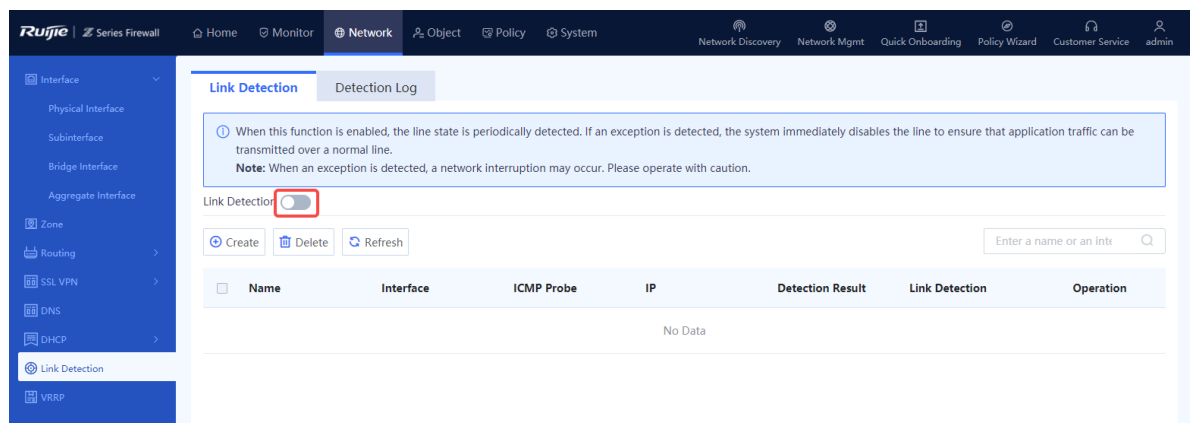
This function is supported from NTOS1.0R3. If your version is lower than NTOS1.0R3, upgrade it to NTOS1.0R3 or higher.

## Procedure

- (1) Choose **Network > Link Detection > Link Detection**.
- (2) Click  to enable link detection.

### Note

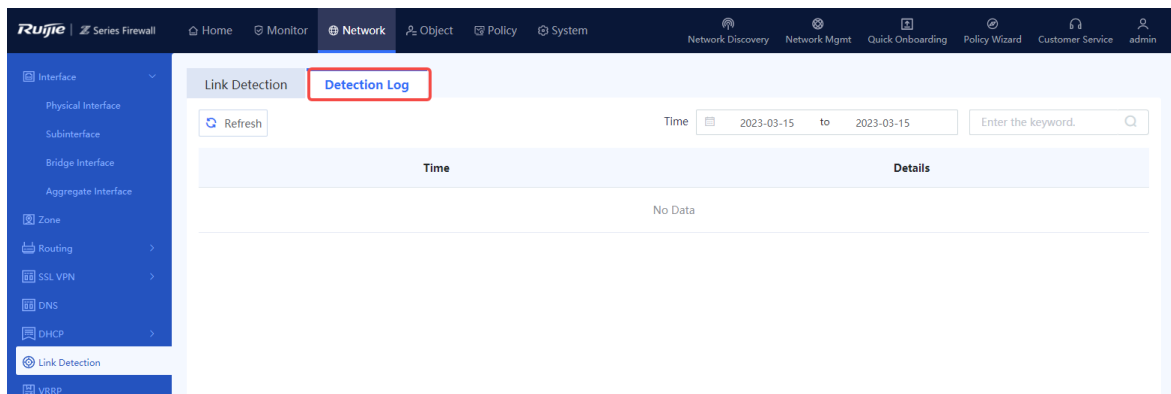
If a single detection policy is enabled but the link detection function is not enabled, the detection policy will not take effect and link detection will not be performed.



- (3) Click **Create** to access the **Add Link Detection** page. Set the detection parameters.

(4) Click **Save**.

(5) After detection is completed, you can view the detection log on the **Detection Log** tab page.

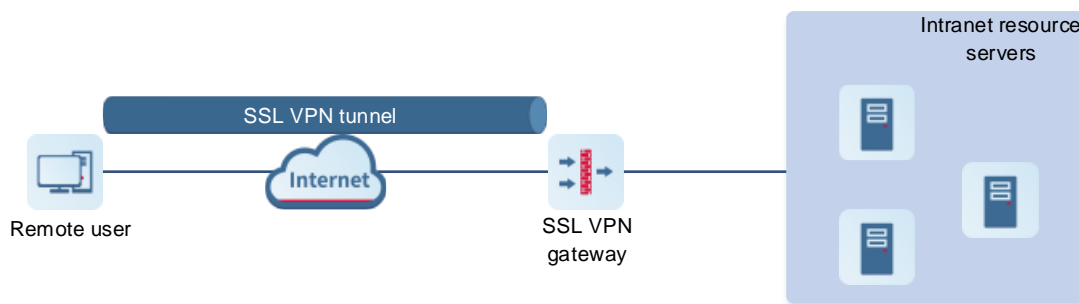


## 7.17 SSL VPN

### 7.17.1 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

## 7.17.2 (Optional) Import Local Certificate

### Application Scenario

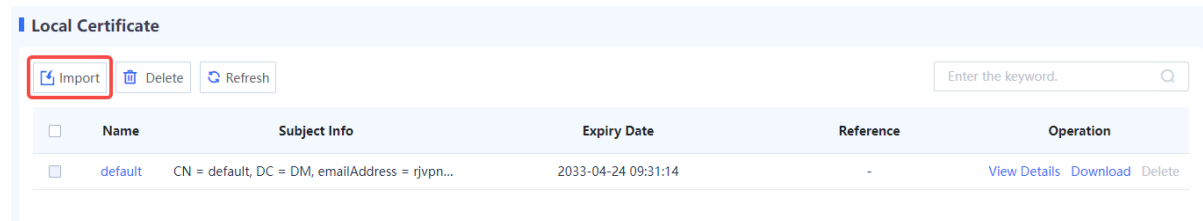
When a remote access user establishes an SSL connection with the SSL VPN gateway on the SSL VPN client, the gateway provides a local certificate to the peer end. In this way, the client can authenticate the SSL VPN gateway based on the digital certificate. If a non-CA certificate is provided, the client 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**.



- (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.

### Import Local Certificate ⊗

---

\* Certificate Format

\* Certificate File

\* Password

### 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.

## 7.17.3 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.

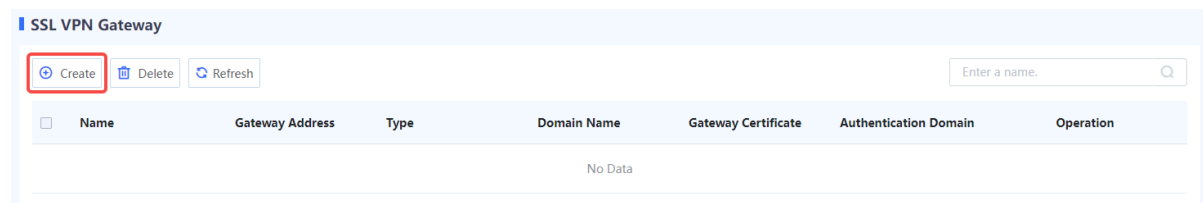
The firewall supports multiple SSL VPN gateways that are independent of each other. Users and resources can be separately configured and managed for different SSL VPN gateways, which meets the remote access requirements of different service departments.

### 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.



- (3) Configure basic information of an SSL VPN gateway.

Basic Config
 Login Control
 Add Resource
 Bind Resource

**Network Config**

\* Gateway Name

Gateway Type  Exclusive  Shared

\* Gateway Address   Port Number

[Create](#)

Domain Name

Intranet DNS

[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

---

**Concurrency Control**

\* Max. Concurrent Users

[Next](#)

Item	Description	Remarks
<b>Network Config</b>		
Gateway Name	Name of the SSL VPN gateway.	[Example] gateway1
Gateway Type	<ul style="list-style-type: none"> <li><b>Exclusive:</b> 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.</li> <li><b>Shared:</b> 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.</li> </ul>	[Example] Shared
Gateway Address	Address for accessing the SSL VPN gateway. You can choose an interface address or configure it manually. A gateway can be configured with a maximum of three	[Example] 1.1.1.1

Item	Description	Remarks
	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
<b>Advanced</b>		
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] TLS1.2
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 <a href="#">7.17.2 (Optional) Import Local Certificate</a> .	N/A
<b>Concurrency Control</b>		
Max. Concurrent	Maximum number of users that can concurrently log in to the SSL VPN gateway. When the maximum number	[Example]

Item	Description	Remarks
Users	of concurrent users is reached, new users cannot log in to the SSL VPN gateway.	20

(4) Verify the configuration and click **Next** to configure the login control parameters.

The screenshot shows the 'Add SSL VPN Gateway' configuration interface. At the top, there are four steps: Basic Config (checked), Login Control (selected), Add Resource, and Bind Resource. The 'Login Control' section is expanded, showing the following settings:

- Authentication:**
  - User Authentication Domain: default
- Prevent Brute-Force Attack:**
  - User Lockout: 
    - Max. User Attempts: 5 Time
    - Lockout Period: 300 Second
  - Single IP Lockout: 
    - Max. Single IP Attempts: 5 Time
    - Lockout Period: 300 Second
- Login Verification:**
  - Graphic Verification:
  - Enable upon: 0 Consecutive Input Errors
  - Hardware Signature Verification:
  - Maximum Signatures Bound to Each User: 3
  - Auto Hardware Signature Approval:
  - Auto User Unbinding:
  - Auto Approval of Trusted Public Terminals:
- 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.)

At the bottom of the configuration page, there are 'Previous' and 'Next' buttons.

Item	Description	Remarks
<b>Authentication</b>		
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
<b>Prevent Brute-Force Attack</b>		

Item	Description	Remarks
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
<b>Login Verification</b>		
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 brute-force attacks.	[Example] Enable
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	Specifies whether to enable automatic approval of hardware signatures for devices attempting to log in to	[Example] Disable

Item	Description	Remarks
Approval	the gateway.	
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 <a href="#">7.17.4 Hardware Signature Management</a> .	[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
<b>Idle Timeout</b>		
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
<b>Client Version Control</b>		
Available Client Versions	Version of the SSL VPN client that connects to the SSL VPN gateway. Currently, only Ruijie SSL VPN client is supported. <ul style="list-style-type: none"> <li>● <b>Any Version:</b> no limit on the version of the SSL VPN client</li> <li>● <b>Latest Version on Secure Cloud:</b> the latest version released on Ruijie Secure Cloud Platform</li> <li>● Custom Config (The earliest version for clients on each platform can be specified.): custom client versions for each type of system</li> </ul>	[Example] Any Version

(5) Verify the configuration and click **Next** to configure resource information.

- a Configure basic information:

< Back
Add SSL VPN Gateway

✔ Basic Config
✔ Login Control
⦿ Add Resource
○ Bind Resource

**Basic Config**

\* ⦿ Available IP Ranges

⦿ Tunnel Mode  Full Tunnel  Split Tunnel

\* ⦿ Tunnel Access Keep-Alive Interval  Second

\* ⦿ Max. Disconnection Time  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: <ul style="list-style-type: none"> <li>● <b>Split Tunnel:</b> Only the traffic to authorized resources is sent through the SSL VPN tunnel.</li> <li>● <b>Full Tunnel:</b> All user traffic, including traffic for Internet access and local communications, is sent through the SSL VPN tunnel.</li> </ul>	[Example] 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	[Example] Disable



Item	Description	Remarks
	resources cannot be accessed.	

- 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**

<input type="checkbox"/>	Resource Group Name	Resource	Description	Operation
No Data				
Total: 0				

**Add Tunnel Resource Group** ⊗

\* Tunnel Resource Group Name

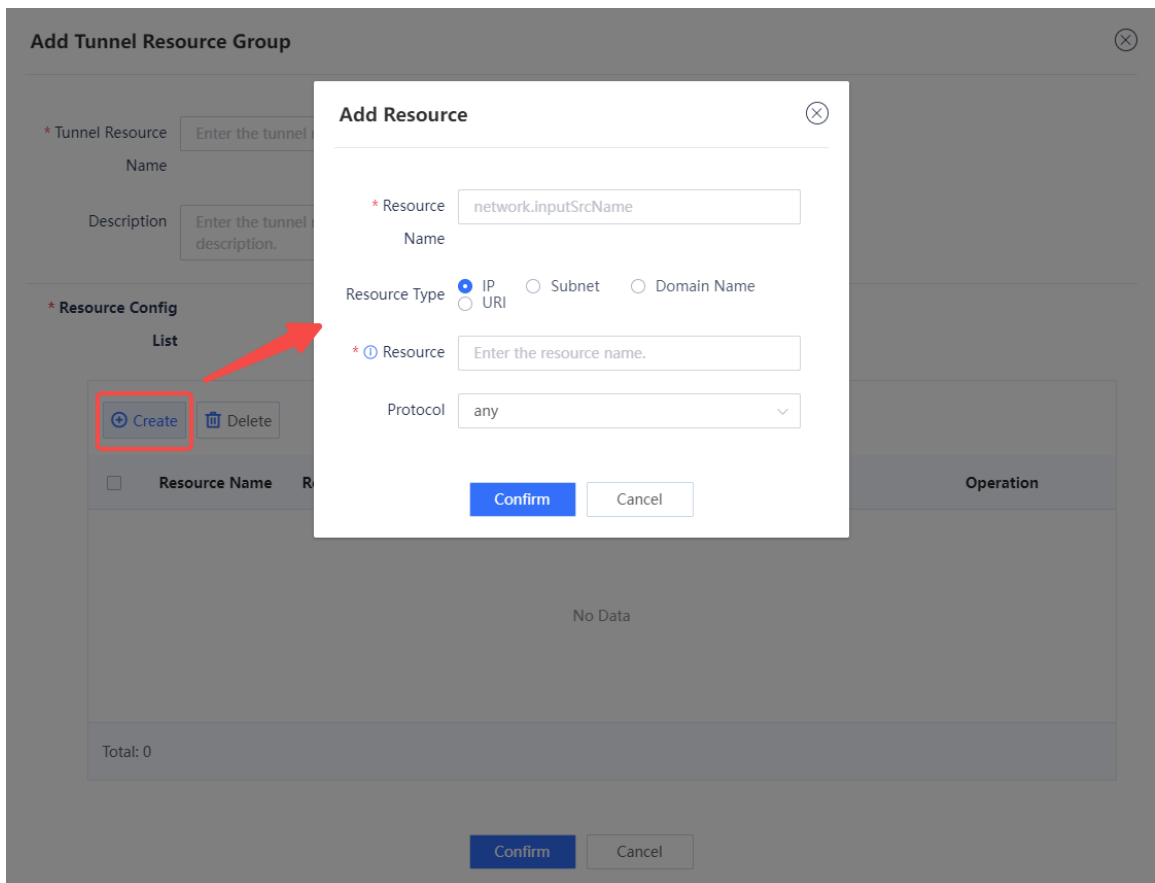
Description

**\* Resource Config List**

<input type="checkbox"/>	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

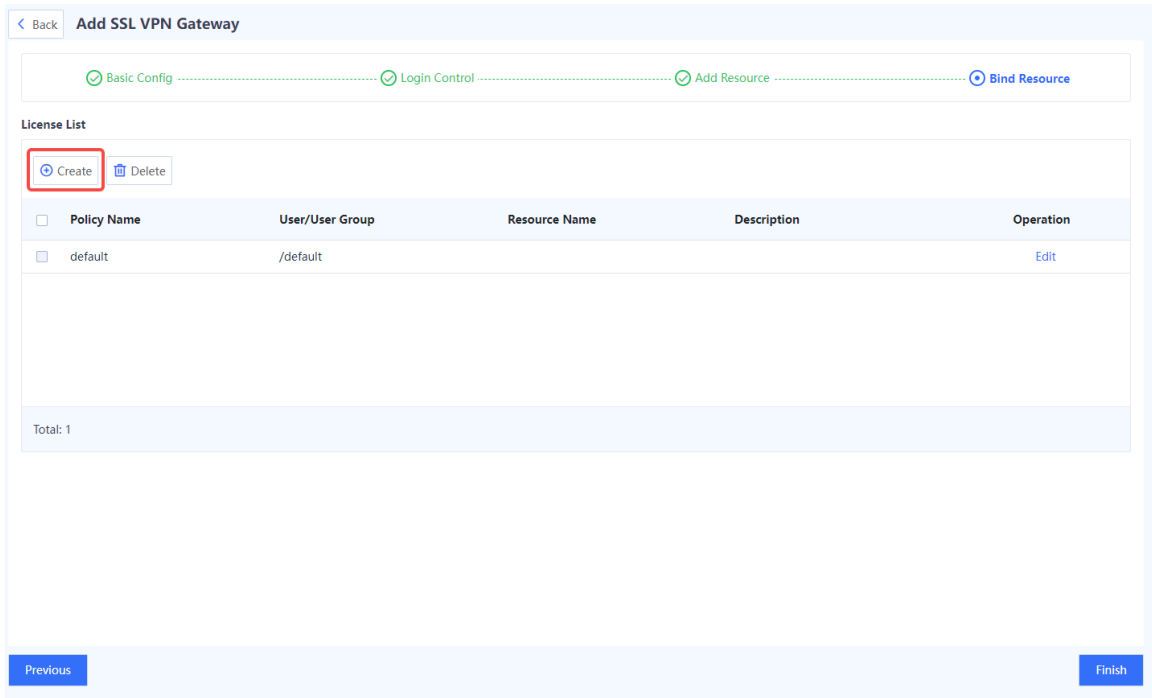
- c In the **Tunnel Resource List** area, click **Create** to configure the information of the resources in the resource group.



Item	Description	Remarks
Resource Name	Name of the resource that can be access through this tunnel.	[Example] IP
Resource	Supported resource types are as follows:	N/A

Item	Description	Remarks
Type	<ul style="list-style-type: none"> <li>● <b>IP:</b> Only a single IP address is supported. Example: 192.168. 1.1.</li> <li>● <b>Subnet:</b> IP/Mask length. Example: 192.168.1.0/24.</li> <li>● <b>Domain Name:</b> Domain name. Example: www.abc.com.</li> <li>● <b>URI:</b> URI. Example: &lt;proto://ip[:port]&gt;.</li> </ul>	
Resource	Resource to be entered based on the selected resource type. For example, enter an IP address if <b>Resource Type</b> is set to <b>IP</b> .	N/A
Protocol	Network protocol that specified resources use for authorized users to access. For example, if <b>Resource Type</b> is set to <b>IP</b> and this parameter is set to <b>any</b> , the user can access all external services provided at the IP address. If this parameter is set to <b>TCP</b> , 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.



b Configure parameters of an authorization policy.

### Add License



\* Authorization   
Policy Name

\* User/User   
Group

IP Tunnel   
Resource

Description

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.

## 7.17.4 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.

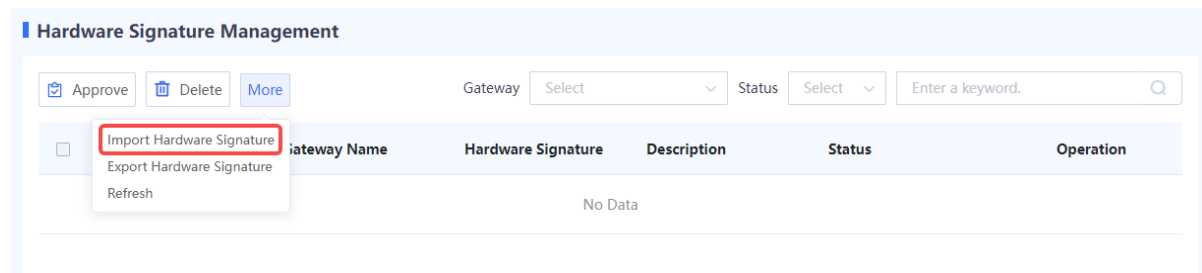
### Precautions

- 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.

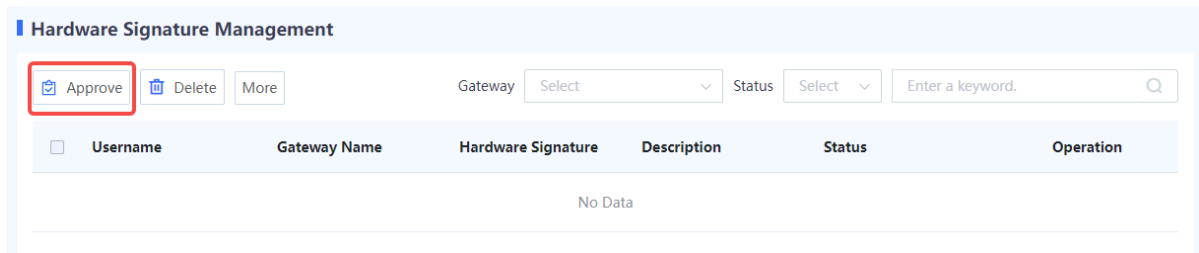
### **i** Note

The format of the hardware signature file is .data. To import hardware signatures in batches, contact a technical engineer for help.

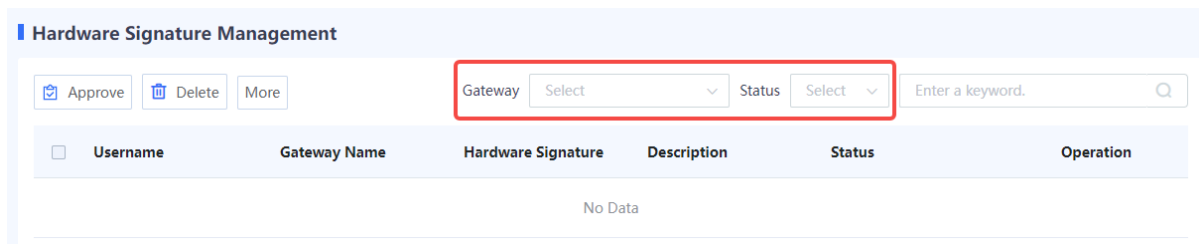
The screenshot shows the 'Import Hardware Signature' dialog box. It has a title bar with a close button. The form includes:
 

- A dropdown menu for 'Gateway' with a red asterisk indicating it is required.
- A text input field for 'Name'.
- A file selection input for 'Signature' with a 'Browse' button.
- Two buttons at the bottom: 'Confirm' (in blue) and 'Cancel'.

- (4) Select multiple hardware signature entries in the list and click **Approve** to approve hardware signatures in batches.



- (5) (Optional) Select a gateway or approval status to view corresponding hardware signature information.



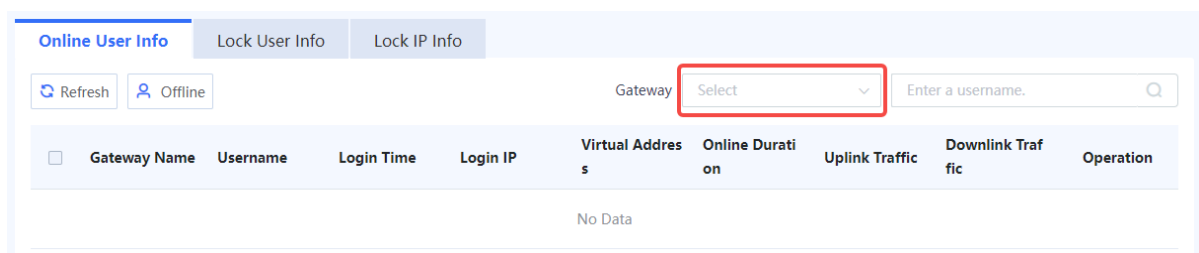
## 7.17.5 Operation Monitoring

### 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.



- (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.

- (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.

- (9) To unlock an IP address, click **Unlock** in the **Operation** column.

## 7.18 IPsec VPN

### 7.18.1 Overview

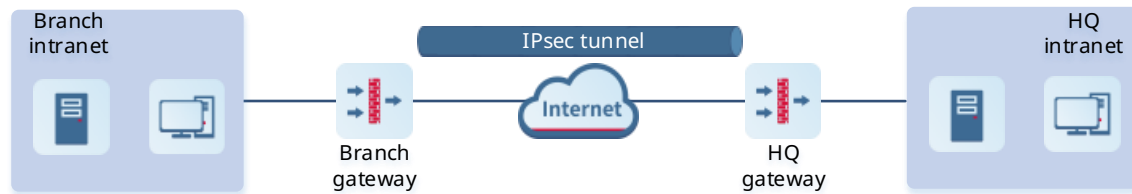
Internet Protocol Security Virtual Private Network (IPsec VPN) is a VPN technology that uses the IPsec protocol to enable remote access. IPsec VPN can provide encrypted, secure communication channels for two or more private networks over public networks. With IPsec VPN, an IPsec tunnel can be established between two communication ends, and specific algorithms are used to encrypt and authenticate the data transmitted over the tunnel. In this way, IPsec VPN protects IP packets from theft, forgery, and tampering during transmission over a public network, thereby guaranteeing secure service data transmission over the Internet.

IPsec VPN is typically used to set up secure interconnection between an enterprise HQ and branch. After an IPsec tunnel is established between the HQ gateway and branch gateway,



data can be securely transferred between the HQ and branch, and intranet resources can be shared.

**Figure 7-14 Typical Application Scenario of IPsec VPN**



## 7.18.2 Principles

### 1. IPsec Working Process

The firewall establishes an IPsec tunnel by using a virtual tunnel interface. When configuring an IPsec tunnel, associate a tunnel interface for the tunnel, and set routing to divert traffic to be protected by IPsec to the tunnel interface. When the tunnel interface receives traffic that matches the interesting traffic, the firewall uses IPsec to encrypt or decrypt the packets on the tunnel interface.

---

#### **Note**

The interesting traffic of a tunnel defines the traffic to be transmitted through an IPsec tunnel and protected by IPsec.

---

The IPsec working process consists of three phases:

(1) Negotiate Security Associations (SAs).

An SA is a group of specifications that are negotiated between two communication ends, including the security protocol, encapsulation mode used for data transmission, encryption and authentication algorithms used by the protocol, and keys for data transmission. The two ends must establish SAs to ensure secure data transmission.

In this phase, the two ends first negotiate and establish an Internet Key Exchange (IKE) SA for identity authentication and key information exchange through IKE, and then negotiate and establish an IPsec SA for secure data transmission on the basis of the IKE SA.

(2) Identify data flows to be protected.

When a packet arrives at the tunnel interface associated with an IPsec tunnel, it is matched against the interesting traffic of the IPsec tunnel. Only matched packets are transmitted over the IPsec tunnel.

(3) Transmit data over the IPsec tunnel.

During data transmission, both ends of the IPsec tunnel encrypt and authenticate the data. The encryption mechanism protects the data from theft, and the authentication mechanism protects the data from forgery and tampering. This ensures data confidentiality, integrity, and validity.

## 2. IKEv1 Negotiation Process

The firewall establishes an IPsec SA through IKEv1 negotiation. The negotiation process consists of two phases:

- (1) Phase 1: Both communication ends negotiate and establish a security channel for IKE, that is, an IKE SA.

In this phase, the two ends negotiate parameters for establishing an IKE SA (including the encryption algorithm, authentication algorithm, identity authentication mode, Diffie-Hellman (DH) group, and IKE SA lifetime), exchange key information using the DH algorithm, and authenticate each other.

In phase 1, two negotiation modes are available: main mode and aggressive mode. In aggressive mode, fewer messages are exchanged between the two ends, and identity information is not encrypted. In scenarios with low requirements for identity protection, the aggressive mode can improve the negotiation speed. The main mode should be used in scenarios with high requirements for identity protection.

- (2) Phase 2: Both communication ends negotiate and establish a pair of IPsec SAs for secure data transmission based on the security channel (IKE SA) configured with authentication and protection in phase 1.

In this phase, the two ends negotiate and verify IPsec security parameters (including the security protocol, encryption algorithm, authentication algorithm, and encapsulation mode) and generate the encryption and authentication keys required for data transmission.

### 7.18.3 Configuring an IPsec Tunnel Using the Wizard

#### Application Scenario

The configuration wizard helps you create IPsec tunnel policies, facilitating IPsec VPN deployment.

IPsec VPN supports the following two deployment scenarios:

- **Point-to-Point:** Establish an IPsec tunnel between two fixed sites (such as sites deployed with egress gateways) so that the two sites and the private networks connected to the two sites can securely access each other. In this scenario, the communication peer end must have a fixed IP address or domain name for the local end to initiate IPsec tunnel negotiation.
- **Point-to-Multipoint:** Establish multiple IPsec tunnels between the HQ site and branch sites to enable interconnection among the sites and private networks connected to the sites. In this scenario, the communication peer end does not need to have a fixed IP address, and IPsec

tunnel negotiation can only be initiated by the peer end.

### Prerequisites

Before configuring IPsec VPN, you have completed the following steps:

- In a point-to-point IPsec VPN scenario, obtain the IP address or domain name of the peer end, as well as the range of addresses to be accessed on the intranet.
- Verify that devices at both ends of the IPsec tunnel to be established are reachable to each other.
- If the peer network of the tunnel is configured with a domain name, you need to configure an available DNS server for the firewall to enable domain name resolution.
- Determine the security parameters of the IPsec tunnel and pre-shared key together with the administrator of the peer device.

#### Caution

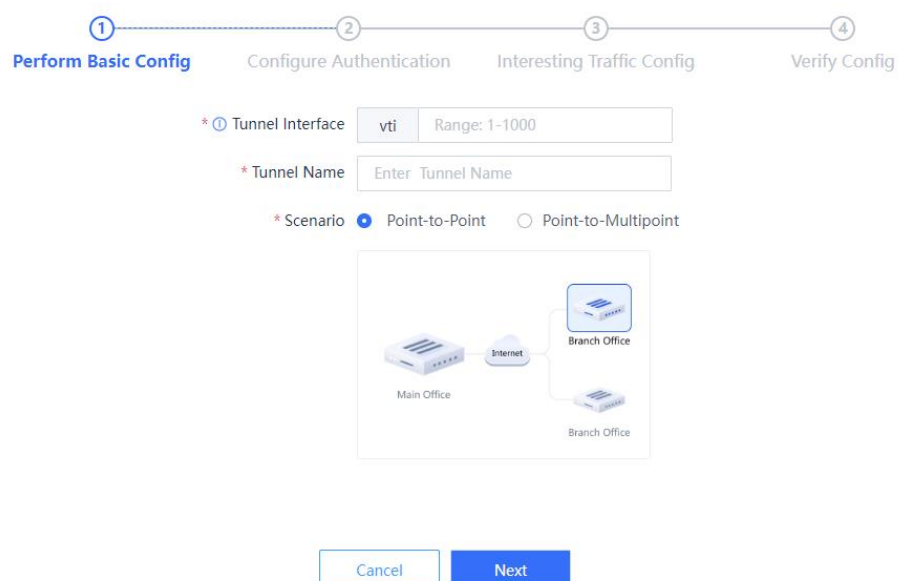
- Both communication ends need to negotiate with each other to establish an IPsec tunnel, and IPsec VPN must be enabled on devices at both ends of the IPsec tunnel.
- The IKE parameters and IPsec parameters (including the security protocol, encryption algorithm, authentication algorithm, and packet encapsulation mode) configured for the devices at both ends of the IPsec tunnel must be the same. Otherwise, tunnel negotiation fails.

### Procedure

(1) Choose **Network > IPsec VPN > Config Wizard**.

(2) Configure basic IPsec tunnel information on the configuration wizard.

#### Config Wizard



① Perform Basic Config    ② Configure Authentication    ③ Interesting Traffic Config    ④ Verify Config

\* ① Tunnel Interface  Range: 1-1000

\* Tunnel Name

\* Scenario  Point-to-Point  Point-to-Multipoint

Diagram: Main Office — Internet — Branch Office (two)

Item	Description	Remarks
Tunnel Interface	<p>Create a tunnel interface for the IPsec tunnel and associate it with the tunnel so that the firewall can use IPsec to process the data flows that arrive at the tunnel interface and match the interesting traffic.</p> <p>The interface name is in the format of <b>vti+Interface number</b>. After completing IPsec VPN configuration on the wizard, you can view the automatically created tunnel interface information on the <b>Tunnel Interface</b> page.</p>	<p>Enter the interface number. Range: 1–1000.</p> <p>[Example] vti2</p>
Tunnel Name	IPsec tunnel name.	<p>Characters such as ~!#%^&amp;*+ \{ };:"/&lt;&gt;? are not allowed.</p> <p>[Example] ipsec_1</p>
Scenario	<p>Select the IPsec tunnel type based on the deployment scenario:</p> <ul style="list-style-type: none"> <li>● <b>Point-to-Point:</b> applies to scenarios where the peer end has a fixed IP address, such as IPsec VPN deployment at an enterprise branch.</li> <li>● <b>Point-to-Multipoint:</b> applies to scenarios where the peer end IP address is not fixed or multiple peer ends exist, such as IPsec VPN deployment at an enterprise HQ. In this case, the peer end needs to initiate tunnel negotiation.</li> </ul>	<p>On the firewall, one point-to-multipoint IPsec VPN tunnel and multiple point-to-point IPsec VPN tunnels can be configured.</p> <p>If a point-to-multipoint tunnel already exists, you can modify the configuration by accessing <b>Network &gt; IPsec VPN &gt; Custom Tunnel</b>.</p> <p>[Example] <b>Point-to-Point</b></p>

(3) Click **Next** to configure identity authentication.



\* Peer Address

\* Outbound Interface

\* Authentication Mode  Pre-shared Key

\* Password

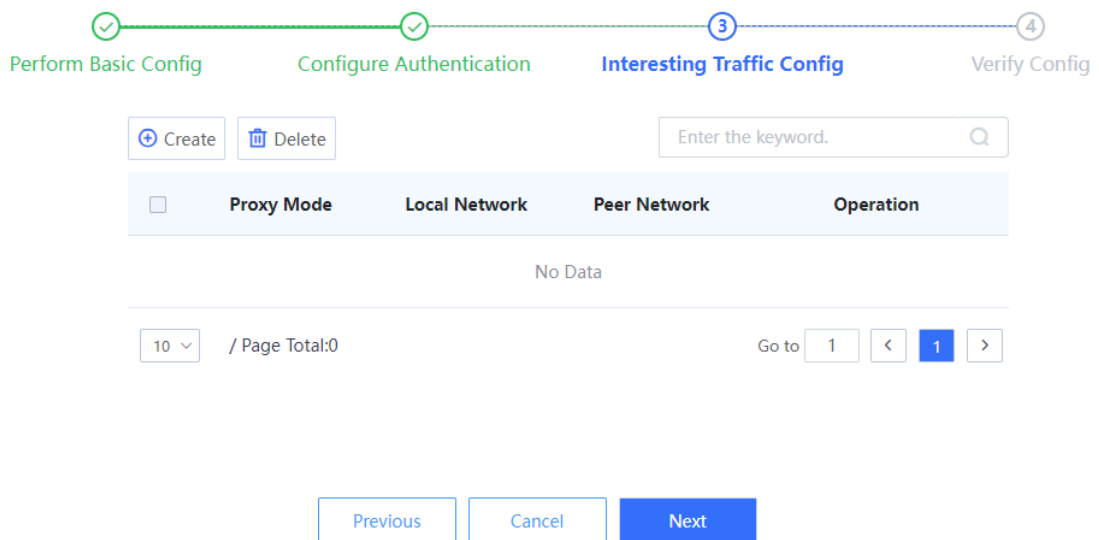
\* Confirm Key

Item	Description	Remarks
Peer Address	IP address or domain name used by the peer device to establish the tunnel.	<ul style="list-style-type: none"> <li>This parameter is mandatory in a point-to-point scenario.</li> <li>After entering the IP address or domain name, click <b>Ping</b> to verify that the devices at both ends are reachable to each other.</li> <li>The value must be the same as that of <b>Local Address</b> configured for the peer device. [Example] 40.0.0.50</li> </ul>
Outbound Interface	<p>Physical interface for establishing an IPsec tunnel with the peer end. Data flows to be protected by IPsec are forwarded through the interface to the peer end of the tunnel.</p> <p>If you use the wizard to configure IPsec VPN, the IP address of the outbound interface is used as the source address of the tunnel interface.</p>	<p>Select an interface in routing mode configured with an IP address.</p> <p>[Example] Ge0/2</p>

Item	Description	Remarks
Authentication Mode	Identity authentication mode of both ends of the tunnel.  By default, pre-shared key authentication is used. In this mode, both ends perform hash calculation on packets using the pre-shared key. If the calculation results are the same, the authentication is successful.	[Example]  Pre-shared Key
Key	Key string for identity authentication in pre-shared key authentication mode.	<ul style="list-style-type: none"> <li>● Length range: 6 to 16 characters.</li> <li>● Configure the same identity authentication mode (pre-shared key) and key for both ends.</li> </ul> [Example]  Ruijie123

(4) Click **Next** to configure data flows to be transmitted over the IPsec tunnel.

a Click **Create** to access the **Create Interesting Traffic Config** page.



b Configure interesting traffic based on the network segments or host addresses at both ends of the tunnel that require secure mutual access.

Create Interesting Traffic Config



Proxy Mode  Auto  Subnet-to-Subnet  Host-to-Host

\* Local Network  \* Peer Network  [Delete](#) [Create](#)

Item	Description	Remarks
Proxy Mode	<p>Set the proxy mode for interesting traffic based on the ranges of addresses at both ends of the tunnel that require secure mutual access:</p> <ul style="list-style-type: none"> <li>● <b>Auto:</b> Traffic to be encrypted is automatically identified based on the interesting traffic defined at the peer end, and no configuration is performed at the local end.</li> <li>● <b>Subnet-to-Subnet:</b> Data flows between two specific subnets are protected.</li> <li>● <b>Host-to-Host:</b> Data flows between two specific hosts are protected.</li> </ul>	<p>Point-to-point IPsec VPN does not support the <b>Auto</b> proxy mode.</p> <p>[Example]</p> <p>Subnet-to-Subnet</p>
Local Network	<p>Source address of interesting traffic. Typically, a network segment or specific host address to be protected on the local intranet is set.</p>	<p>The address format varies with the proxy mode:</p> <ul style="list-style-type: none"> <li>● <b>Subnet-to-Subnet:</b> Enter an IP range. Example: 192.168.1.0/255.255.255.0 or 192.168.1.0/24.</li> <li>● <b>Host-to-Host:</b> Enter an IP address. Example: 192.168.1.1.</li> </ul>
Peer Network	<p>Destination address of interesting traffic. Typically, a network segment or specific host address to be protected on the peer intranet is set.</p>	<p>The address format varies with the proxy mode:</p> <ul style="list-style-type: none"> <li>● <b>Subnet-to-Subnet:</b> Enter an IP range. Example: 192.168.1.0/255.255.255.0 or 192.168.1.0/24.</li> </ul>

Item	Description	Remarks
		<ul style="list-style-type: none"> <li>● <b>Host-to-Host:</b> Enter an IP address. Example: 192.168.1.1.</li> </ul>

c Click **OK** to save interesting traffic configuration. Click **Create** to add more interesting traffic.

Perform Basic Config
Configure Authentication
3
Verify Config

	Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/>	Subnet-to-Subnet	1.1.1.0/24	2.2.2.0/24	<a href="#">Edit</a> <a href="#">Delete</a>

10 / Page Total:1
Go to

(5) Click **Next** to confirm configured parameters on the page that is displayed. Click **Edit** to modify the configurations.

ⓘ The tunnel configured on the wizard will be added to the custom tunnel list.
×

**Perform Basic Config** [edit](#)

Tunnel Interface:

Tunnel Name:

Scenario:  Point-to-Point  Point-to-Multipoint

**Configure Authentication** [edit](#)

Peer Address:

Outbound Interface:

Authentication Mode:  Pre-shared Key

Password:

**Interesting Traffic Config** [edit](#)

Local Network	Peer Network
1.1.1.0/24	2.2.2.0/24

**Advanced Settings** [unfold](#)



(6) (Optional) Set security parameters for IPsec tunnel negotiation in the **Advanced Settings** area.

The system provides default IPsec security parameter values, which apply to most IPsec VPN deployment scenarios. If the default values do not meet negotiation requirements, you can modify them in the **Advanced Settings** area.

- a Click **Unfold** next to **Advanced Settings**.
- b Modify negotiation parameters.

**Advanced Settings** [pack up](#)

Enable Peer Identity Authentication

\* Local ID Type

DPD Type

DPD Retry Interval  Second

---

**IKE Parameter**

\* Negotiation Mode

\* Encryption Algorithm

\* Verification Algorithm

\* DH Group

\* SA Lifetime  Second

---

**IPsec Parameter**

\* Protocol

\* Encapsulation Mode

\* Encryption Algorithm

\* Verification Algorithm

Perfect Forward Secrecy

\* SA Lifetime  Second

Item	Description	Remarks
<b>Identity Authentication Parameters</b>		
Peer Identity Authentication	Whether to enable identity authentication for the peer device.	Toggle it on or off to enable or disable this function. After enabling this

Item	Description	Remarks
		function, you need to set identity authentication information for the peer device.  [Example]  <b>Enable</b>
Local ID Type	A local ID identifies the local device and is used by the peer device to authenticate the local device. The following types are supported: <ul style="list-style-type: none"> <li>● <b>IPV4_ADDRESS</b>: An IPv4 address is used as the local ID for IKE negotiation.</li> <li>● <b>FQDN</b>: A Fully Qualified Domain Name (FQDN) string is used as the local ID for IKE negotiation.</li> <li>● <b>USER_FQDN</b>: A user FQDN string is used as the local ID for IKE negotiation.</li> </ul>	If <b>IPV4_ADDRESS</b> is selected, the device uses the local IP address (outbound interface IP address) as the local ID.  [Example]  IPV4_ADDRESS
Local ID	String that identifies the local device for identity authentication.	<ul style="list-style-type: none"> <li>● The value must be the same as that of <b>Peer ID</b> configured for the peer device.</li> <li>● The string format varies with the local ID type:                             <ul style="list-style-type: none"> <li>○ <b>FQDN</b>: Domain name of the local end. Example: <b>aaa.com</b>.</li> <li>○ <b>USER_FQDN</b>: User domain name of the local end in the format of <i>Username@Domain name</i>. Example: <b>julia@aaa.com</b>.</li> </ul> </li> </ul>
Peer ID Type	A peer ID identifies the peer device for identity authentication. The following types are	<ul style="list-style-type: none"> <li>● This parameter is mandatory when <b>Peer Identity Authentication</b> is enabled.</li> <li>● The value must be the</li> </ul>

Item	Description	Remarks
	supported: <ul style="list-style-type: none"> <li>● <b>IPV4_ADDRESS</b>: The peer end uses an IPv4 address as the peer ID for identity authentication.</li> <li>● <b>FQDN</b>: The peer end uses an FQDN string as the peer ID for identity authentication.</li> <li>● <b>USER_FQDN</b>: The peer end uses a user FQDN string as the peer ID for identity negotiation.</li> </ul>	same as that of <b>Local ID Type</b> configured for the peer device. Obtain the value from the administrator of the peer device. [Example] IPV4_ADDRESS
Peer ID	String that identifies the peer device for identity authentication.	<ul style="list-style-type: none"> <li>● This parameter is mandatory when <b>Peer Identity Authentication</b> is enabled.</li> <li>● The value must be the same as that of <b>Local ID</b> configured for the peer device. Obtain the value from the administrator of the peer device.</li> <li>● The string format varies with the peer ID type:                             <ul style="list-style-type: none"> <li>○ <b>IPV4_ADDRESS</b>: IP address of the peer end. Example: 10.1.1.1.</li> <li>○ <b>FQDN</b>: Domain name of the peer end. Example: <b>bbb.com</b>.</li> <li>○ <b>USER_FQDN</b>: User domain name of the peer end in the format of <i>Username@Domain name</i>. Example: <b>susan@bbb.com</b>.</li> </ul> </li> </ul>
<p><b>DPD</b></p> <p>Dead Peer Detection (DPD) is used to detect peer status of an IPsec tunnel. A device sends DPD messages to detect whether the peer end is available to remove abnormal tunnels in a timely manner.</p>		
DPD Type	Two DPD modes are supported: <ul style="list-style-type: none"> <li>● <b>Idle Mode</b>: If the local</li> </ul>	This parameter is supported in a

Item	Description	Remarks
	end does not receive a response message from the peer end after sending a message, it sends a DPD message to the peer end. <ul style="list-style-type: none"> <li> <b>Regular Mode:</b> The local end sends DPD messages periodically based on the configured DPD detection interval.                             </li> </ul>	point-to-point scenario. [Example] Idle Mode
DPD Detection Interval	In regular mode, set the interval between two DPD detections, in seconds.	The default value is 30 seconds. [Example] 30
DPD Retry Interval	Interval for retransmitting DPD messages.  After sending a DPD request message, if the local end does not receive a response message within the retry interval, it retransmits the DPD request message. If the local end does not receive a response message after three retransmissions, it regards the peer end as unavailable and automatically removes the IPsec tunnel.	The default value is 5 seconds. [Example] 3
<p><b>Reverse Route Injection</b></p> <p>When reverse route injection is enabled, the device automatically adds the route to the protected peer network segment to the routing table, eliminating the need for administrators to manually configure static routes. You are advised to enable this function on the HQ gateway that interconnects with multiple branches.</p>		
Reverse Route	Whether to enable reverse route injection.	[Example]

Item	Description	Remarks
Injection		Enable
Next-Hop Address	Next-hop address of the route.	<ul style="list-style-type: none"> <li>Optional.</li> <li>The default outbound interface of the route is the virtual tunnel interface associated with the IPsec tunnel.</li> </ul> [Example] 192.168.1.1
Priority	Route priority.	Range: 1–255. Default: 5. [Example] 5
<p><b>IKE Parameters</b></p> <p>The devices at both ends of the IPsec VPN tunnel must have at least one set of the same IKE parameters to establish an IKE SA.</p> <p>All of the following IKE parameters except <b>SA Lifetime</b> must have the same values in the IPsec VPN configuration of the peer device.</p>		
Negotiation Mode	<p>IKE negotiation mode in phase 1. The following modes are supported:</p> <ul style="list-style-type: none"> <li><b>IKEv1 Main Mode:</b> In this mode, identity information is encrypted and protected for higher security.</li> <li><b>IKEv1 Aggressive Mode:</b> In this mode, the negotiation speed is faster, but identity information is not encrypted or protected.</li> </ul>	[Example] IKEv1 Main Mode
Encryption Algorithm	<p>Encryption algorithm used in IKE negotiation for establishing IPsec SAs. The following values are supported:</p> <ul style="list-style-type: none"> <li><b>DES:</b> DES algorithm using 56-bit keys</li> <li><b>3DES:</b> 3DES algorithm using 168-bit keys</li> <li><b>AES-128:</b> AES</li> </ul>	<ul style="list-style-type: none"> <li>Select one or more options from the drop-down list.</li> <li>The default encryption algorithm is <b>AES-128</b>.</li> </ul> [Example] AES-192

Item	Description	Remarks
	<p>algorithm using 128-bit keys</p> <ul style="list-style-type: none"> <li>● <b>AES-192:</b> AES algorithm using 192-bit keys</li> <li>● <b>AES-256:</b> AES algorithm using 256-bit keys</li> </ul> <p>In order of security from high to low: AES-256 &gt; AES-192 &gt; AES-128 &gt; 3DES &gt; DES.</p>	
Authentication Algorithm	<p>Authentication algorithm used in IKE negotiation. The following values are supported:</p> <ul style="list-style-type: none"> <li>● <b>MD5:</b> MD5 algorithm that produces a 128-bit message digest</li> <li>● <b>SHA:</b> SHA1 algorithm that produces a 160-bit message digest</li> <li>● <b>SHA-256:</b> SHA2-256 algorithm that produces a 256-bit message digest</li> <li>● <b>SHA-384:</b> SHA2-384 algorithm that produces a 384-bit message digest</li> <li>● <b>SHA-512:</b> SHA2-512 algorithm that produces a 512-bit message digest</li> </ul> <p>A longer message digest indicates higher security and slower calculation.</p>	<ul style="list-style-type: none"> <li>● Select one or more options from the drop-down list.</li> <li>● The default authentication algorithm is <b>SHA</b>. [Example] MD5</li> </ul>
DH Group	<p>DH group used in IKE negotiation. The following values are supported:</p> <ul style="list-style-type: none"> <li>● <b>GROUP1:</b> 768-bit DH group</li> <li>● <b>GROUP2:</b> 1024-bit DH</li> </ul>	<ul style="list-style-type: none"> <li>● Select one or more options from the drop-down list.</li> <li>● The default value is <b>GROUP5</b>. [Example] GROUP14</li> </ul>

Item	Description	Remarks
	<p>group</p> <ul style="list-style-type: none"> <li>● <b>GROUP5</b>: 1536-bit DH group</li> <li>● <b>GROUP14</b>: 2048-bit DH group</li> <li>● <b>GROUP15</b>: 3072-bit DH group</li> <li>● <b>GROUP16</b>: 4096-bit DH group</li> </ul> <p>The DH group determines the strength of the key used in IKE negotiation. A larger group number indicates higher security and slower key calculation.</p>	
SA Lifetime	<p>IKE SA lifetime.</p> <p>When the lifetime of an IKE SA exceeds this value, the device replaces the old SA with a newly established SA.</p> <p>The actual IKE SA lifetime depends on the negotiation result of the two ends.</p>	<ul style="list-style-type: none"> <li>● Range: 120–604800, in seconds.</li> <li>● The default value is 86400 seconds (one day).</li> </ul> <p>[Example]</p> <p>86400</p>
<p><b>IPsec Parameters</b></p> <p>The devices at both ends of the IPsec tunnel must have at least one set of the same IPsec parameters to establish an IPsec SA.</p> <p>All of the following IPsec parameters except <b>SA Lifetime</b> must have the same values in the IPsec VPN configuration of the peer device.</p>		
Protocol	<p>Security protocol used by IPsec. Currently, only Encapsulating Security Payload (ESP) is supported.</p> <p>The ESP protocol supports packet encryption and</p>	<p>[Example]</p> <p>ESP</p>

Item	Description	Remarks
	authentication.	
Encapsulation Mode	Encapsulation mode of IPsec. Currently, only the tunnel mode is supported.	[Example] Tunnel
Encryption Algorithm	<p>Encryption algorithm used by the IPsec tunnel. The following values are supported:</p> <ul style="list-style-type: none"> <li>● <b>DES</b>: DES algorithm using 56-bit keys</li> <li>● <b>3DES</b>: 3DES algorithm using 168-bit keys</li> <li>● <b>AES-128</b>: AES algorithm using 128-bit keys</li> <li>● <b>AES-192</b>: AES algorithm using 192-bit keys</li> <li>● <b>AES-256</b>: AES algorithm using 256-bit keys</li> <li>● <b>NULL</b>: no encryption</li> </ul> <p>In order of security from high to low: AES-256 &gt; AES-192 &gt; AES-128 &gt; 3DES &gt; DES.</p>	<ul style="list-style-type: none"> <li>● Select one or more options from the drop-down list.</li> <li>● The default encryption algorithm is <b>AES-128</b>.</li> </ul> <p>[Example] AES-192</p>
Authentication Algorithm	<p>Authentication algorithm used by the IPsec tunnel. The following values are supported:</p> <ul style="list-style-type: none"> <li>● <b>MD5</b>: MD5 algorithm that produces a 128-bit message digest</li> <li>● <b>SHA</b>: SHA1 algorithm that produces a 160-bit message digest</li> <li>● <b>SHA-256</b>: SHA2-256 algorithm that produces a 256-bit message digest</li> <li>● <b>SHA-384</b>: SHA2-384 algorithm that produces</li> </ul>	<ul style="list-style-type: none"> <li>● Select one or more options from the drop-down list.</li> <li>● The default authentication algorithm is <b>SHA</b>.</li> </ul> <p>[Example] MD5</p>



Item	Description	Remarks
	<p>a 384-bit message digest</p> <ul style="list-style-type: none"> <li>● <b>SHA-512:</b> SHA2-512 algorithm that produces a 512-bit message digest</li> </ul> <p>A longer message digest indicates higher security and slower calculation.</p>	
<p>Perfect Forward Secrecy</p>	<p>Whether to enable the Perfect Forward Secrecy (PFS) function.</p> <p>When PFS is enabled, an additional DH key exchange is performed. In this way, the keys used in IPsec SAs remain indecipherable even if the key used in the IKE SA is deciphered.</p>	<p>[Example]</p> <p><b>Enable</b></p>
<p>DH Group</p>	<p>DH group used by PFS. The following values are supported:</p> <ul style="list-style-type: none"> <li>● <b>GROUP1:</b> 768-bit DH group</li> <li>● <b>GROUP2:</b> 1024-bit DH group</li> <li>● <b>GROUP5:</b> 1536-bit DH group</li> <li>● <b>GROUP14:</b> 2048-bit DH group</li> <li>● <b>GROUP15:</b> 3072-bit DH group</li> <li>● <b>GROUP16:</b> 4096-bit DH group</li> </ul> <p>A larger group number indicates higher security and slower key calculation.</p>	<ul style="list-style-type: none"> <li>● Select one or more options from the drop-down list.</li> <li>● When PFS is enabled, <b>GROUP5</b> is set by default.</li> </ul> <p>[Example]</p> <p>GROUP14</p>
<p>SA Lifetime</p>	<p>IPsec SA lifetime.</p>	<ul style="list-style-type: none"> <li>● Range: 60–604800, in seconds.</li> </ul>

Item	Description	Remarks
	<p>When the lifetime of an IPsec SA exceeds this value, the device replaces the old SA with a newly established SA.</p> <p>The actual IPsec SA lifetime depends on the negotiation result of the two ends.</p>	<ul style="list-style-type: none"> <li>The default value is 3600 seconds (1 hour). [Example] 3000</li> </ul>
Tunnel MTU	<p>Maximum number of bytes that can be transmitted over the IPsec tunnel at a time.</p>	<ul style="list-style-type: none"> <li>The default value is 1400 bytes.</li> <li>The tunnel MTU must be smaller than the outbound interface MTU. [Example] 1480</li> </ul>


(7) Click **Finish** to save configurations.

#### Follow-up Procedure

- After you complete IPsec tunnel parameter configuration on the wizard, the system automatically synchronizes the following configurations to the firewall.

Item	Description
IPv4 Address Object	<p>IPv4 address objects (subnet or host addresses at both ends of the VPN tunnel) are added to identify the local and peer networks configured in interesting traffic.</p>
Security Zone	<p>A security zone is added:</p> <ul style="list-style-type: none"> <li><b>Name:</b> The value is the same as that of <b>Tunnel Name</b> set for the IPsec tunnel.</li> <li><b>Interface List:</b> The IPsec tunnel interface is added to the list.</li> </ul>
Tunnel Interface	<p>The IPsec tunnel interface is added:</p> <ul style="list-style-type: none"> <li><b>Security Zone:</b> The value is the same as that of <b>Tunnel Name</b> set for the IPsec tunnel.</li> <li><b>Tunnel Local Address:</b> IP address of the outbound interface.</li> <li><b>Tunnel Remote Address:</b> IP address used by the peer end to establish the IPsec tunnel. The value is the same as that of <b>Peer Address</b> set in <b>Configure Authentication</b>.</li> </ul>

Item	Description
Static Routing	<p>The static route to the peer intranet is added:</p> <ul style="list-style-type: none"> <li>● <b>Dest. IP Range/Mask:</b> Peer network address set in interesting traffic configuration.</li> <li>● <b>Interface:</b> IPsec tunnel interface.</li> <li>● <b>Priority:</b> 5</li> </ul>
Security Policy	<p>Security policies are added to permit traffic from intranets at both ends of the tunnel in the inbound and outbound directions:</p> <ul style="list-style-type: none"> <li>● Security policy in the inbound direction:                             <ul style="list-style-type: none"> <li>○ <b>Src. Security Zone:</b> The value is the same as that of <b>Tunnel Name</b> set for the IPsec tunnel. (The tunnel interface is added to the zone.)</li> <li>○ <b>Src. Address:</b> Peer network address set in interesting traffic configuration.</li> <li>○ <b>Dest. Security Zone:</b> any</li> <li>○ <b>Dest. Address:</b> Local network address set in interesting traffic configuration.</li> <li>○ <b>Action:</b> permit</li> </ul> </li> <li>● Security policy in the outbound direction:                             <ul style="list-style-type: none"> <li>○ <b>Src. Security Zone:</b> any</li> <li>○ <b>Src. Address:</b> Local network address set in interesting traffic configuration.</li> <li>○ <b>Src. Security Zone:</b> The value is the same as that of <b>Tunnel Name</b> set for the IPsec tunnel. (The tunnel interface is added to the zone.)</li> <li>○ <b>Dest. Address:</b> Peer network address set in interesting traffic configuration.</li> <li>○ <b>Action:</b> permit</li> </ul> </li> </ul>
Local Defense Policy	<p>A local defense policy is added to permit IKE and ESP protocol traffic to the local device and ensure proper operation of the IPsec tunnel.</p> <ul style="list-style-type: none"> <li>● <b>Src. Security Zone:</b> any</li> <li>● <b>Src. Address:</b> any</li> <li>● <b>Dest. Address:</b> any</li> <li>● <b>Service:</b> IKE, ESP</li> <li>● <b>Action:</b> permit</li> </ul>

- After completing IPsec tunnel policy configuration, you can view the configurations on the **Custom Tunnel** page.
  - Toggle on or off  to enable or disable the tunnel policy.

- Click **View Details** to view detailed negotiation parameters of the IPsec tunnel.
- Click **Edit** to modify tunnel configurations.
- Click **Delete** to delete the IPsec tunnel policy.

## 7.18.4 Custom Tunnel

### Application Scenario

In addition to using the configuration wizard, you can also manually configure IPsec tunnels for the firewall. Compared with the configuration wizard, custom tunnel configuration is more flexible but also more complex. To prevent IPsec VPN from being unavailable due to configuration errors, you are advised to use the configuration wizard to configure IPsec tunnels.

### Prerequisites

Before configuring IPsec VPN, you have completed the following steps:

- Create tunnel interfaces to be bound to IPsec tunnel policies based on actual networking requirements.
- In a point-to-point IPsec VPN scenario, obtain the IP address or domain name of the peer end, as well as the range of addresses to be accessed on the intranet.
- Verify that devices at both ends of the IPsec tunnel to be established are reachable to each other.
- If the peer network of the tunnel is configured with a domain name, you need to configure an available DNS server for the firewall to enable domain name resolution.
- Determine the security parameters of the IPsec tunnel and pre-shared key together with the administrator of the peer device.

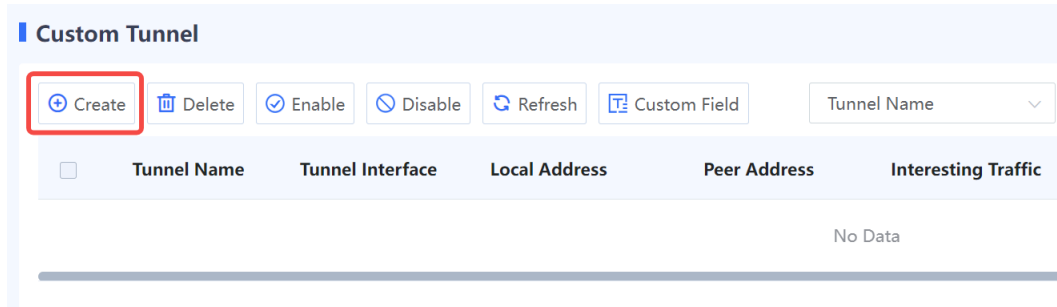
---

#### Caution

- Both communication ends need to negotiate with each other to establish an IPsec tunnel, and IPsec VPN must be enabled on devices at both ends of the IPsec tunnel.
  - The IKE parameters and IPsec parameters (including the security protocol, encryption algorithm, authentication algorithm, and packet encapsulation mode) configured for the devices at both ends of the IPsec tunnel must be the same. Otherwise, tunnel negotiation fails.
- 

### Procedure

- (1) Choose **Network > IPsec VPN > Custom Tunnel**.



(2) Click **Create** to access the **Create Custom Tunnel Details** page.

①
②
③

**Basic Config**
Interesting Traffic Config
Security Parameter Config

\* Scenario  Point-to-Point ⓘ  Point-to-Multipoint ⓘ

\* Tunnel Name  Enter Tunnel Name

Description

\* Enabled State  Enable  Disable

\* Tunnel Interface  ⊕ Add Tunnel Interface

\* Authentication Mode

\* Password

\* Confirm Key

\* Local Address  Interface ⓘ  IP ⓘ

\* Peer Address  Ping

Enable Peer Identity Authentication

\* Local ID Type

DPD Type

DPD Retry Interval  Second

Cancel
Next

Item	Description	Remarks
Scenario	Select the IPsec tunnel	On the firewall, one

Item	Description	Remarks
	<p>type based on the deployment scenario:</p> <ul style="list-style-type: none"> <li>● <b>Point-to-Point:</b> applies to scenarios where the peer end has a fixed IP address, such as IPsec VPN deployment at an enterprise branch.</li> <li>● <b>Point-to-Multipoint:</b> applies to scenarios where the peer end IP address is not fixed or multiple peer ends exist, such as IPsec VPN deployment at an enterprise HQ. In this case, the peer end needs to initiate tunnel negotiation.</li> </ul>	<p>point-to-multipoint IPsec VPN tunnel and multiple point-to-point IPsec VPN tunnels can be configured.</p> <p>[Example]</p> <p><b>Point-to-Point</b></p>
Tunnel Name	IPsec tunnel name.	<p>Characters such as ~!#%^&amp;*+ {};:"',/&lt;&gt;? are not allowed.</p> <p>[Example]</p> <p>ipsec_1</p>
Description	Tunnel description. Provide brief description to help the administrator understand the function of the tunnel.	<p>[Example]</p> <p>Mutual access between branch at 11.1.1.2 and HQ at 10.1.1.2</p>
Enabled State	Whether to enable the IPsec tunnel policy.	<p>[Example]</p> <p><b>Enable</b></p>
Tunnel Interface	Tunnel interface associated with the IPsec tunnel policy. IPsec data packets are encapsulated and decapsulated on this interface.	<ul style="list-style-type: none"> <li>● Select a configured tunnel interface from the drop-down list.</li> <li>● To add a tunnel interface, click <b>Add Tunnel Interface</b>.</li> </ul> <p>[Example]</p> <p>vti2</p>
Authentication Mode	<p>Identity authentication mode of both ends of the tunnel.</p> <p>Currently, only pre-shared key authentication is</p>	<p>[Example]</p> <p>Pre-shared Key</p>

Item	Description	Remarks
	supported.	
Key	Key string for identity authentication in pre-shared key authentication mode.	<ul style="list-style-type: none"> <li>● Length range: 6 to 16 characters.</li> <li>● Configure the same identity authentication mode (pre-shared key) and key for both ends. [Example] Ruijie123</li> </ul>
Local Address	Select the local interface or IP address for establishing a tunnel with the peer end.	<ul style="list-style-type: none"> <li>● If <b>Interface</b> is selected, specify the physical interface to which the IPsec tunnel policy applies. If the interface has multiple IP addresses, any of the IP addresses can be used to establish the IPsec tunnel.</li> <li>● If <b>IP</b> is selected, specify a local IP address as the local address of the IPsec tunnel.</li> <li>● The value must be the same as that of <b>Peer Address</b> configured for the peer device.</li> </ul>
Peer Address	IP address or domain name used by the peer device to establish the tunnel.	<ul style="list-style-type: none"> <li>● This parameter is mandatory in a point-to-point scenario.</li> <li>● After entering the IP address or domain name, click <b>Ping</b> to verify that the devices at both ends are reachable to each other.</li> <li>● The value must be the same as that of <b>Local Address</b> configured for the peer device. [Example] 40.0.0.5</li> </ul>
Peer Identity Authentication	Whether to enable identity authentication for the peer device.	Toggle it on or off to enable or disable this function. After enabling this function, you need to set identity authentication information for the peer device.

Item	Description	Remarks
		[Example] Enable
Local ID Type	<p>A local ID identifies the local device and is used by the peer device to authenticate the local device. The following types are supported:</p> <ul style="list-style-type: none"> <li>● <b>IPV4_ADDRESS</b>: An IPv4 address is used as the local ID for IKE negotiation.</li> <li>● <b>FQDN</b>: A Fully Qualified Domain Name (FQDN) string is used as the local ID for IKE negotiation.</li> <li>● <b>USER_FQDN</b>: A user FQDN string is used as the local ID for IKE negotiation.</li> </ul>	<p>If <b>IPV4_ADDRESS</b> is selected, the device uses the local IP address as the local ID.</p> <p>[Example]                      IPV4_ADDRESS</p>
Local ID	<p>String that identifies the local device for identity authentication.</p>	<ul style="list-style-type: none"> <li>● The value must be the same as that of <b>Peer ID</b> configured for the peer device.</li> <li>● The string format varies with the local ID type:                             <ul style="list-style-type: none"> <li>○ <b>FQDN</b>: Domain name of the local end. Example: <b>aaa.com</b>.</li> <li>○ <b>USER_FQDN</b>: User domain name of the local end in the format of <i>Username@Domain name</i>. Example: <b>julia@aaa.com</b>.</li> </ul> </li> </ul>
Peer ID Type	<p>A peer ID identifies the peer device for identity authentication. The following types are supported:</p> <ul style="list-style-type: none"> <li>● <b>IPV4_ADDRESS</b>: The peer end uses an IPv4 address as the peer ID for identity authentication.</li> <li>● <b>FQDN</b>: The peer end uses an FQDN string as the peer ID for identity</li> </ul>	<ul style="list-style-type: none"> <li>● This parameter is mandatory when <b>Peer Identity Authentication</b> is enabled.</li> <li>● The value must be the same as that of <b>Local ID Type</b> configured for the peer device. Obtain the value from the administrator of the peer device.</li> </ul> <p>[Example]                      IPV4_ADDRESS</p>



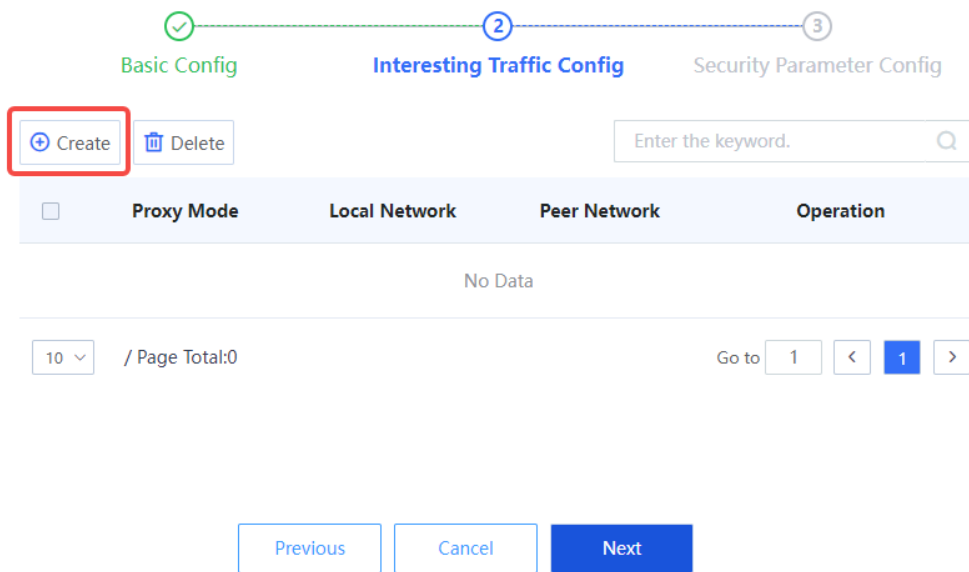
Item	Description	Remarks
	<p>authentication.</p> <ul style="list-style-type: none"> <li>● <b>USER_FQDN:</b> The peer end uses a user FQDN string as the peer ID for identity negotiation.</li> </ul>	
Peer ID	String that identifies the peer device for identity authentication.	<ul style="list-style-type: none"> <li>● This parameter is mandatory when <b>Peer Identity Authentication</b> is enabled.</li> <li>● The value must be the same as that of <b>Local ID</b> configured for the peer device. Obtain the value from the administrator of the peer device.</li> <li>● The string format varies with the peer ID type: <ul style="list-style-type: none"> <li>○ <b>IPV4_ADDRESS:</b> IP address of the peer end. Example: 10.1.1.1.</li> <li>○ <b>FQDN:</b> Domain name of the peer end. Example: <b>bbb.com</b>.</li> <li>○ <b>USER_FQDN:</b> User domain name of the peer end in the format of <i>Username@Domain name</i>. Example: <b>susan@bbb.com</b>.</li> </ul> </li> </ul>
DPD Type	<p>DPD is used to detect peer status of an IPsec tunnel and remove abnormal tunnels in a timely manner.</p> <p>Two DPD modes are supported:</p> <ul style="list-style-type: none"> <li>● <b>Idle Mode:</b> If the local end does not receive a response message from the peer end after sending a message, it sends a DPD message to the peer end.</li> <li>● <b>Regular Mode:</b> The local end sends DPD messages periodically based on the configured DPD detection interval.</li> </ul>	<p>This parameter is supported in a point-to-point scenario.</p> <p>[Example]</p> <p>Idle Mode</p>

Item	Description	Remarks
DPD Detection Interval	In regular mode, set the interval between two DPD detections, in seconds.	The default value is 30 seconds. [Example] 30
DPD Retry Interval	Interval for retransmitting DPD messages. After sending a DPD request message, if the local end does not receive a response message within the retry interval, it retransmits the DPD request message. If the local end does not receive a response message after three retransmissions, it regards the peer end as unavailable and automatically removes the IPsec tunnel.	The default value is 5 seconds. [Example] 3
Reverse Route Injection	Whether to enable reverse route injection. When reverse route injection is enabled, the device automatically adds the route to the protected peer network segment to the routing table.	This parameter is supported in a point-to-multipoint scenario. [Example] Enable
Next-Hop Address	Next-hop address of the route.	<ul style="list-style-type: none"> <li>● This parameter takes effect only when reverse route injection is enabled.</li> <li>● The default outbound interface of the route is the IPsec tunnel interface.</li> </ul> [Example] 192.168.1.1
Priority	Route priority.	<ul style="list-style-type: none"> <li>● This parameter takes effect only when reverse route injection is enabled.</li> </ul>

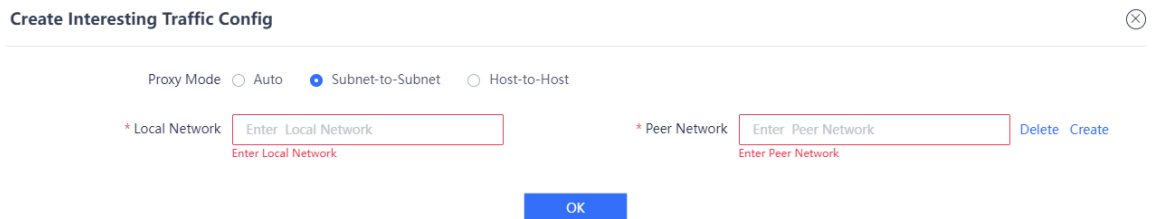
Item	Description	Remarks
		<ul style="list-style-type: none"> <li>Range: 1–255. Default: 5. [Example]</li> </ul> <p>5</p>

(3) Click **Next** to configure interesting traffic of the IPsec tunnel.

a Click **Create** to access the **Create Interesting Traffic Config** page.



b Configure interesting traffic based on the network segments or host addresses at both ends of the tunnel that require secure mutual access.



Item	Description	Remarks
Proxy Mode	Set the proxy mode for interesting traffic based on the ranges of addresses at both ends of the tunnel that require secure mutual access:	[Example] Subnet-to-Subnet

Item	Description	Remarks
	<ul style="list-style-type: none"> <li>● <b>Auto:</b> Traffic to be encrypted is automatically identified based on the interesting traffic defined at the peer end, and no configuration is performed at the local end.</li> <li>● <b>Subnet-to-Subnet:</b> Data flows between two specific subnets are protected.</li> <li>● <b>Host-to-Host:</b> Data flows between two specific hosts are protected.</li> </ul>	
Local Network	Source address of interesting traffic. Typically, a network segment or specific host address to be protected on the local intranet is set.	<p>The address format varies with the proxy mode:</p> <ul style="list-style-type: none"> <li>● <b>Subnet-to-Subnet:</b> Enter an IP range. Example: 192.168.1.0/255.255.255.0 or 192.168.1.0/24.</li> <li>● <b>Host-to-Host:</b> Enter an IP address. Example: 192.168.1.1.</li> </ul>
Peer Network	Destination address of interesting traffic. Typically, a network segment or specific host address to be protected on the peer intranet is set.	<p>The address format varies with the proxy mode:</p> <ul style="list-style-type: none"> <li>● <b>Subnet-to-Subnet:</b> Enter an IP range. Example: 192.168.1.0/255.255.255.0 or 192.168.1.0/24.</li> <li>● <b>Host-to-Host:</b> Enter an IP address. Example: 192.168.1.1.</li> </ul>

- c Click **OK** to save interesting traffic configuration. Click **Create** to add more interesting traffic.

Basic Config ✓ Interesting Traffic Config 2 Security Parameter Config 3

<input type="checkbox"/>	Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/>	Subnet-to-Subnet	1.1.1.0/24	2.2.2.0/24	<a href="#">Edit</a> <a href="#">Delete</a>

10 ▾ / Page Total:1 Go to

(4) Click **Next** to configure the security parameters used in IKE negotiation for establishing an IPsec tunnel.



**IKE Parameter**

\* Negotiation Mode: IKEv1 Main Mode

\* Encryption Algorithm: AES-128

\* Verification Algorithm: SHA

\* DH Group: GROUP5

\* SA Lifetime: 86400 Second

---

**IPsec Parameter**

\* Protocol: ESP

\* Encapsulation Mode: Tunnel

\* Encryption Algorithm: AES-128

\* Verification Algorithm: SHA

Perfect Forward Secrecy:

\* SA Lifetime: 3600 Second

Tunnel MTU: 1400 Second

Previous Cancel Finish

Item	Description	Remarks
<p><b>IKE Parameters</b></p> <p>The devices at both ends of the IPsec VPN tunnel must have at least one set of the same IKE parameters to establish an IKE SA.</p> <p>All of the following IKE parameters except <b>SA Lifetime</b> must have the same values in the IPsec VPN configuration of the peer device.</p>		
Negotiation Mode	<p>IKE negotiation mode in phase 1. The following modes are supported:</p> <ul style="list-style-type: none"> <li>● <b>IKEv1 Main Mode:</b> In this mode, identity information is encrypted and protected for higher security.</li> </ul>	<p>[Example]</p> <p>IKEv1 Main Mode</p>

Item	Description	Remarks
	<ul style="list-style-type: none"> <li>● <b>IKEv1 Aggressive Mode:</b> In this mode, the negotiation speed is faster, but identity information is not encrypted or protected.</li> </ul>	
Encryption Algorithm	<p>Encryption algorithm used in IKE negotiation for establishing IPsec SAs. The following values are supported:</p> <ul style="list-style-type: none"> <li>● <b>DES:</b> DES algorithm using 56-bit keys</li> <li>● <b>3DES:</b> 3DES algorithm using 168-bit keys</li> <li>● <b>AES-128:</b> AES algorithm using 128-bit keys</li> <li>● <b>AES-192:</b> AES algorithm using 192-bit keys</li> <li>● <b>AES-256:</b> AES algorithm using 256-bit keys</li> </ul> <p>In order of security from high to low: AES-256 &gt; AES-192 &gt; AES-128 &gt; 3DES &gt; DES.</p>	<ul style="list-style-type: none"> <li>● Select one or more options from the drop-down list.</li> <li>● The default encryption algorithm is <b>AES-128</b>.</li> </ul> <p>[Example] AES-192</p>
Authentication Algorithm	<p>Authentication algorithm used in IKE negotiation. The following values are supported:</p> <ul style="list-style-type: none"> <li>● <b>MD5:</b> MD5 algorithm that produces a 128-bit message digest</li> <li>● <b>SHA:</b> SHA1 algorithm that produces a 160-bit message digest</li> <li>● <b>SHA-256:</b> SHA2-256 algorithm that produces a 256-bit message digest</li> <li>● <b>SHA-384:</b> SHA2-384 algorithm that produces a 384-bit message digest</li> <li>● <b>SHA-512:</b> SHA2-512 algorithm that produces a 512-bit message digest</li> </ul> <p>A longer message digest indicates higher security and slower calculation.</p>	<ul style="list-style-type: none"> <li>● Select one or more options from the drop-down list.</li> <li>● The default authentication algorithm is <b>SHA</b>.</li> </ul> <p>[Example] MD5</p>

Item	Description	Remarks
DH Group	<p>DH group used in IKE negotiation. The following values are supported:</p> <ul style="list-style-type: none"> <li>● <b>GROUP1</b>: 768-bit DH group</li> <li>● <b>GROUP2</b>: 1024-bit DH group</li> <li>● <b>GROUP5</b>: 1536-bit DH group</li> <li>● <b>GROUP14</b>: 2048-bit DH group</li> <li>● <b>GROUP15</b>: 3072-bit DH group</li> <li>● <b>GROUP16</b>: 4096-bit DH group</li> </ul> <p>The DH group determines the strength of the key used in IKE negotiation. A larger group number indicates higher security and slower key calculation.</p>	<ul style="list-style-type: none"> <li>● Select one or more options from the drop-down list.</li> <li>● The default value is <b>GROUP5</b>.</li> </ul> <p>[Example] GROUP14</p>
SA Lifetime	<p>IKE SA lifetime.</p> <p>The actual IKE SA lifetime depends on the negotiation result of the two ends.</p>	<ul style="list-style-type: none"> <li>● Range: 120–604800, in seconds.</li> <li>● The default value is 86400 seconds (one day).</li> </ul> <p>[Example] 86400</p>
<p><b>IPsec Parameters</b></p> <p>The devices at both ends of the IPsec tunnel must have at least one set of the same IPsec parameters to establish an IPsec SA.</p> <p>All of the following IPsec parameters except <b>SA Lifetime</b> must have the same values in the IPsec VPN configuration of the peer device.</p>		
Protocol	<p>Security protocol used by IPsec. Currently, only ESP is supported.</p> <p>The ESP protocol supports packet encryption and authentication.</p>	<p>[Example] ESP</p>
Encapsulation Mode	<p>Encapsulation mode of IPsec. Currently, only the tunnel mode is supported.</p>	<p>[Example] Tunnel</p>



Item	Description	Remarks
Encryption Algorithm	<p>Encryption algorithm used by the IPsec tunnel. The following values are supported:</p> <ul style="list-style-type: none"> <li>● <b>DES</b>: DES algorithm using 56-bit keys</li> <li>● <b>3DES</b>: 3DES algorithm using 168-bit keys</li> <li>● <b>AES-128</b>: AES algorithm using 128-bit keys</li> <li>● <b>AES-192</b>: AES algorithm using 192-bit keys</li> <li>● <b>AES-256</b>: AES algorithm using 256-bit keys</li> <li>● <b>NULL</b>: no encryption</li> </ul> <p>In order of security from high to low: AES-256 &gt; AES-192 &gt; AES-128 &gt; 3DES &gt; DES.</p>	<ul style="list-style-type: none"> <li>● Select one or more options from the drop-down list.</li> <li>● The default encryption algorithm is <b>AES-128</b>.</li> </ul> <p>[Example] AES-192</p>
Authentication Algorithm	<p>Authentication algorithm used by the IPsec tunnel. The following values are supported:</p> <ul style="list-style-type: none"> <li>● <b>MD5</b>: MD5 algorithm that produces a 128-bit message digest</li> <li>● <b>SHA</b>: SHA1 algorithm that produces a 160-bit message digest</li> <li>● <b>SHA-256</b>: SHA2-256 algorithm that produces a 256-bit message digest</li> <li>● <b>SHA-384</b>: SHA2-384 algorithm that produces a 384-bit message digest</li> <li>● <b>SHA-512</b>: SHA2-512 algorithm that produces a 512-bit message digest</li> </ul> <p>A longer message digest indicates higher security and slower calculation.</p>	<ul style="list-style-type: none"> <li>● Select one or more options from the drop-down list.</li> <li>● The default authentication algorithm is <b>SHA</b>.</li> </ul> <p>[Example] MD5</p>
Perfect Forward Secrecy	<p>Whether to enable the PFS function.</p> <p>When PFS is enabled, an additional DH key exchange is</p>	<p>[Example] <b>Enable</b></p>

Item	Description	Remarks
	performed. In this way, the keys used in IPsec SAs remain indecipherable even if the key used in the IKE SA is deciphered.	
DH Group	<p>DH group used by PFS. The following values are supported:</p> <ul style="list-style-type: none"> <li>● <b>GROUP1</b>: 768-bit DH group</li> <li>● <b>GROUP2</b>: 1024-bit DH group</li> <li>● <b>GROUP5</b>: 1536-bit DH group</li> <li>● <b>GROUP14</b>: 2048-bit DH group</li> <li>● <b>GROUP15</b>: 3072-bit DH group</li> <li>● <b>GROUP16</b>: 4096-bit DH group</li> </ul> <p>A larger group number indicates higher security and slower key calculation.</p>	<ul style="list-style-type: none"> <li>● Select one or more options from the drop-down list.</li> <li>● When PFS is enabled, <b>GROUP5</b> is set by default.</li> </ul> <p>[Example] GROUP14</p>
SA Lifetime	<p>IPsec SA lifetime.</p> <p>When the lifetime of an IPsec SA exceeds this value, the device replaces the old SA with a newly established SA.</p> <p>The actual IPsec SA lifetime depends on the negotiation result of the two ends.</p>	<ul style="list-style-type: none"> <li>● Range: 60–604800, in seconds.</li> <li>● The default value is 3600 seconds (1 hour).</li> </ul> <p>[Example] 3000</p>
Tunnel MTU	Maximum number of bytes that can be transmitted over the IPsec tunnel at a time.	<ul style="list-style-type: none"> <li>● The default value is 1400 bytes.</li> <li>● The tunnel MTU must be smaller than the outbound interface MTU.</li> </ul> <p>[Example] 1480</p>

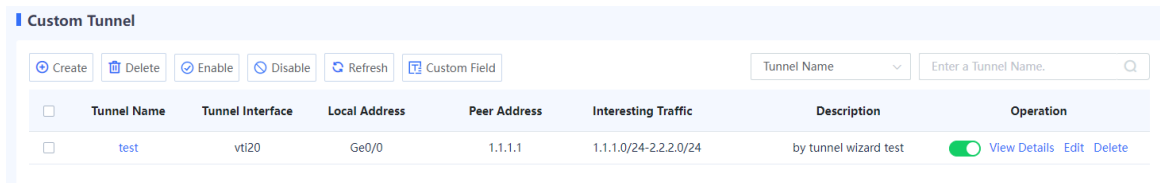
(5) After verifying the configurations, click **Finish** to save the configurations. To modify the configurations, click **Previous**.

**Follow-up Procedure**

- Different from configuration on the wizard, the system does not generate other IPsec VPN configurations (including security policies and routes) after a custom IPsec tunnel is created. You need to configure at least the following parameters for IPsec VPN to work properly.

Item	Description	Configuration Example (For Reference Only)
Routing	Configure routing to forward traffic to be transmitted over the IPsec tunnel to the tunnel interface for IPsec processing.	<ul style="list-style-type: none"> <li>● <b>Dest. IP Range/Mask:</b> Peer network address set in interesting traffic configuration.</li> <li>● <b>Interface:</b> Tunnel interface associated with the IPsec tunnel.</li> <li>● <b>Priority:</b> 5</li> </ul>
Security Policy	Configure security policies to permit traffic from intranets at both ends of the tunnel in the inbound and outbound directions:	<ul style="list-style-type: none"> <li>● Security policy in the inbound direction:                             <ul style="list-style-type: none"> <li>○ <b>Src. Security Zone:</b> untrust</li> <li>○ <b>Src. Address:</b> Peer network address set in interesting traffic configuration.</li> <li>○ <b>Dest. Security Zone:</b> trust</li> <li>○ <b>Dest. Address:</b> Local network address set in interesting traffic configuration.</li> <li>○ <b>Action:</b> permit</li> </ul> </li> <li>● Security policy in the outbound direction:                             <ul style="list-style-type: none"> <li>○ <b>Src. Security Zone:</b> any</li> <li>○ <b>Src. Address:</b> Local network address set in interesting traffic configuration.</li> <li>○ <b>Dest. Security Zone:</b> untrust</li> <li>○ <b>Dest. Address:</b> Peer network address set in interesting traffic configuration.</li> <li>○ <b>Action:</b> permit</li> </ul> </li> </ul>

- You can modify or delete a custom tunnel.



- Toggle on or off to enable or disable the tunnel policy.
- Click **View Details** to view detailed negotiation parameters of the IPsec tunnel.
- Click **Edit** to modify tunnel configurations.
- Click **Delete** to delete the IPsec tunnel policy.

### 7.18.5 Advanced Settings

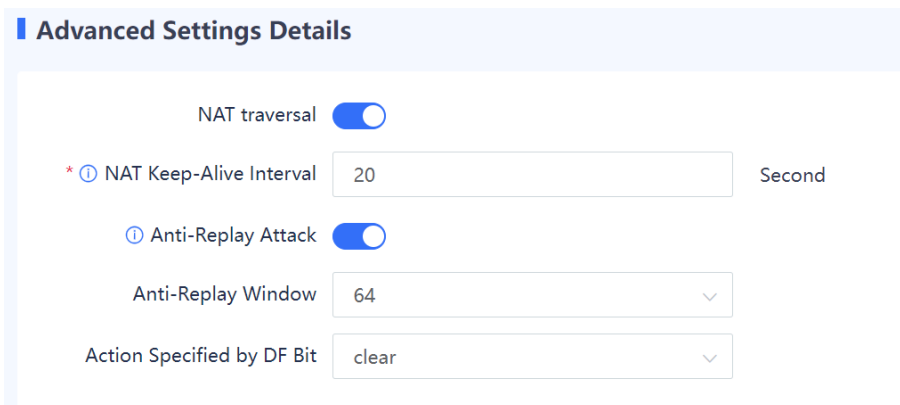
#### Application Scenario

You can configure advanced settings for IPsec VPN to meet VPN function requirements in different scenarios.

Advanced settings take effect globally and apply to all IPsec tunnels created on the device. If you have no special requirements, it is recommended that the default settings be used.

#### Procedure

- (1) Choose **Network > IPsec VPN > Advanced Settings Details**.
- (2) Modify the advanced settings of IPsec VPN.



Item	Description	Remarks
NAT Traversal	Whether to enable NAT traversal. When this function is enabled, the device adds a standard UDP header between the new IP header and ESP header of	Enabled by default. [Example] Enable

Item	Description	Remarks
	<p>an IPsec-encapsulated packet so that the packet can traverse the NAT device.</p>	
<p>NAT Keep-Alive Interval</p>	<p>Sending interval of NAT keepalive packets.</p> <p>The NAT mapping session on a NAT device has a lifetime. If no packet traverses the device long after the IPsec tunnel is established, the NAT session entry is deleted. As a result, tunnel data transmission is interrupted. To prevent NAT session entries from being aged, an IKE SA on the intranet side of the NAT device sends NAT keepalive packets to its peer end at a certain interval to maintain the NAT session.</p>	<ul style="list-style-type: none"> <li>● This parameter takes effect only when <b>NAT Traversal</b> is enabled.</li> <li>● The default NAT keep-alive interval is 20 seconds.</li> </ul> <p>[Example] 20 seconds</p>
<p>Anti-Replay Attack</p>	<p>Whether to enable the anti-replay attack function.</p> <p>A replay attack occurs when an attacker obtains and sends packets that have been received by the target host to deceive the host.</p> <p>When this function is enabled, IPsec detects replay packets through the anti-replay window mechanism and discards these packets before decapsulating them.</p> <p>After anti-replay attack parameters are modified, the modification takes effect for newly negotiated SAs, but does not take effect for existing SAs. This ensures normal service running.</p>	<p>Enabled by default.</p> <p>[Example] 20 seconds</p>

Item	Description	Remarks
<p>Anti-Replay Window</p>	<p>Anti-replay window size. The following values are supported: 64 bits, 128 bits, 256 bits, and 1024 bits.</p> <p>After the anti-replay window size is modified, the modification takes effect for newly negotiated SAs, but does not take effect for existing SAs. This ensures normal service running.</p>	<ul style="list-style-type: none"> <li>● This parameter takes effect only when the anti-replay attack function is enabled.</li> <li>● The default value is 64 bits.</li> <li>● In specific situations, the sequence numbers of some service data packets may differ from those of common data packets. In this case, you can increase the IPsec anti-replay window size to a proper value to meet service requirements.</li> <li>● However, a large anti-replay window increases the system cost and deteriorates system performance. It is recommended a small anti-replay window be used as required.</li> </ul> <p>[Example]</p> <p>64</p>
<p>Action Specified by DF Bit</p>	<p>Configure the Don't Fragment (DF) flag bit value of the outer IP header of the IPsec packet to control whether to allow fragmentation of the IPsec-encapsulated packets:</p> <ul style="list-style-type: none"> <li>● <b>clear</b>: The DF flag bit is set to 0, which indicates that IPsec-encapsulated packets can be fragmented.</li> <li>● <b>set</b>: The DF flag bit is set to 1, which indicates that IPsec-encapsulated packets cannot be fragmented.</li> <li>● <b>copy</b>: The DF flag bit of the outer IP header is set to the same as the DF flag bit of the original packet.</li> </ul>	<ul style="list-style-type: none"> <li>● If IPsec packet fragmentation is not allowed, the MTUs of the interfaces on the IPsec packet forwarding path must exceed the IPsec packet length. Otherwise, IPsec packets are discarded, affecting normal service data transmission.</li> <li>● If you cannot determine whether the MTU of each interface on the forwarding path is larger than the length of IPsec packets, you are advised to configure IPsec packet fragmentation (that is, set the action to <b>clear</b>).</li> <li>● The default action is <b>clear</b>, which allows IPsec packet fragmentation.</li> </ul> <p>[Example]</p>

Item	Description	Remarks
		clear

(3) After verifying the configuration, click **Save**.

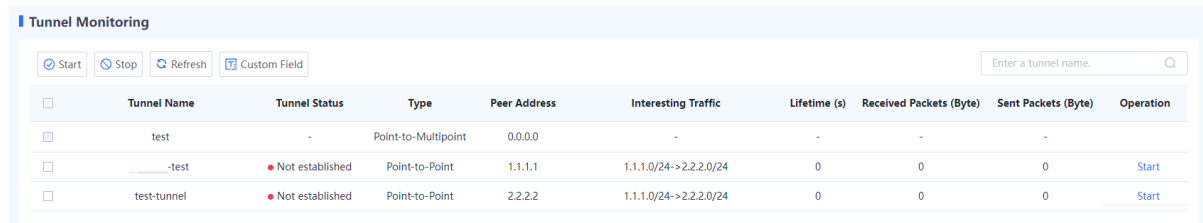
### 7.18.6 Tunnel Monitoring

#### Application Scenario

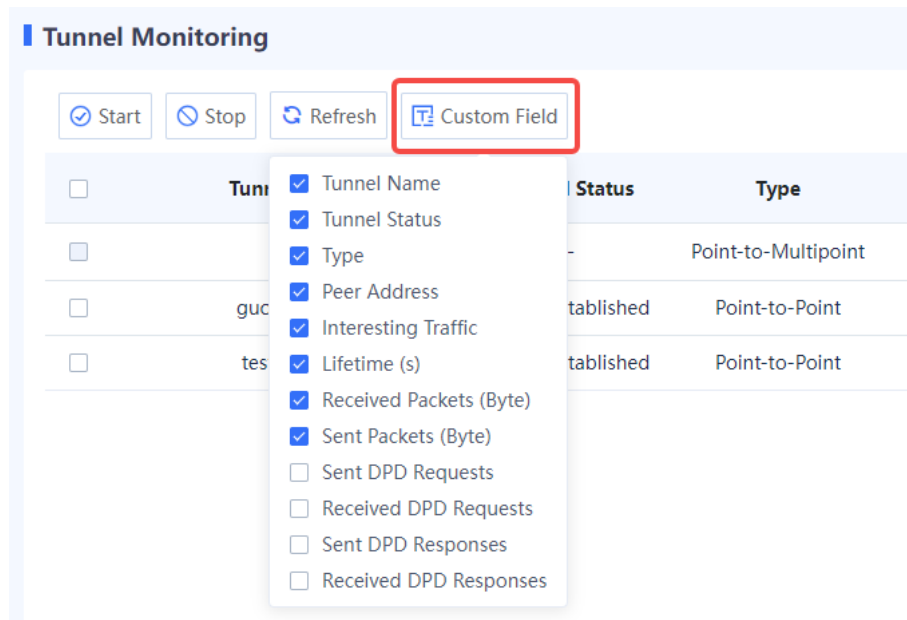
By using this function, the administrator can view configuration and status information about all IPsec tunnels to check whether IPsec VPN is working properly. In addition, the IPsec tunnels can be enabled or disabled.

#### Procedure

(1) Choose **Network > IPsec VPN > Tunnel Monitoring**.



(2) (Optional) Click **Custom Field** to set the fields to be displayed.



(3) The web UI displays selected configuration and status information about IPsec tunnels, as described in the following table.

Item	Description
Tunnel Name	IPsec tunnel name.
Tunnel Status	Tunnel status, indicating whether IPsec tunnel negotiation is completed and whether the tunnel is successfully established.
Type	Tunnel type.
Peer Address	Peer IP address of the tunnel.
Interesting Traffic	Source and destination addresses of the data flows to be encrypted and transmitted over the tunnel.
Lifetime (s)	Remaining lifetime of the current IPsec SA. After the IPsec SA lifetime expires, the device replaces the old SA with a newly negotiated SA and updates the tunnel connection.
Received Packets (Byte)	Total number of bytes that the local end receives from the IPsec tunnel.
Sent Packets (Byte)	Total number of bytes that the local end sends to the IPsec tunnel.
Sent DPD Requests	Number of times the local end sends DPD request messages to the peer end.
Received DPD Requests	Number of times the local end receives DPD request messages from the peer end.
Sent DPD Responses	Number of times the local end sends DPD response messages to the peer end.
Received DPD Responses	Number of times the local end receives DPD response messages from the peer end.

**Note**

For a point-to-multipoint IPsec tunnel:

- The local end of the tunnel can only passively respond to the negotiation request initiated by the peer end, and establish a data transmission channel based on the negotiation result. If no negotiation request is received, only the tunnel name and type are displayed, interesting traffic is displayed as 0.0.0.0, and all the other information is empty.
- The device can establish VPN connections with multiple branch sites simultaneously. The administrator can view the running status and connection information of the data



transmission channels established between the device and branch sites on the tunnel monitoring page.

### Follow-up Procedure

- Click **Refresh** to view the latest IPsec tunnel information.
- Enter a tunnel name in the search box in the upper right corner of the page to search for an IPsec tunnel.
- Enable an IPsec tunnel: Click **Start** in the **Operation** column of a tunnel to enable an IPsec tunnel that has been manually terminated.
- Enable IPsec tunnels in a batch: Select multiple tunnels to be enabled and click **Start**.
- Disable an IPsec tunnel: When an IPsec tunnel is no longer needed, you can click **Stop** in the **Operation** column of the tunnel to terminate it.
- Disable IPsec tunnels in a batch: Select multiple tunnels to be disabled and click **Stop**.

## 7.18.7 Viewing IPsec VPN Logs

### Application Scenario

IPsec VPN logs record important events and abnormal information during the working process of IPsec tunnels. The logs help administrators obtain IPsec tunnel running status, as well as locate and rectify faults when IPsec VPN functions are abnormal.

### Procedure

- (1) Choose **Monitor > Log Monitoring > IPsec VPN Log**.
- (2) The information about IPsec VPN logs is displayed on the web page.

Log Level	Time	Tunnel Name	Peer Address	Details
Medium	2023-07-21 16:43:18	32	40.0.0.40	IKE SA established.
Medium	2023-07-21 16:43:18	32	40.0.0.40	IPsec SA has been established (message ID: 2c7be916).
High	2023-07-21 13:57:15	32	40.0.0.40	Packet 113 of main mode negotiation is not received.
High	2023-07-21 13:57:15	32	40.0.0.40	Failed to send the packet from 40.0.0.50 to 40.0.0.40: Check network connectiv...
Medium	2023-07-21 13:56:51	32	40.0.0.40	DPD detection timeout.
Medium	2023-07-21 13:19:41	32	40.0.0.40	IPsec SA has been established (message ID: 734cd113).
Medium	2023-07-21 12:20:26	32	40.0.0.40	IPsec SA has been established (message ID: 3f0f9600).
Medium	2023-07-21 11:21:11	32	40.0.0.40	IPsec SA has been established (message ID: 7647f0a1).
Medium	2023-07-21 10:21:56	32	40.0.0.40	IPsec SA has been established (message ID: 5ecfbd90).
Medium	2023-07-21 09:22:41	32	40.0.0.40	IPsec SA has been established (message ID: 4afbe4d7).

Field	Description
Log Level	Importance level of the log. Levels in order of importance from low to high: prompt, low, medium, and high.
Time	Record time of the IPsec VPN log.
Tunnel Name	Name of the IPsec tunnel that generates the log.
Peer Address	Remote IP address of the IPsec tunnel.
Details	Detailed log content.

---

**Note**

Enter a keyword, including the log record date, log level, log content keyword, to search for specific logs.

---

**Follow-up Procedure**

- Click **Export** to export 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 logs.

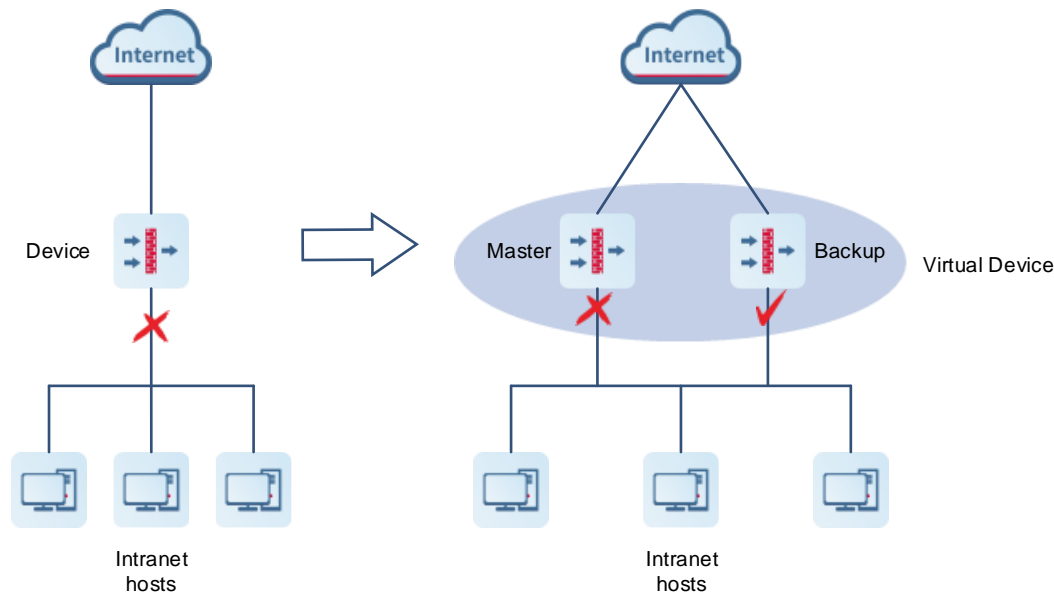
## 7.19 VRRP

### 7.19.1 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.

---

## 7.19.2 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.

### 7.19.3 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.



- (3) Configure the parameters of the VRRP group.

< Back

## Add VRRP Group

**Basic Info**

\* VRRP Group Name

① Priority

\* ① Deployment Interface

\* ① Virtual IP

① Monitoring Interface

---

**Advanced**

① Preemption Delay  Second

① Advertisement Interval  Second

**Authentication**

① Plain Text Authentication

Item	Description	Remarks
<b>Basic Info</b>		
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
<b>Advanced</b>		
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
<b>Authentication</b>		
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.

## 7.19.4 Viewing VRRP Logs

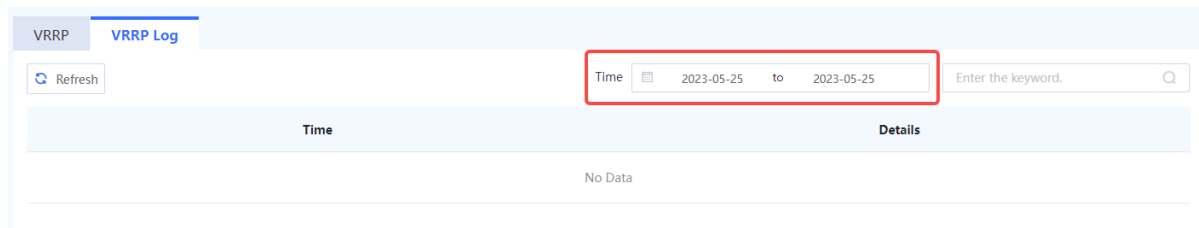
### Application Scenario

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.



## 7.20 User Authentication

### 7.20.1 Overview

For SSL VPN access or scenarios requiring web authentication, the firewall needs to authenticate remote access users to ensure connection security.

#### 1. SSL VPN Authentication

The SSL VPN 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.

- o 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.

## 2. Web Authentication

Web authentication is an identity authentication method to control users' network access permissions. When users access the Internet using a browser, the device forces the browser to access a specific site (portal authentication page). The users need to pass the portal authentication to access the Internet.

The web authentication process is as follows:

- (1) Intranet users access the Internet using a browser. (The access traffic passes through the firewall.)
- (2) The firewall intercepts all HTTP or HTTPS requests from unauthenticated users and sends a redirection URL (portal authentication page) to the browser.

The device supports both local portal authentication and custom portal authentication. If you select local portal authentication, the built-in portal authentication page of the firewall is used without using a third-party portal server. If you select custom portal authentication, a portal server is required.

No matter which authentication method you select, configure user information on the firewall or RADIUS server in advance.

- (3) After entering the username and password on the portal authentication page, a user can access the Internet upon successful authentication.

## 7.20.2 User Management

### 1. Configuring User Groups

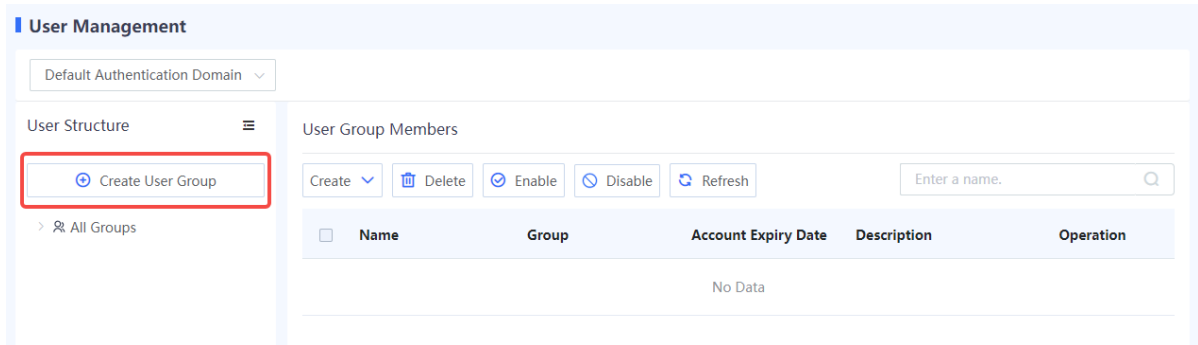
#### Application Scenario

Add users with similar attributes such as the same resource access requirements to a user group to facilitate unified management.

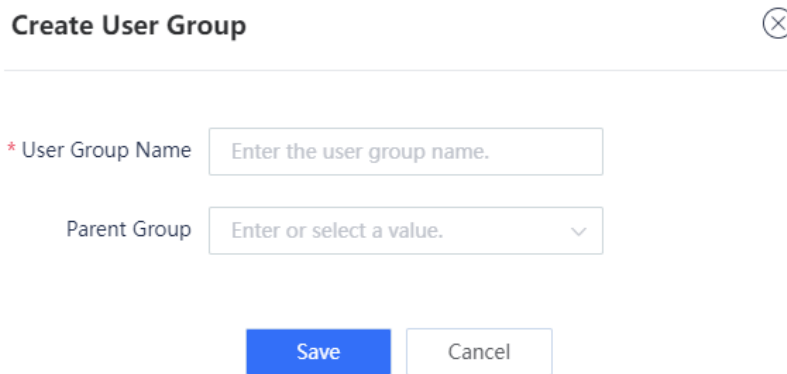


**Procedure**

- (1) Choose **Object > User Authentication > User Management**.
- (2) Click Create User Group.



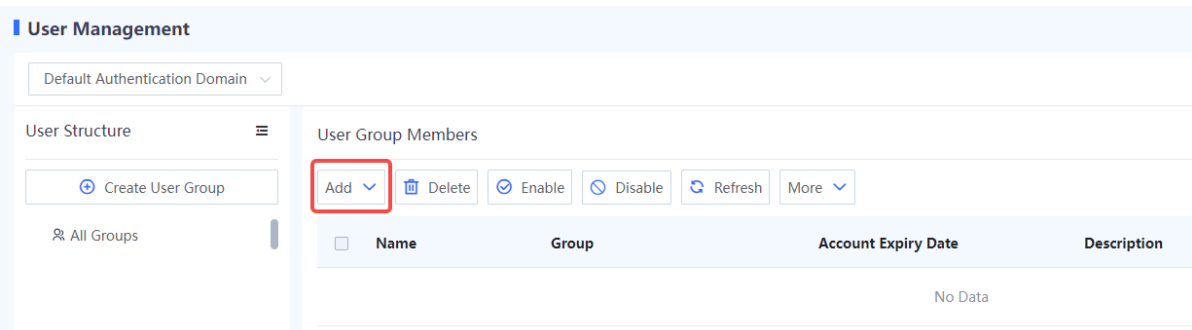
- (3) Enter the user group name and select a parent group.



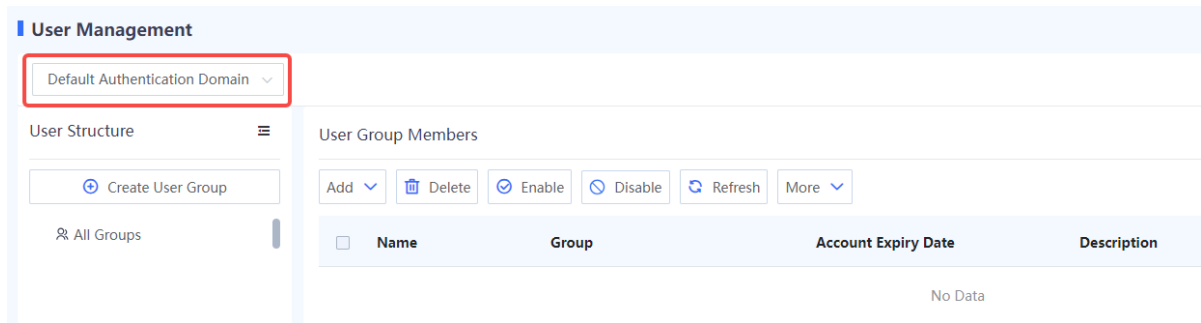
- (4) After verifying the configuration, click **Save**.

**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.



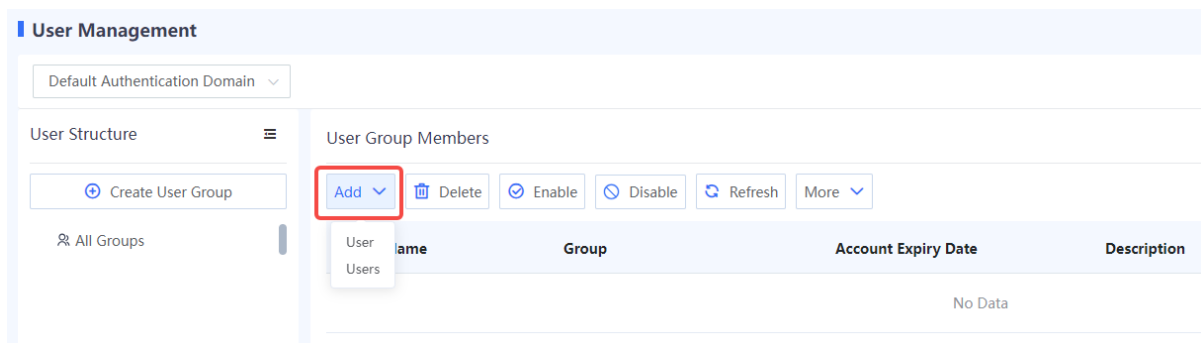
## 2. Configuring Users

### Application Scenario

For SSL VPN access or scenarios requiring web authentication, if you use the local authentication method to authenticate a remote access user, you need to configure user identity information on the **User Management** page first. Otherwise, the authentication may fail.

### Procedure

- (1) Choose **Object > User Authentication > User Management**.
- (2) 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

< Back

## Add User

**Basic Info**

\* Login Username

Enabled State  Enable  Disable

Displayed Username

\* Parent Group

Description

---

**Password**

\* 🔒 Password

\* Confirm Password

**⋮ Advanced Settings**

Bind IP/MAC  Not Bind  One-Way Binding  Two-Way Binding

Expiry Date  Permanent  With Expiry Date

Save

Item	Description	Remarks
<b>Basic Info</b>		
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 <b>Login Username</b> .	[Example] user1
Group	Group to which the user belongs.	[Example] /default
Description	User description.	N/A
<b>Password</b>		

Item	Description	Remarks
Password	Password for the remote user to log in to the virtual gateway. For details about password complexity requirements, see <a href="#">7.20.7 Authentication Settings</a> .	N/A
Confirm Password	The value must be the same as that of <b>Password</b> .	N/A
<b>Advanced Settings</b>		
Bind IP/MAC	<p>Whether to specify the IP or MAC address for user login:</p> <ul style="list-style-type: none"> <li>● <b>Not Bind:</b> Unrestricted.</li> <li>● <b>One-Way Binding:</b> A user can log in to the virtual gateway using only the specified IP or MAC address.</li> <li>● <b>Two-Way Binding:</b> A user can log in to the virtual gateway using only the specified IP and MAC addresses.</li> </ul>	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

Enabled State  Enable  Disable

\* Parent Group

Description

---

**Password**

\* ⓘ Password

\* Confirm Password

**⌵ Advanced Settings**

Bind IP/MAC  Not Bind  One-Way Binding

Expiry Date  Permanent  With Expiry Date

Save

Item	Description	Remarks
<b>Basic Info</b>		
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
<b>Password</b>		
Password	Shared password for the remote users to log in to the virtual gateway on the SSL VPN	N/A

Item	Description	Remarks
	client.	
Confirm Password	The value must be the same as that of <b>Password</b> .	N/A
<b>Advanced Settings</b>		
Bind IP/MAC	Whether to specify the IP or MAC address for user login: <ul style="list-style-type: none"> <li>● <b>Not Bind</b>: Unrestricted.</li> <li>● <b>One-Way Binding</b>: A user can log in to the virtual gateway using only the specified IP or MAC address.</li> <li>● <b>Two-Way Binding</b>: A user can log in to the virtual gateway using only the specified IP and MAC addresses.</li> </ul>	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

(3) After verifying the configuration, click **Save**.

#### Follow-up Procedure

- Click **Edit** in the **Operation** column to modify user information. If you modify the IP-MAC binding configuration (for example, change the option from **Not Bind** to **One-Way Binding**), authenticated users may be disconnected.
- To delete users in a batch, select the users and click **Delete**. After being deleted, the authenticated users are disconnected and cannot be re-authenticated.
- To disable users in a batch, select the users and click **Disable**. After being disabled, the authenticated users are disconnected and cannot be re-authenticated.
- To enable users in a batch, select the users and click **Enable**.
- Click **More** to export user information of the current zone or all zones.

### 7.20.3 User Import

#### Application Scenario

For SSL VPN access or scenarios requiring web authentication, if you use the local authentication method to authenticate a remote access user, you need to configure user

identity information on the device. Otherwise, the authentication may fail. You can use this function to batch configure user information.

### Procedure

- (1) Choose **Object > User Authentication> Import User**.
- (2) Click **Download CSV Sample File** to download the import template. Fill in user information according to template requirements and examples.
- (3) Click **click Select to select a file** to import the file of user information.
- (4) (Optional) Select **Overwrite Existing Local User Records** or **Skip Failed User Records**. If neither is selected, a message is displayed upon repeated user records or import failures.

### Import User

Import User

① The format of the configuration file to be imported must be user-config-yyyyMMddHHmmssSSS.csv.  
For example, user-config-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](#).

Overwrite Existing Local User Records     Skip Failed User Records

[Start Import](#)

- (5) Click **Start Import**.

### Follow-up Procedure

After the user information is imported, you can check it on the **User Management** page.

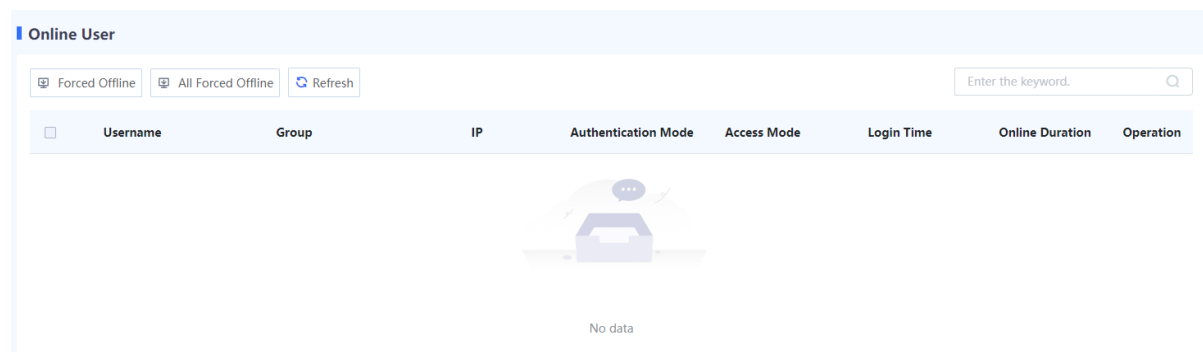
## 7.20.4 Online User

### Application Scenario

When a remote user accesses the intranet through SSL VPN or passes the web authentication, you can check online user information on the **Online User** page.

### Procedure

- (1) Choose **Object > User Authentication > Online User**.
- (2) (Optional) Select one or multiple users and click **Forced Offline** to batch disconnect users. To disconnect all users, click **All Forced Offline**.



## 7.20.5 Authentication Domain Management

### Application Scenario

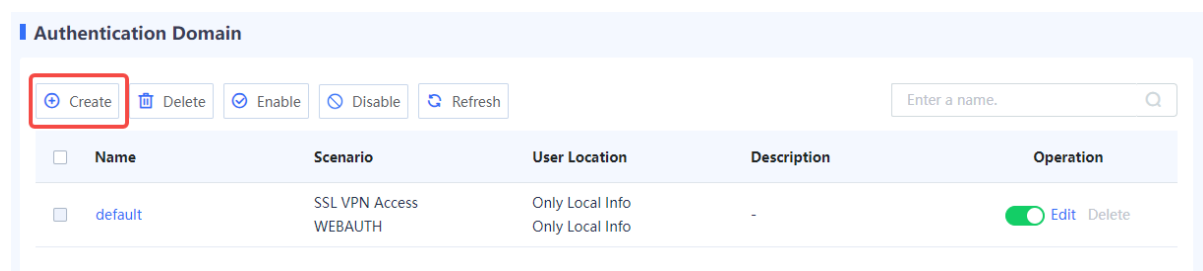
For SSL VPN access or scenarios requiring web authentication, the firewall implements the same policies, including login authentication and resource authorization, for users in the same authentication domain, facilitating unified management.

### Prerequisites

You have configured user information on the firewall or authentication server. For details, see [7.20.2 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**.





(3) Configure authentication domain information.

← Back

## Create Authentication Domain

**Basic Info**

\* Name

Enabled State  Enable  Disable

Description

---

**User Management**

\* Scenario  SSL VPN Access ⓘ |  WEBAUTH ⓘ

User Location

Authentication Server  [⊕ Add RADIUS Server](#)

---

**Advanced Settings**

ⓘ Domain Name Removal

ⓘ Default Online User   
Group

Item	Description	Remarks
<b>Basic Info</b>		
Name	Authentication domain name.	[Example] auth_domain_1
Enabled State	Whether to enable the authentication domain.	[Example] Enable
Description	Authentication domain description.	N/A
<b>User Management</b>		
Scenario	Application scenario of an authentication domain. After you select a scenario, the authentication domain is displayed only on the configuration page of the specified scenario.	[Example] SSL VPN

Item	Description	Remarks
User Location	<p>Set the user authentication mode. The options are as follows:</p> <ul style="list-style-type: none"> <li>● <b>Prefer Info on Server:</b> 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.</li> <li>● <b>Prefer Local Info:</b> 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.</li> <li>● <b>Only Info on Server:</b> User identity information, including the username and password, is stored on the authentication server for authentication.</li> <li>● <b>Only Local Info:</b> User identity information, including the username and password, is stored on the local firewall for authentication.</li> </ul>	N/A
Authentication Server	Authentication server.	N/A
<b>Advanced Settings</b> (Valid Only for Scenarios with Server Authentication)		
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
Default Online User Group	Configure the default user group for users that go online through server authentication.	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**.

## 7.20.6 Authentication Policies

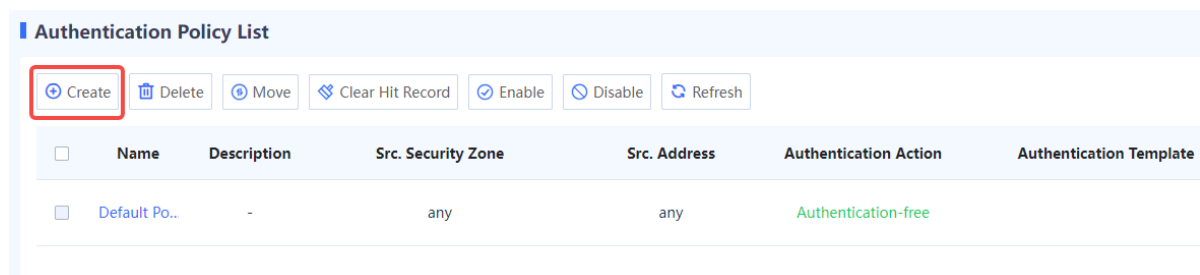
### Application Scenario

For scenarios where web authentication is required, you can configure authentication policies to execute specified authentication actions on user traffic from a specific source security zone or source IP address. On the device, a default policy is predefined to execute the authentication-free action for all users. That is, users can go online without being authenticated.

When you configure multiple authentication policies, the list of the policies is arranged in the order of configuration by default. The policies that are configured earlier have higher priorities. You can adjust the priority of a policy by moving its position.

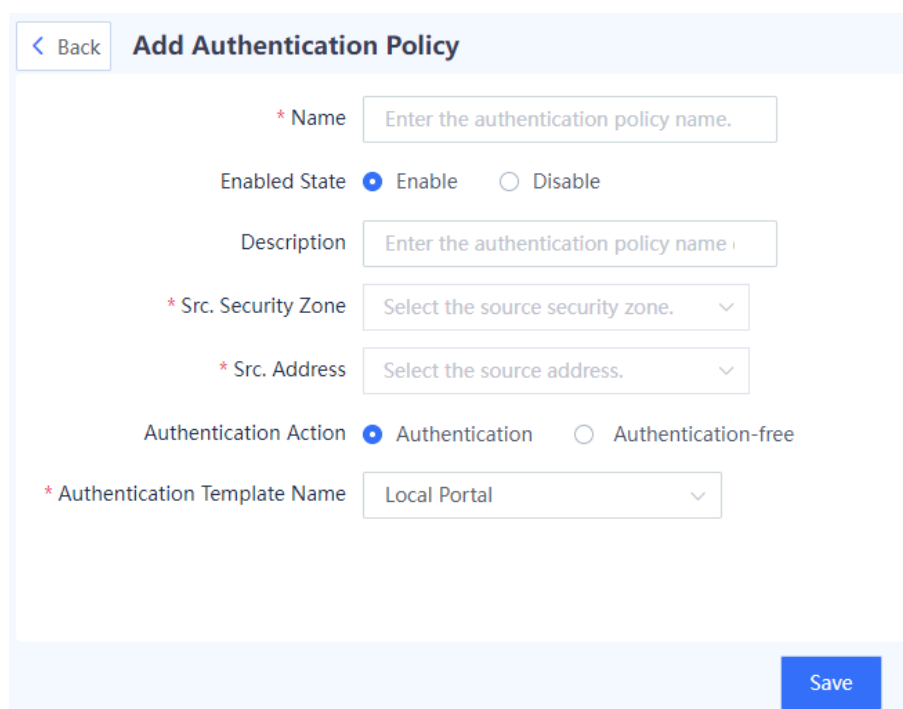
### Procedure

- (1) Choose **Object > User Authentication > Authentication Policy List**.
- (2) Click **Create**.



<input type="checkbox"/>	Name	Description	Src. Security Zone	Src. Address	Authentication Action	Authentication Template
<input type="checkbox"/>	Default Po..	-	any	any	Authentication-free	

- (3) Configure an authentication policy.



[Back](#) **Add Authentication Policy**

\* Name

Enabled State  Enable  Disable

Description

\* Src. Security Zone

\* Src. Address

Authentication Action  Authentication  Authentication-free

\* Authentication Template Name

**Save**

Item	Description	Remarks
Name	Name of the authentication policy.	[Example] policy_1
Enabled State	Whether to enable the authentication policy.	[Example] Enable
Description	Description of the authentication policy.	-
Src. Security Zone	User traffic from the specified source security zone matches this authentication policy and needs to be authenticated. User traffic from non-specified zones is permitted without being authenticated.	-
Src. Address	User traffic from the specified source IP address matches this authentication policy and needs to be authenticated. User traffic from non-specified IP addresses is permitted without being authenticated.	-
Authentication Action	Action taken on the traffic that matches the authentication policy. If <b>Authentication</b> is selected, authentication template needs to be specified.	[Example] Authentication
Authentication Template Name	Select the portal authentication template. For details, see <a href="#">7.20.7 Authentication Settings</a> .	

(4) After verifying the configuration, click **Save**.

#### Follow-up Procedure

- Click **Create** to add more authentication policies.
- Select an authentication policy, and click **Delete** or **Disable** to delete or disable the policy. This allows users of the source security zone or source IP address specified in the policy to access the extranet without being authenticated.
- Select an authentication policy, and click **Move** to adjust the policy position. The closer a policy is to the front, the higher its priority in matching.

## 7.20.7 Authentication Settings

### 1. Local Portal

#### Application Scenario

In a web authentication scenario where local portal authentication is selected, the firewall redirects the access page to the built-in portal authentication page when an unauthenticated user accesses the extranet. The user can access extranet resources only after being authenticated.

#### Precautions

Select either local portal authentication or custom portal authentication. If local portal authentication is enabled, custom portal authentication will be automatically disabled, and vice versa.

#### Procedure

- (1) Choose **Object > User Authentication > Authentication Settings > Local Portal**.
- (2) Toggle on  to enable local portal authentication. Configure the authentication port and redirection page upon authentication as required.

The screenshot shows the configuration page for Local Portal Authentication. The page has a top navigation bar with tabs: Local Portal (selected), Custom Portal, Real-Name User Info Reception, Allowlist, and Other Authentication Settings. Below the tabs, there is a toggle switch for 'Local Portal Authentication' which is currently turned off. Underneath, there is a text input field for 'Authentication Port' with the value '8081'. Below that, there are three radio button options for 'Redirection upon Authentication': 'No Redirection' (selected), 'Redirect to Previous Web Page', and 'Redirect to Custom URL'. At the bottom right of the configuration area, there is a blue 'Apply' button.

---

#### Note

You are advised to use the default settings if no special requirements exist.

---

- (3) After verifying the configuration, click **Apply**.

### 2. Custom Portal

#### Application Scenario

In a web authentication scenario where custom portal authentication is selected, the firewall redirects the access page to the portal authentication page on the portal server when an

unauthenticated user accesses the extranet. The user can access extranet resources only after being authenticated.

**Precautions**

Select either local portal authentication or custom portal authentication. If local portal authentication is enabled, custom portal authentication will be automatically disabled, and vice versa.

**Procedure**

- (1) Choose **Object > User Authentication > Authentication Settings > Custom Portal**.
- (2) Toggle on  to enable custom portal authentication. Configure the authentication template as required.

Item	Description	Remarks
Portal Authentication Template 1 Name	Name of the portal authentication template.	[Example] template_1
Portal Server URL	URL of the portal authentication page on the server. Ensure that the firewall can communicate with the server. Otherwise, the authentication page cannot be	[Example] http://www.123.com/

Item	Description	Remarks
	displayed.	
NAS Configuration	Select <b>IP</b> or <b>Interface</b> for the firewall to communicate with the server. If the firewall has multiple outbound interfaces, <b>IP</b> or <b>Interface</b> must be selected, and an interface or interface IP address must be set for NAS.	[Example] Default
Custom URL Parameters	Customize the redirect URL (of the portal authentication page) format. Choose whether to carry specific fields in the redirect URL and whether to display them in ciphertext. Ensure that custom parameter settings are the same as those on the server. Otherwise, the authentication page cannot be displayed.	-

(3) Configure the following parameters for the portal server.

**Portal 3.0**

**Basic Info**

\* Portal Server IP  Port

\* Shared Key

Sending Source  Default  Interface

MAB

[Advanced Settings](#)

App

Item	Description	Remarks
<b>Basic Info</b>		
Portal	IPv4 address of the portal server.	[Example]

Item	Description	Remarks
Server IP		1.1.1.1
Port	Port number that the server uses to exchange portal packets with the device, which must be the actual port number used by the server.	[Example] 50100
Shared Key	Communication key used between the device and authentication server, which must be the same as that configured on the server.  During authentication, the communication key is used to encrypt some data exchanged between the device and authentication server to improve security.	[Example] Default
Sending Source	In a NAT scenario where the NAS-IP field in the URL parameter customization is enabled, you must configure the outbound interface that sends packets to the server as the sending source.	-
MAB	If this function is enabled, a user only needs to enter the username and password once, and can subsequently go online without authentication.	[Example] Enabled
<b>Advanced Settings</b>		
Server Detection	This function is used to periodically detect the availability of the portal server. It must be enabled when the user escape function is enabled.	[Example] Enabled
Server Detection Protocol Type	Protocol used by the device for detecting server availability.	[Example] ICMP
Detection Interval	Interval for the device to send detection packets, in seconds.	[Example] 30
Detection Retries	Number of resending detection packets when the device does not receive a reply packet from the server. If the consecutive retransmission times reach the configured detection retry times, the server is deemed as unavailable.	



Item	Description	Remarks
Escape	<p>If this function is enabled, new users can access network resources without authentication when no server is available. If some mission-critical services on the network cannot be interrupted, you can enable this function. It ensures service continuity when the portal server is faulty.</p> <p>When the server recovers, users that were allowed to access are forced to go offline, and users need to be re-authenticated to go online.</p>	[Example] Enabled
<b>Listening Port</b>		
Listening Port	Port number that the device uses to exchange portal packets with the server, which must be the same as that configured on the server.	[Example] 2000

(4) After verifying the configuration, click **Apply**.

**Follow-up Procedure**

Click **Create** or **Delete** in the upper right corner to create more portal authentication templates or delete a specific template.



**3. Real-Name User Info Reception**

**Application Scenario**

When two devices on the network function as authentication devices simultaneously, you can use the real-name user information reception function to synchronize user information between the two devices.

**Prerequisites**

The two devices can communicate with each other.

**Procedure**

- (1) Choose **Object > User Authentication > Authentication Settings > Real-Name User Info Reception**.
- (2) Toggle on  to enable the LINK-SAM association function and configure the TCP port.

**Note**

The TCP port must be the same as that configured for the peer end. Otherwise, synchronization fails.

(3) After verifying the configuration, click **Apply**.

## 4. Allowlist

### Application Scenario

After an allowlist is configured, users can access some network resources before being authenticated. The following allowlist types are supported:

- **Src. IP:** After a source IP address allowlist is configured, users at IP addresses in the allowlist can go online without being authenticated.
- **Dest. IP:** After a destination IP address allowlist is configured, all users can access the IP resources at the IP addresses in the allowlist without being authenticated.
- **Src. MAC:** After a source MAC address allowlist is configured, users at MAC addresses in the allowlist can go online without being authenticated.
- **URL:** After a URL allowlist is configured, all users can access URLs in the allowlist without being authenticated.

### Procedure

(1) Choose **Object > User Authentication > Authentication Settings > Allowlist**.

(2) Click **Create**.

(3) Select an allowlist type and configure an IP address or IP range.



(4) After verifying the configuration, click **Save**.

#### Follow-up Procedure

- Click **Create** to add more allowlists.
- Click **Delete** to delete a specified allowlist. After it is deleted, users that correspond to the addresses in the allowlist need to be re-authenticated before accessing the extranet.

## 5. Other Authentication Settings

### Application Scenario

You can configure the following functions on the **Other Authentication Settings** tab page.

- **Password Settings:** Set password complexity requirements for user login to reduce the risk caused by weak passwords. After a password strength level is set, the passwords of newly added users must meet the complexity requirements of the strength level.
- **Auto Logout Settings:** Choose whether to enable the **Force No-Traffic Users Offline** function. When this function is enabled, users with no traffic interaction within the specified period are forced to go offline.

### Procedure

- (1) Choose **Object > User Authentication > Authentication Settings > Other Authentication Settings**.
- (2) Select a password strength level and enable the **Force No-Traffic Users Offline** function as required.

### **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 [7.20.2 2. Configuring Users](#).

(3) After verifying the configuration, click **Apply**.

## 7.20.8 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**.

(3) Configure the server.

< Back
**Add RADIUS Server**

**Basic Info**

\* Server Name

\* Shared Password

\* Active Authentication Server IP 
Ⓞ Authentication Port 
Ⓞ Accounting Port 
Tx Interface

Standby Authentication Server IP 
Ⓞ Authentication Port 
Ⓞ Accounting Port 
Tx Interface

**Advanced Settings**

Retransmission Times

Unit

Response Timeout

Ⓞ Enable Active Detection

\* Detection Username

Save

Item	Description	Remarks
<b>Basic Info</b>		
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	<p>Authentication server that performs authentication.</p> <ul style="list-style-type: none"> <li>● <b>IP:</b> IP address of the authentication server.</li> <li>● <b>Authentication Port:</b> Port on the authentication server that provides the authentication service.</li> <li>● <b>Accounting Port:</b> Port on the authentication server that provides the accounting service.</li> <li>● <b>Tx Interface:</b> Interface on the firewall for sending authentication packets.</li> </ul>	N/A
Standby Authentication Server	<p>When the active authentication server fails or has no user information, the standby authentication server performs authentication.</p> <ul style="list-style-type: none"> <li>● <b>IP:</b> IP address of the authentication server.</li> <li>● <b>Authentication Port:</b> Port on the</li> </ul>	N/A

Item	Description	Remarks
	authentication server that provides the authentication service. <ul style="list-style-type: none"> <li>● <b>Accounting Port:</b> Port on the authentication server that provides the accounting service.</li> <li>● <b>Tx Interface:</b> Interface on the firewall for sending authentication packets.</li> </ul>	
<b>Advanced Settings</b>		
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

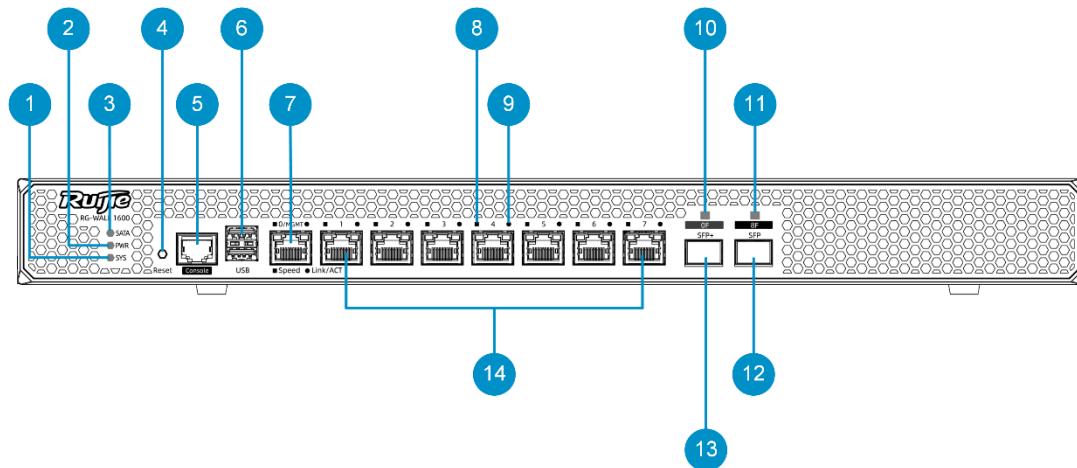


Table 8-1 Components on the Front Panel

No.	Component	Description
1	SYS indicator	<ul style="list-style-type: none"> <li>● Blinking green: The device is powered on and being initialized.</li> <li>● Steady green: Initialization is complete.</li> <li>● Steady red: An alarm is generated.</li> </ul>
2	PWR indicator	<ul style="list-style-type: none"> <li>● Steady green: The power supply is normal.</li> <li>● Off: The power supply is cut off or fails.</li> </ul>
3	SATA hard disk indicator	<ul style="list-style-type: none"> <li>● Steady green: A hard disk is connected.</li> <li>● Blinking green: Data is being read or written.</li> </ul>
4	Reset button	<ul style="list-style-type: none"> <li>● Restarting the device: Press the button for less than 3 seconds.</li> <li>● Restoring factory settings: Press the button for more</li> </ul>



No.	Component	Description
		<p>than 3 seconds.</p> <p>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 <b>System &gt; One-Click Collection</b>, and download the information.</p>
5	Console port	<p>It is used to connect to the console for device maintenance and diagnosis.</p> <p>Note: The console port is used only in special scenarios. For details, contact technical support personnel.</p>
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	<ul style="list-style-type: none"> <li>● Steady orange: Gbit/s port speed</li> <li>● Off: 100/10 Mbit/s port speed</li> </ul>
9	Link/ACT status indicators (round) of electrical ports 0 to 7	<ul style="list-style-type: none"> <li>● Steady green: The port is connected.</li> <li>● Blinking green: The port is receiving or sending data.</li> <li>● Off: The port is incorrectly connected.</li> </ul>
10	Optical port 0F indicator	<ul style="list-style-type: none"> <li>● Steady green: The port is connected.</li> <li>● Blinking green: The port is receiving or sending data.</li> <li>● Off: The optical port is incorrectly connected.</li> </ul>
11	Optical port 8F indicator	<ul style="list-style-type: none"> <li>● Steady green: The port is connected.</li> <li>● Blinking green: The port is receiving or sending data.</li> <li>● Off: The optical port is incorrectly connected.</li> </ul>
12	Optical port 8F	Gigabit optical port. For details about optical modules that support this port, see <a href="#">Table 1-3</a> .

No.	Component	Description
13	Optical port 0F	10 Gigabit optical port. For details about optical modules that support this port, see <a href="#">Table 1-3</a> .
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**.



- (3) The page displays the CPU usage, memory usage, and hard disk usage in different areas.



**Follow-up Procedure**

Item	Description
CPU	<p>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.</p> <p>The possible causes for high CPU usage are as follows:</p> <ul style="list-style-type: none"> <li>● App protection or DDoS protection is enabled.</li> <li>● Too many connections are created, many of which are initiated by attackers.</li> </ul>
Memory	<p>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.</p>

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.

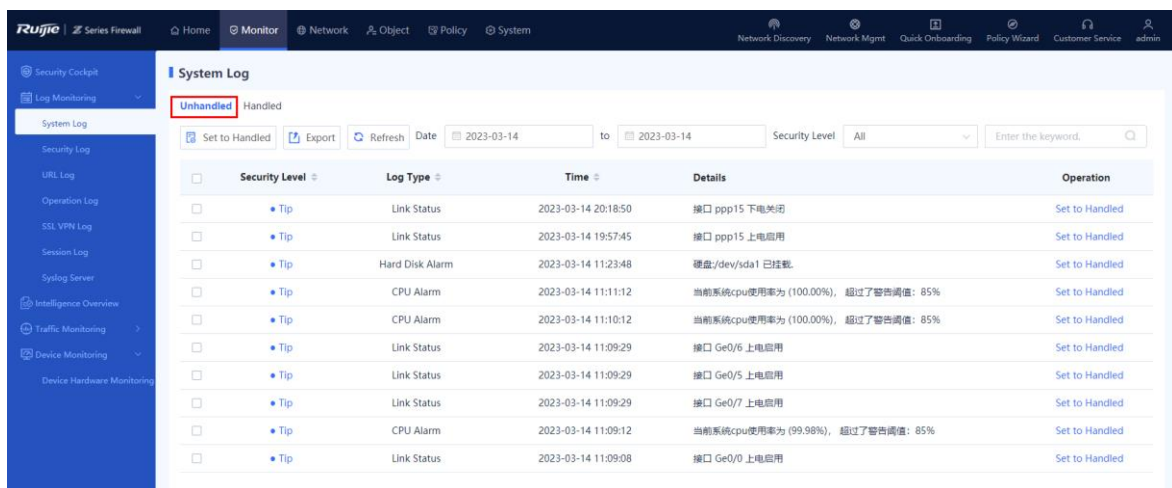
### 8.3.1 Querying System Logs

#### 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**.



- (2) The system log-related information is displayed on the web page.

Field	Description
Security Level	Security level of a system log.

Field	Description
Log Type	Type of a system log.
Time	Time when a system log is generated.
Details	Detailed information of a system log.
Operation	Click <b>Set to Handled</b> to mark a log as <b>Handled</b> and switch to the <b>Handled</b> 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.

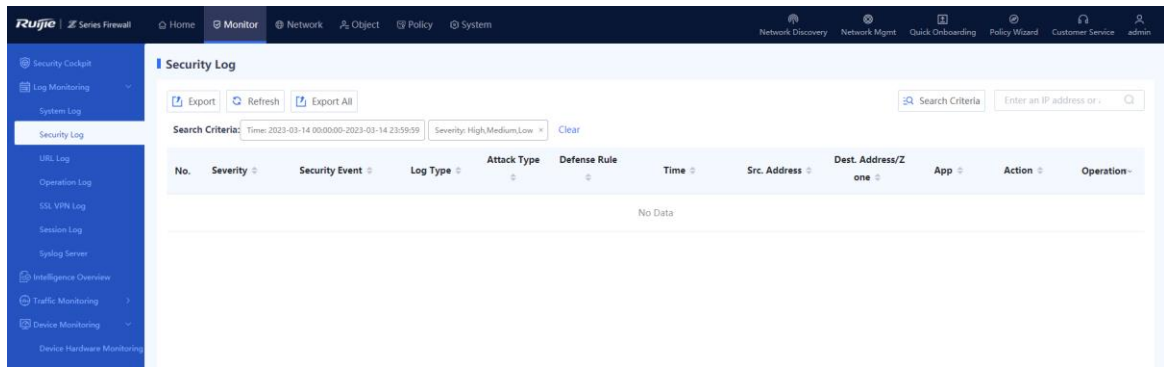
## 8.3.2 Querying Security Logs

#### 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.



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.
Dest. Security Zone	Destination security zone in a security policy.
Dest. Address/Zone	Destination address in a security policy.

Field	Description
Action	Operation result of a security policy on the traffic.
Operation	Click <b>View Details</b> 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.

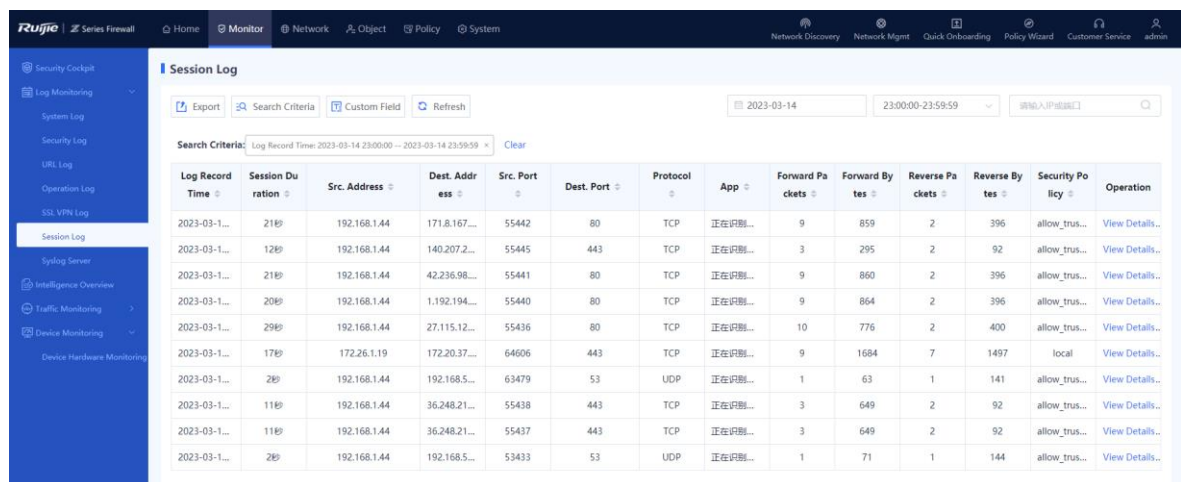
### 8.3.3 Querying Session Logs

**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.



### **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.

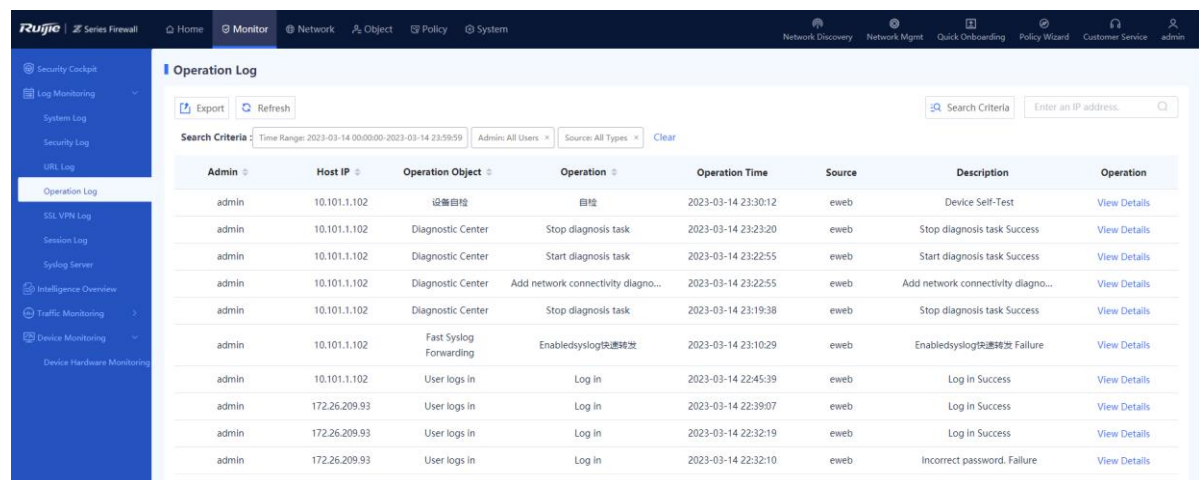
## 8.3.4 Querying Operation Logs

### 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**.



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	<a href="#">View Details</a>
admin	10.101.1.102	Diagnostic Center	Stop diagnosis task	2023-03-14 23:23:20	eweb	Stop diagnosis task Success	<a href="#">View Details</a>
admin	10.101.1.102	Diagnostic Center	Start diagnosis task	2023-03-14 23:22:55	eweb	Start diagnosis task Success	<a href="#">View Details</a>
admin	10.101.1.102	Diagnostic Center	Add network connectivity diagno...	2023-03-14 23:22:55	eweb	Add network connectivity diagno...	<a href="#">View Details</a>
admin	10.101.1.102	Diagnostic Center	Stop diagnosis task	2023-03-14 23:19:38	eweb	Stop diagnosis task Success	<a href="#">View Details</a>
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	<a href="#">View Details</a>
admin	10.101.1.102	User logs in	Log in	2023-03-14 22:45:39	eweb	Log In Success	<a href="#">View Details</a>
admin	172.26.209.93	User logs in	Log in	2023-03-14 22:39:07	eweb	Log In Success	<a href="#">View Details</a>
admin	172.26.209.93	User logs in	Log in	2023-03-14 22:32:19	eweb	Log In Success	<a href="#">View Details</a>
admin	172.26.209.93	User logs in	Log in	2023-03-14 22:32:10	eweb	Incorrect password. Failure	<a href="#">View Details</a>

(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 <b>View Details</b> 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.

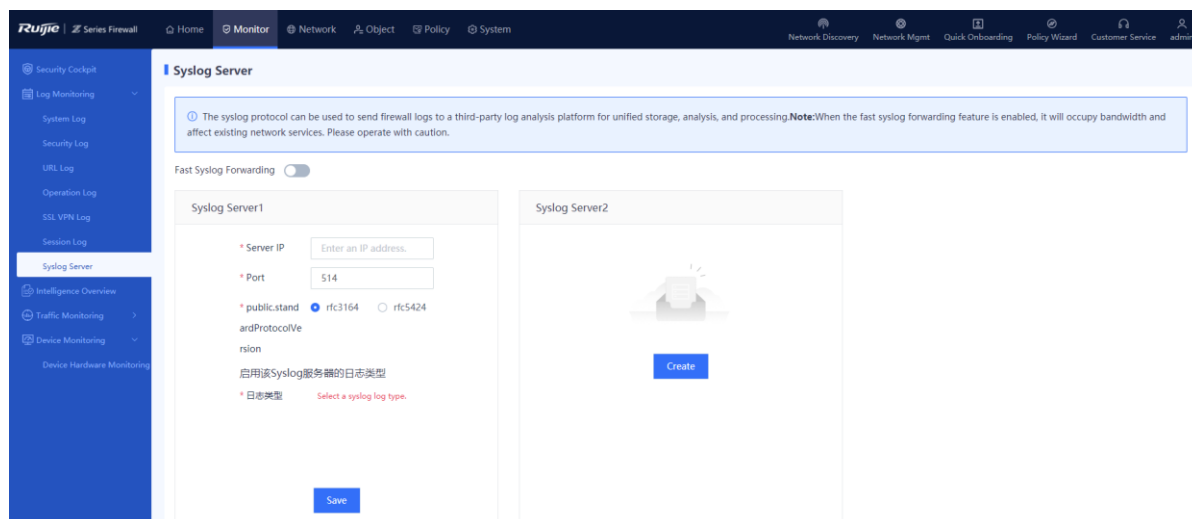
### 8.3.5 Configuring the Syslog Server

#### 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.



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 notification, including system log and security log.	Select the log type for which a Syslog notification needs to be sent.

(3) Click **Save**.

## 8.4 Traffic Monitoring

### 8.4.1 Querying Interface Traffic Monitoring

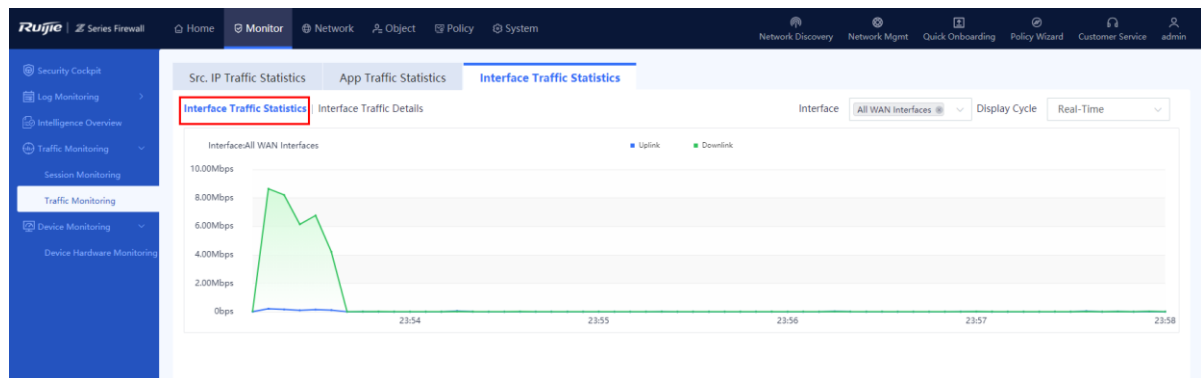
#### Application Scenario

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.



- (3) Click **Interface Traffic Details** to view the detailed traffic information of the interface.

Interface	Interface Status	Zone	IP	Uplink	Downlink
<input type="checkbox"/> Ge0/0	<span style="color: green;">■</span>	trust	192.168.1.200/24	748bps	1.11Kbps
<input type="checkbox"/> Ge0/1	<span style="color: green;">■</span>	untrust		0bps	0bps
<input type="checkbox"/> Ge0/2	<span style="color: grey;">■</span>	trust		0bps	0bps
<input type="checkbox"/> Ge0/3	<span style="color: grey;">■</span>	untrust		0bps	0bps
<input type="checkbox"/> Ge0/4	<span style="color: grey;">■</span>	trust1		0bps	0bps
<input type="checkbox"/> Ge0/5	<span style="color: green;">■</span>	untrust1		553bps	614bps
<input type="checkbox"/> Ge0/6	<span style="color: green;">■</span>	trust	192.168.1.1/24	0bps	512bps
<input type="checkbox"/> Ge0/7	<span style="color: green;">■</span>	untrust	172.20.37.124/24	2.12Kbps	177.31Mbps
<input type="checkbox"/> Ge0/8	<span style="color: grey;">■</span>			0bps	0bps
<input type="checkbox"/> TenGe0/0	<span style="color: grey;">■</span>			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

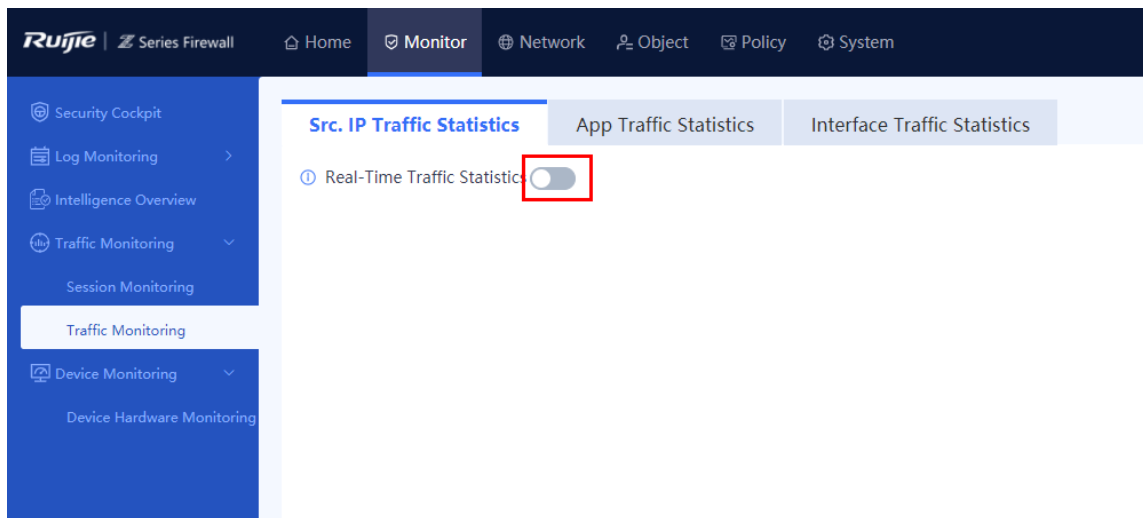
### Application Scenario

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.

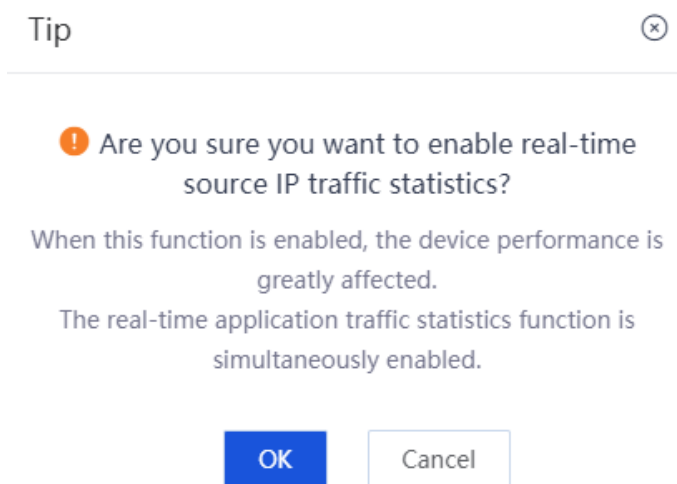
### Procedure

- (1) Choose **Monitor > Traffic Monitoring > Src. IP Traffic Statistics**.

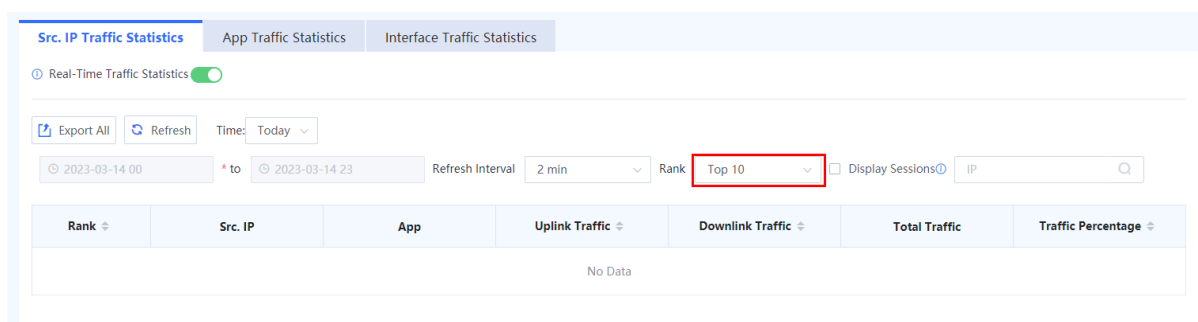
(2) Enable **Real-Time Traffic Statistics**.



(3) In the dialog box that is displayed, click **OK**.



(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.



(5) (Optional) Click **Export All** to export the real-time traffic statistics to the local device.

The screenshot shows the 'Src. IP Traffic Statistics' page. At the top, there are tabs for 'Src. IP Traffic Statistics', 'App Traffic Statistics', and 'Interface Traffic Statistics'. Below the tabs, there is a toggle for 'Real-Time Traffic Statistics' which is turned on. A control bar includes an 'Export All' button (highlighted with a red box), a 'Refresh' button, a 'Time' dropdown set to 'Today', and a date range selector from '2023-03-14 00' to '2023-03-14 23'. Other controls include 'Refresh Interval' (2 min), 'Rank' (Top 10), 'Display Sessions' (checkbox), and an 'IP' search field. Below the control bar is a table with the following columns: Rank, Src. IP, App, Uplink Traffic, Downlink Traffic, Total Traffic, and Traffic Percentage. The table content is '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.

The screenshot shows the 'App Traffic Statistics' page. At the top, there are tabs for 'Src. IP Traffic Statistics', 'App Traffic Statistics', and 'Interface Traffic Statistics'. Below the tabs, there is a toggle for 'Real-Time Traffic Statistics' which is turned on. A control bar includes an 'Export All' button (highlighted with a red box), a 'Refresh' button, a 'Time' dropdown set to 'Today', and a date range selector from '2023-03-15 00' to '2023-03-15 23'. Other controls include 'Refresh Interval' (2 min), 'Rank' (Top 10), 'Display Sessions' (checkbox), and a 'Query App' search field. Below the control bar is a table with the following columns: Rank, App, Src. IP, Uplink Traffic, Downlink Traffic, Total Traffic, and Traffic Percentage. The table displays the following data:

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.

This screenshot is identical to the one above, showing the 'App Traffic Statistics' page with the 'Export All' button highlighted. It displays the same table of traffic statistics for the top 4 apps.

## 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.

	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Security Policy	Operation
<input type="checkbox"/>	2023-03-15 00:05:55	1Second	10.101.1.102	172.20.37.124	7771	443	TCP	HTTPProtocol	local	Block View Details
<input type="checkbox"/>	2023-03-15 00:05:55	29Minute59Second	10.101.1.102	172.20.37.124	7772	443	TCP	HTTPProtocol	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

Disable

(3) (Optional) Click **Search Criteria** to set the criteria for filtering sessions.

The screenshot shows the 'Real-Time Session Info' tab. At the top, there are buttons for 'Block', 'Search Criteria', 'Custom Field', and 'Refresh'. The 'Search Criteria' button is highlighted with a red box. Below the buttons, the search criteria is set to 'Session Creation Time: 60Minute'. A table below displays a list of sessions with columns for Session Creation Time, Time Before Session Timeout, Src. Address, Dest. Address, Src. Port, Dest. Port, Protocol, App, Security Policy, and Operation.

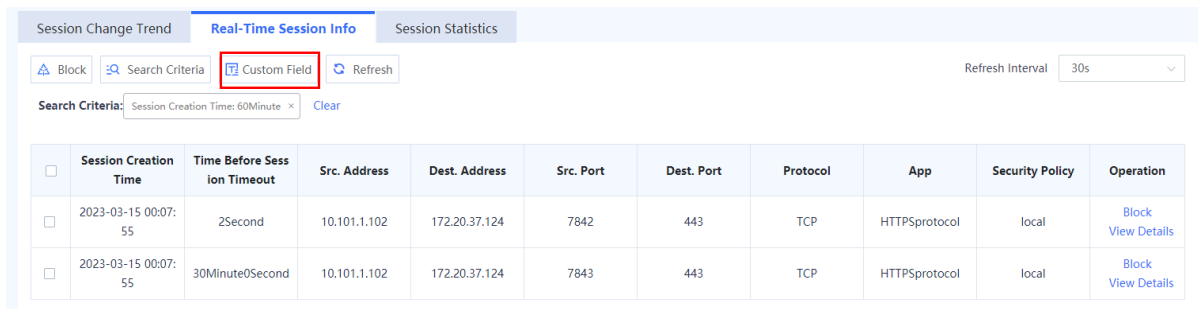
Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Security Policy	Operation
2023-03-15 00:07:20	9Second	192.168.1.44	112.64.200.152	55896	80	TCP	HTTP-BROWSE	allow_trust_to_untrust	Block View Details
2023-03-15 00:07:21	6Second	192.168.1.44	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.

The screenshot shows the 'Real-Time Session Info' tab. The 'Block' button is highlighted with a red box. The search criteria remains 'Session Creation Time: 60Minute'. The table below shows a filtered list of sessions.

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.



The screenshot shows the 'Real-Time Session Info' tab in a web interface. At the top, there are tabs for 'Session Change Trend', 'Real-Time Session Info', and 'Session Statistics'. Below the tabs are buttons for 'Block', 'Search Criteria', 'Custom Field' (highlighted with a red box), and 'Refresh'. A 'Refresh Interval' dropdown is set to '30s'. Below these buttons is a search criteria input field containing 'Session Creation Time: 60Minute' and a 'Clear' button. The main area contains a table with the following columns: Session Creation Time, Time Before Session Timeout, Src. Address, Dest. Address, Src. Port, Dest. Port, Protocol, App, Security Policy, and Operation. Two rows of session data are visible.

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

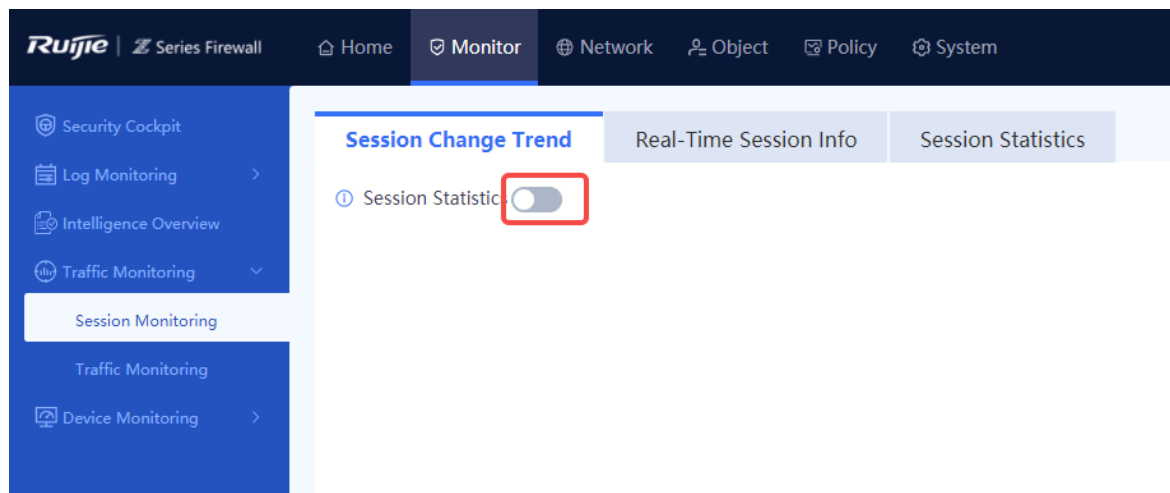
## 8.5.3 Session Statistics Collection

### 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.

**OK** Cancel

- (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.

The screenshot shows the 'Session Statistics' tab in a web interface. At the top, there are three tabs: 'Session Change Trend', 'Real-Time Session Info', and 'Session Statistics'. Below the tabs, there is a 'Refresh' button and a 'Refresh Interval' dropdown set to '30s'. To the right, there is a 'Rank' dropdown menu, which is highlighted with a red box and set to 'Top 10'. Below these controls is a table with the following data:

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

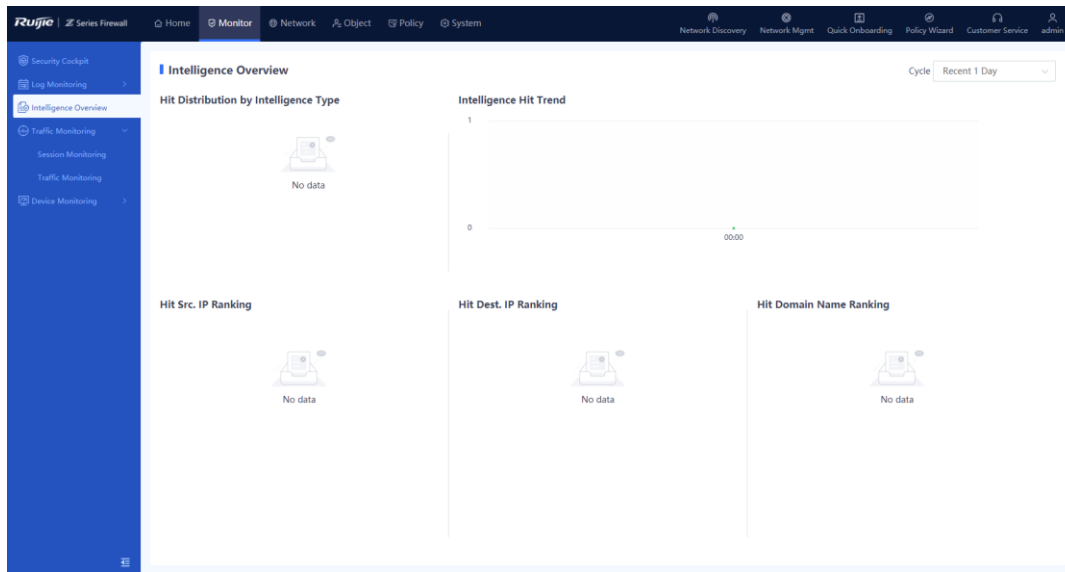
## 8.6 Intelligence Overview

### Application Scenario

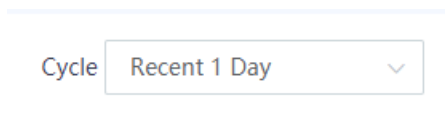
The intelligence overview function is used to display the hit distribution by intelligence type and the intelligence hit trend. This information can help administrators effectively master threats in the current network environment and then develop more refined protection policies to protect LAN hosts.

### Procedure

- (1) Choose **Monitor > Intelligence Overview**.



(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.



(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 by Intelligence Type	Displays hit distribution by intelligence type in a pie chart. This information 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	Displays the ranking of source IP addresses with threat intelligence by the number of hits. This information helps administrators analyze the threat

Ranking	<p>source and then develop corresponding protection measures to block the traffic from these source IP addresses.</p> <p>Click an IP address to switch to the security log page. Security logs of this source IP address are automatically filtered out.</p>
Hit Dest. IP Ranking	<p>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.</p> <p>Click an IP address to switch to the security log page. Security logs of this destination IP address are automatically filtered out.</p>
Hit Domain Name Ranking	<p>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.</p> <p>Click a domain name to switch to the security log page. Security logs of this domain name are automatically filtered out.</p>

# 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.

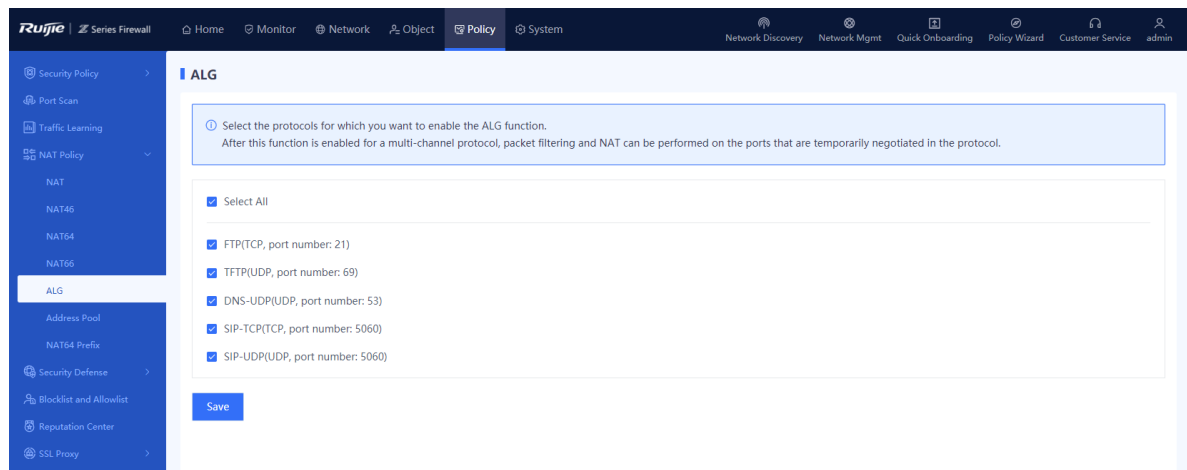
### 9.1.2 Configuring ALG

#### 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**.



(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.

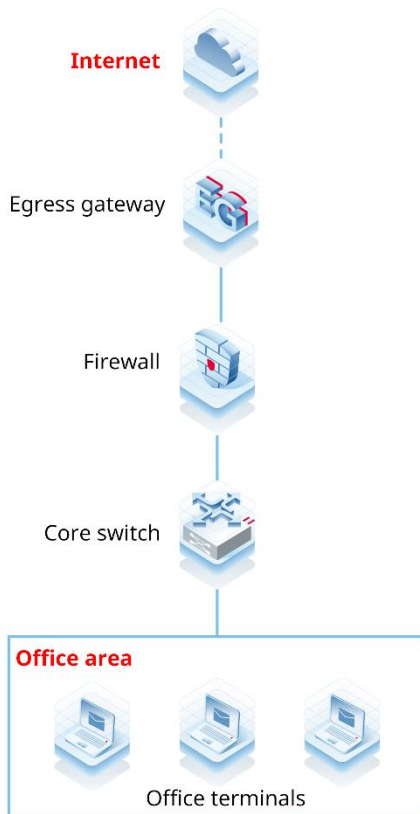
## 10.2 Firewall Deployment

### 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:

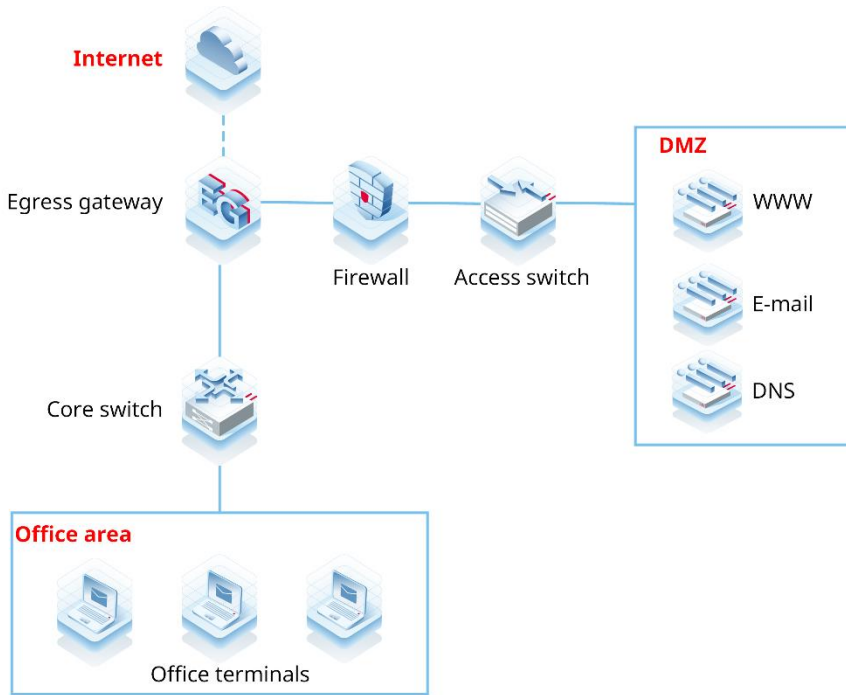
- Transparent mode - office network egress link - single-in single-out

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.



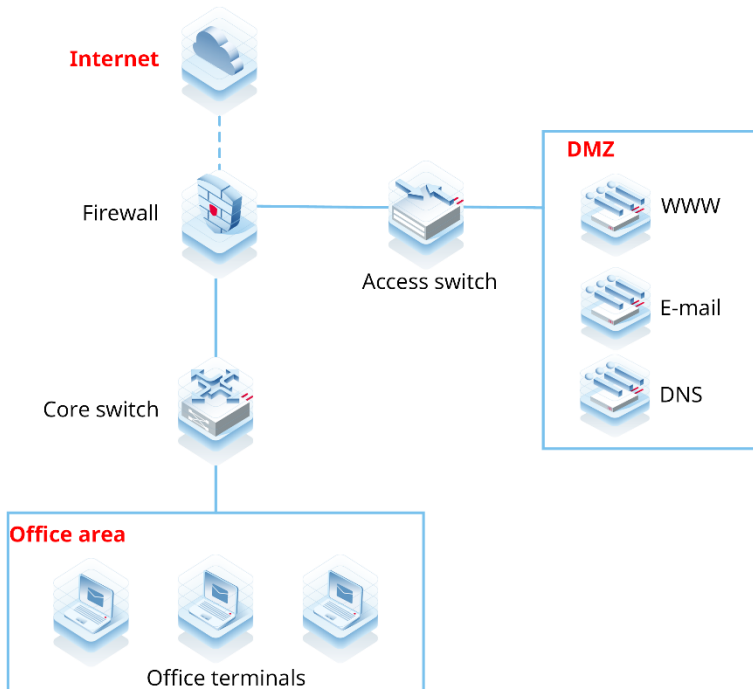
- Transparent mode – area boundary - single-in single-out

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

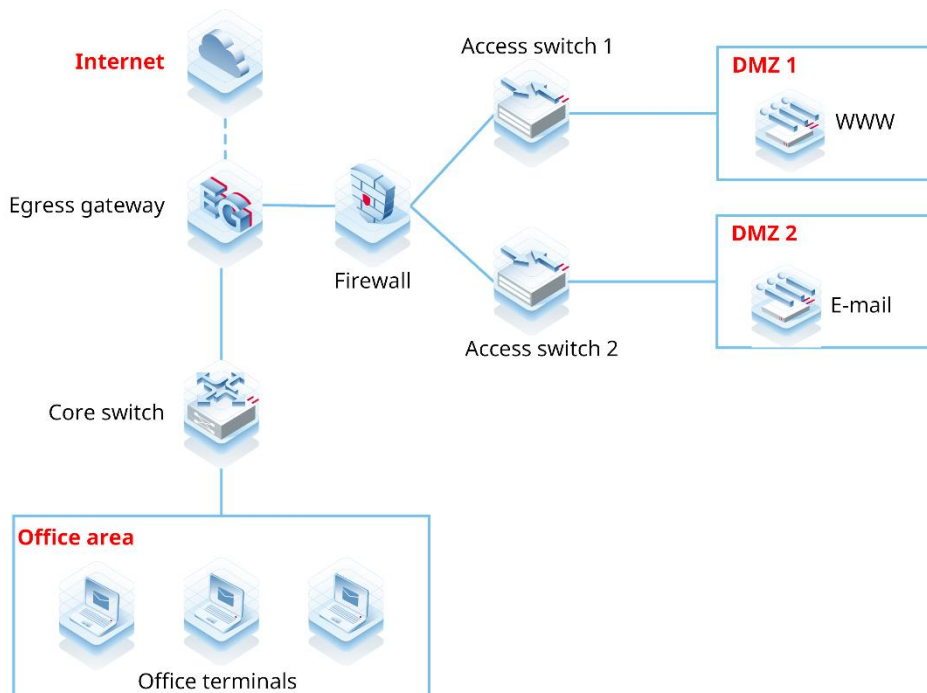
Scenario overview: The firewall is deployed at the Internet egress in gateway mode and is connected to a single ISP. The WAN GE port is configured with DHCP or a fixed IP address. The firewall connects to the LAN office area and the DMZ server area through GE electrical ports. NAT and DHCP are enabled 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.

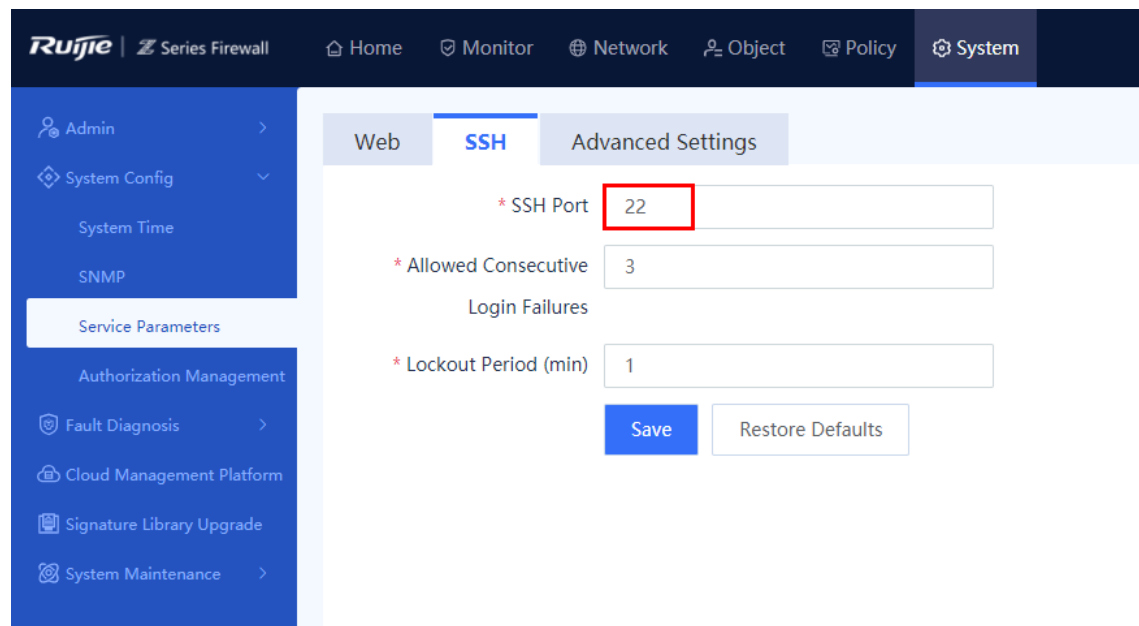
### 10.4.2 What Can I Do If I Fail to Log In to the System Through SSH?

#### Possible Causes

The SSH port number is incorrect.

#### Solution

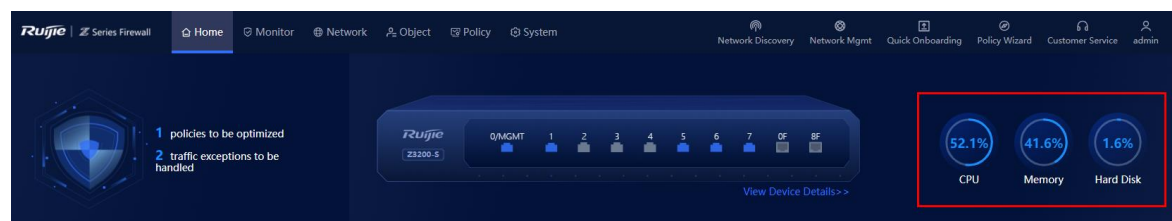
- (1) Check the network connection.
- (2) If the network connection is normal, choose **System > System Config > Service Parameters > SSH** and modify the SSH port number.

**Figure 10-1 Modifying the SSH Port Number**

## 10.5 O&M and Monitoring

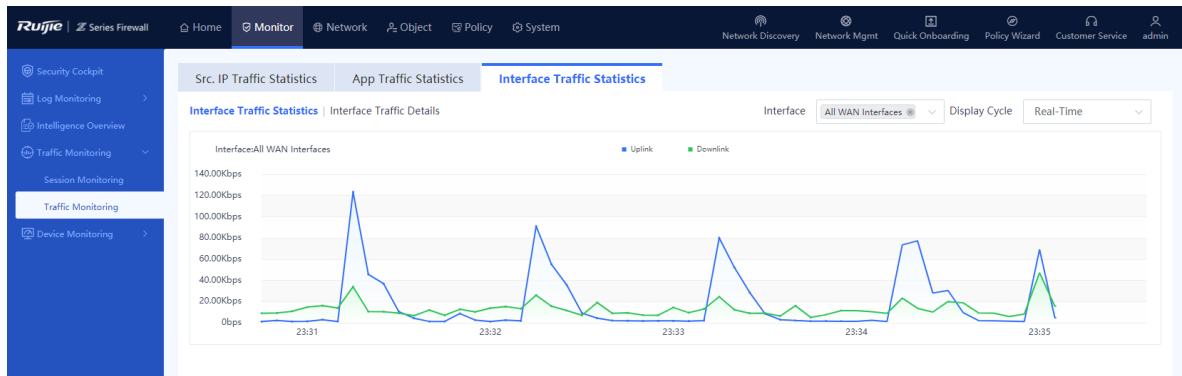
### 10.5.1 How Do I View the CPU, Memory, and Hard Disk Information of the Firewall?

Log in to the web management page, and view the CPU, memory, and hard disk usage on the home page.



### 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.



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.

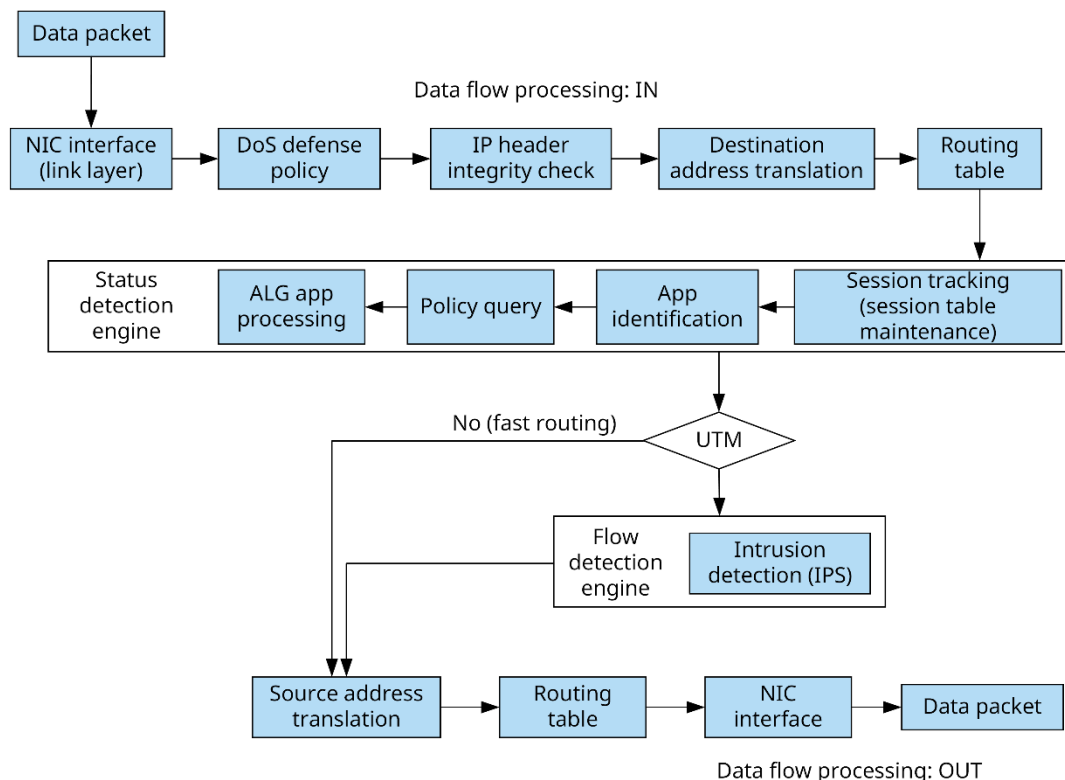
The data flow direction is determined by the source security zone and destination security zone, while the source address, destination address, service, and time range can directly reference defined objects.

- (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

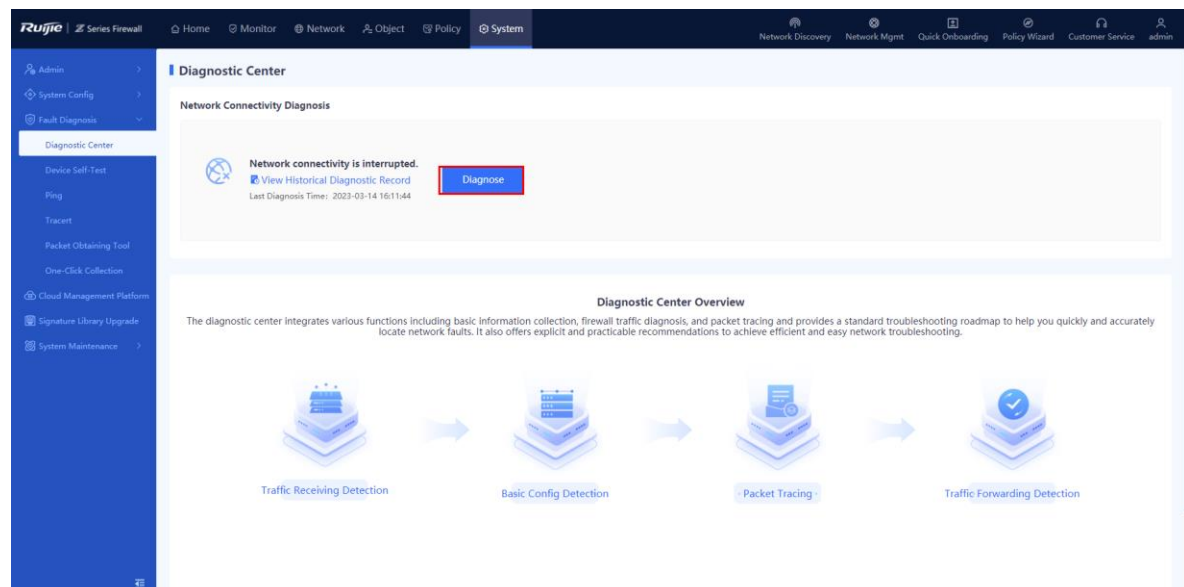
The diagnostic center integrates various functions including traffic receiving detection, basic configuration (security policy and NAT policy) detection, packet tracing, and traffic forwarding detection and provides a standard troubleshooting roadmap to help you locate network faults with one click. 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**.



- (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**

① 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.

\* ① Src. Address       ① Src. Port

① Dest. Address       ① Dest. Port

Inbound Interface       \* Protocol

① Src. MAC       ① Dest. MAC

(4) (Optional) Stop diagnosis or exit the diagnostic task at any time if required.

### Network Connectivity Diagnosis

**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

23%

① ② ③ ④

① Traffic Receiving Detection completed within 235second      ② Basic Config Detection      ③ Packet Tracing      ④ Traffic Forwarding Detection

**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

**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

Traffic Receiving Detection       Basic Config Detection       Packet Tracing       Traffic Forwarding Detection

The following 1 errors have been found. Please handle them according to suggestions.

**Diagnostic Result**

Result	Suggestion	Operation
interfacemodule: The interface has not obtained an IPv4 address.(Ge0/1)	interfacemodule: The interface has not obtained an IPv4 address.(Ge...	Check interface configuration and connections. <input type="button" value="Troubleshooting Operation"/> <input type="button" value="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 WAN 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 interface.	
The NAT module passes the check. <input checked="" type="checkbox"/>		
The security policy module passes the check. <input checked="" type="checkbox"/>		
The DNS module passes the check. <input checked="" type="checkbox"/>		
The DHCP module passes the check. <input checked="" type="checkbox"/>		

- (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.

Confirm

Cancel


- (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


Diagnose

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.




Traffic Receiving Detection



Basic Config Detection



Packet Tracing



Traffic Forwarding Detection

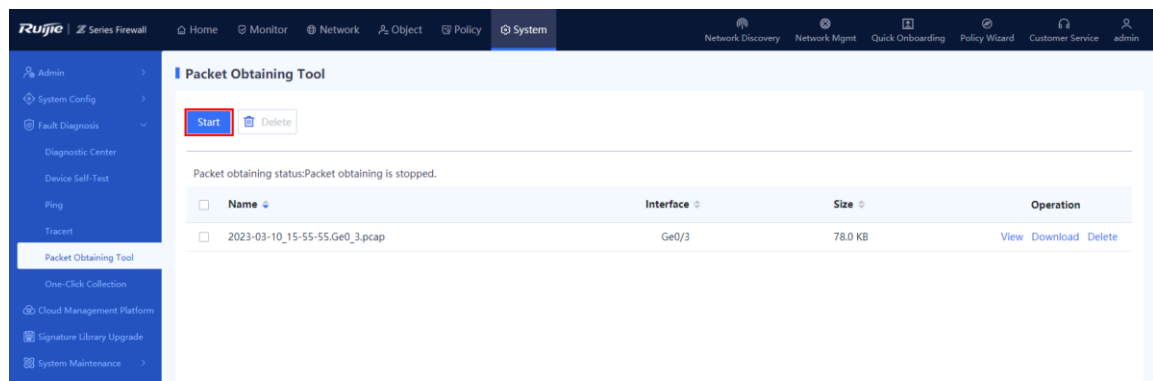
## 11.4 Packet Obtaining

### 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 Option



**i** 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**

#### Packet

#### Obtaining Rule

Layer 2 Protocol  any  IP  ARP

**1** Src. MAC

**1** Dest. MAC

**Start**

**Cancel**

- (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

**Packet Obtaining Rule**

Layer 2 Protocol  any  IP  ARP

Layer 3 Protocol  any  TCP  UDP

ⓘSrc. IP (Port)

ⓘDest. IP (Port)

ⓘ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



**i** 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**

#### Packet

#### Obtaining Rule

Layer 2 Protocol  any  IP  ARP

Layer 3 Protocol  any  TCP  UDP

**i**Src. IP (Port)

**i**Dest. IP (Port)

**i**Src. MAC

**i**Dest. MAC

Start

Cancel

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

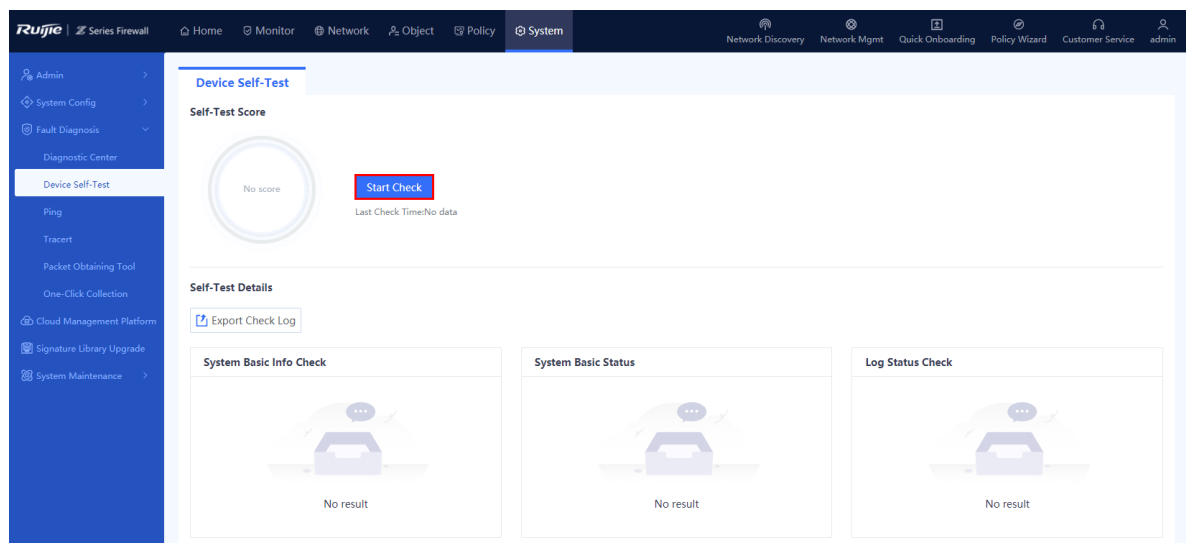
The device self-test function can detect the device version, CPU usage, memory usage, and whether risky configuration exists.

### **i** Note

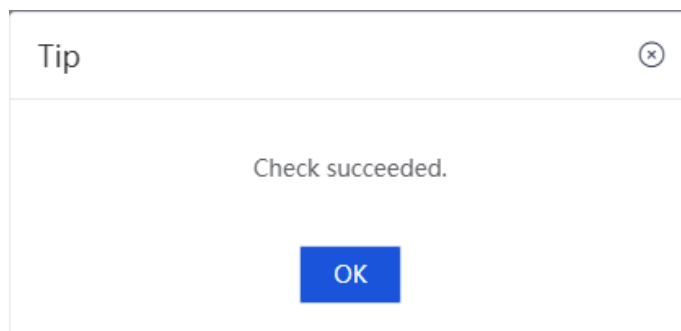
The device self-test function is supported from NTOS1.0R3. If your version is lower than NTOS1.0R3, upgrade it to NTOS1.0R3 or higher.

## 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**.



- (4) For an abnormal item, click **Fix** to switch to the corresponding configuration page.

**Device Self-Test**

**Self-Test Score**

83  
Self-Test Score

Start Check  
Last Check Time:2023-03-14 23:30:13

---

**Self-Test Details**

Export Check Log

<p><b>System Basic Info Check</b></p> <ul style="list-style-type: none"> <li>Device Model:Z3200-S</li> <li>Device Hardware SN:MACC932672666</li> <li>Device Software SN:M20540903132023</li> <li>Device Software Version:NGFW_NTOS 1.0R5, Release(03151320) Unable to obtain the version recommended by the cloud server.</li> </ul>	<p><b>System Basic Status</b></p> <p>CPU Usage: 35.4%</p> <p>Memory Usage: 41.5%</p>	<p><b>Log Status Check</b> -2points</p> <ul style="list-style-type: none"> <li>Whether Hard Disk Is Available:Yes</li> <li>Whether Syslog Server Is Set:No syslog server is set. The log storage time requirement may not be met.</li> </ul> <p>Fix</p>
<p><b>Management Mode Check</b> -10points</p> <ul style="list-style-type: none"> <li>SSH Login Failure Limit</li> <li>Admin Timeout Period: The login timeout period is long, and security risks exist.</li> </ul> <p>Fix</p>	<p><b>Authorization Status Check</b> -5points</p> <ul style="list-style-type: none"> <li>Threat Intelligence (TI): The license file has expired.</li> </ul>	<p><b>Policy Check</b></p> <ul style="list-style-type: none"> <li>High-risk policy: The interface configuration of the policy is any.</li> </ul>

## 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**.

Ruijie | Z Series Firewall | Home | Monitor | Network | Object | Policy | System | Network Discovery | Network Mgmt

**One-Click Collection**

One-click collection is complete. You can download collected information or perform collection again.

Last Collection Time:2023-03-11 13:40:28

One-Click Collection | Download

Admin | System Config | Fault Diagnosis | Diagnostic Center | Device Self-Test | Ping | Tracert | Packet Obtaining Tool | One-Click Collection | Cloud Management Platform | Signature Library Upgrade | System Maintenance

- (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
==== ebttables 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><E
5><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><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.

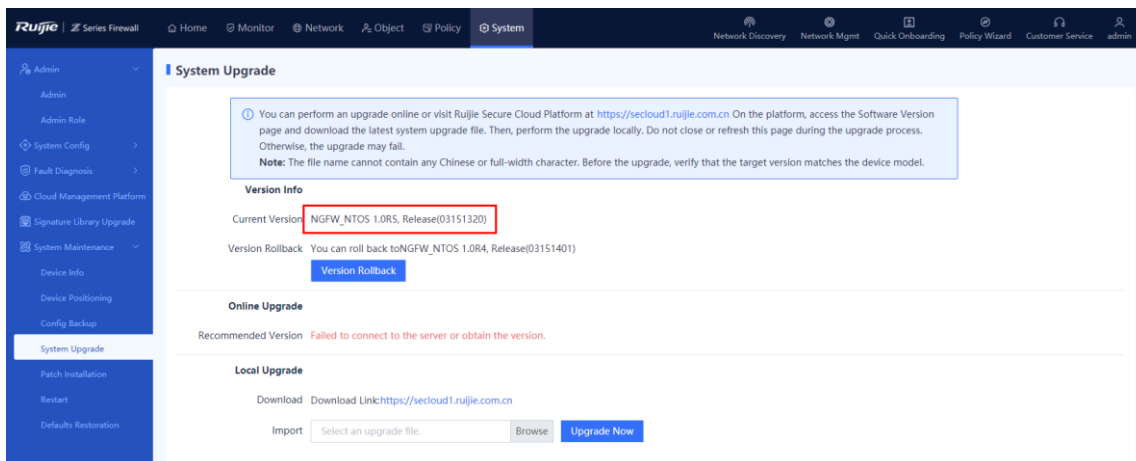
### Method

(1) Check whether the software version is recommended using one of the following methods:

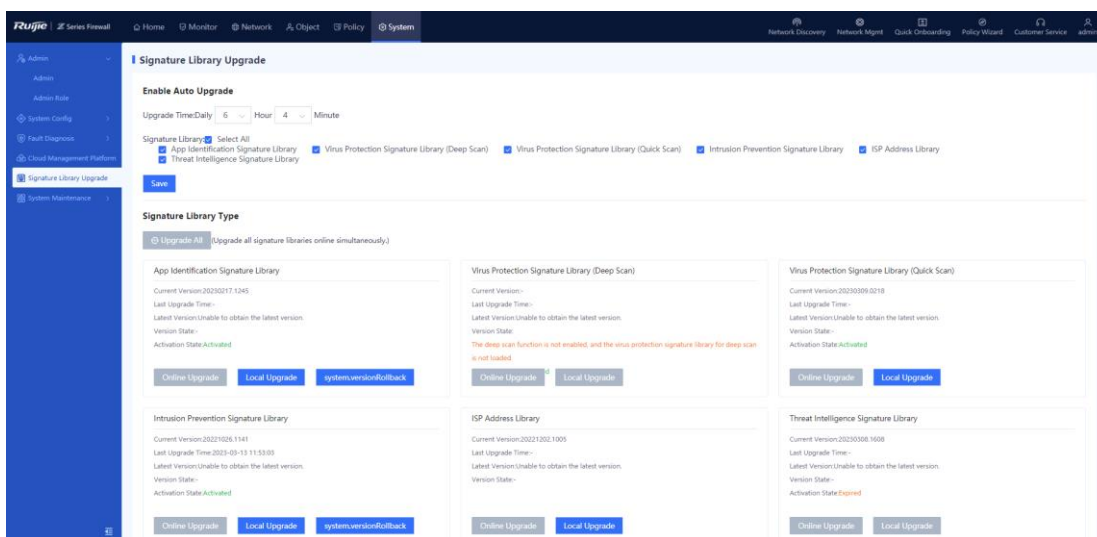
- Method 1: Log in to the Secure Cloud Platform (<https://secloud-en.ruijienetworks.com/>), click **Version Upgrade**, and select an applicable version to download it.

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	4C8772E66DCA4...	Z8620_Z8680	1.00	Universal	hijtest: z8600-20...	<a href="#">Download</a> <a href="#">View Version</a>
2	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2023-01-04	163.69	5FA916C58951B8...	Z8620_Z8680	1.00	Universal	hijtest: z8600-20...	<a href="#">Download</a> <a href="#">View Version</a>
3	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2022-12-29	167.41	a7277963ee08653...	Z8620_Z8680	1.00	Universal	lyftest1	<a href="#">Download</a> <a href="#">View Version</a>
4	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2022-12-28	127.76	07bee08c49f3c121...	Z5100	1.00	Universal	lyftest1	<a href="#">Download</a> <a href="#">View Version</a>

- 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**.



- (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.



## 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.

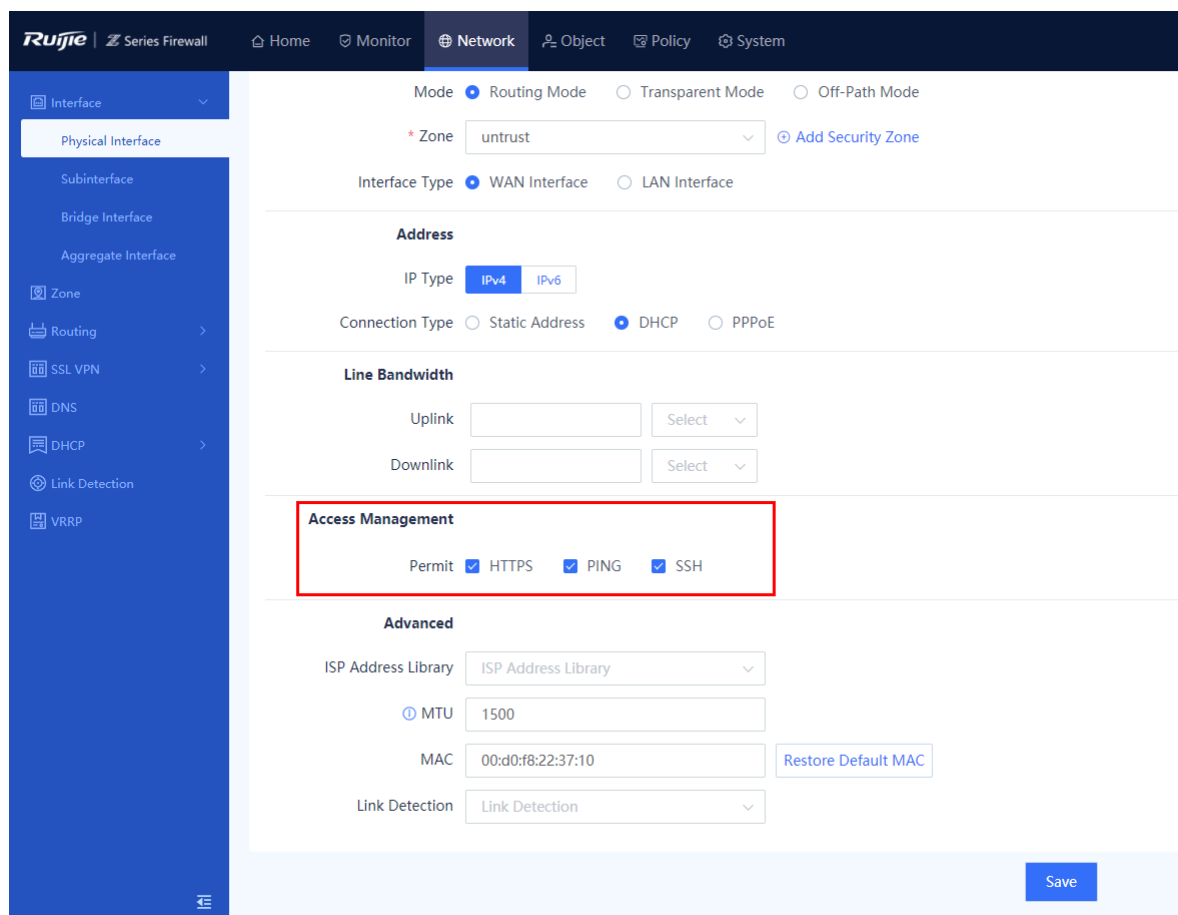
## Precautions

- 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.

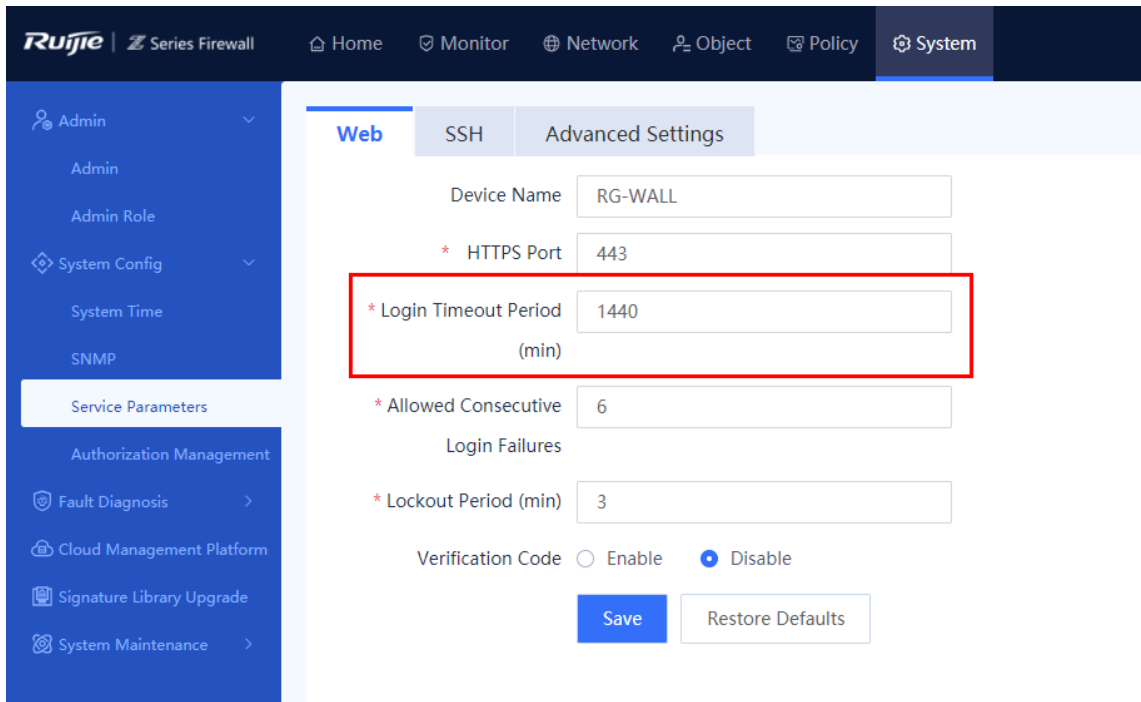
Log in to the web management page and choose **Network > Interface > Physical Interface**.



(2) Check whether web service parameters are set.

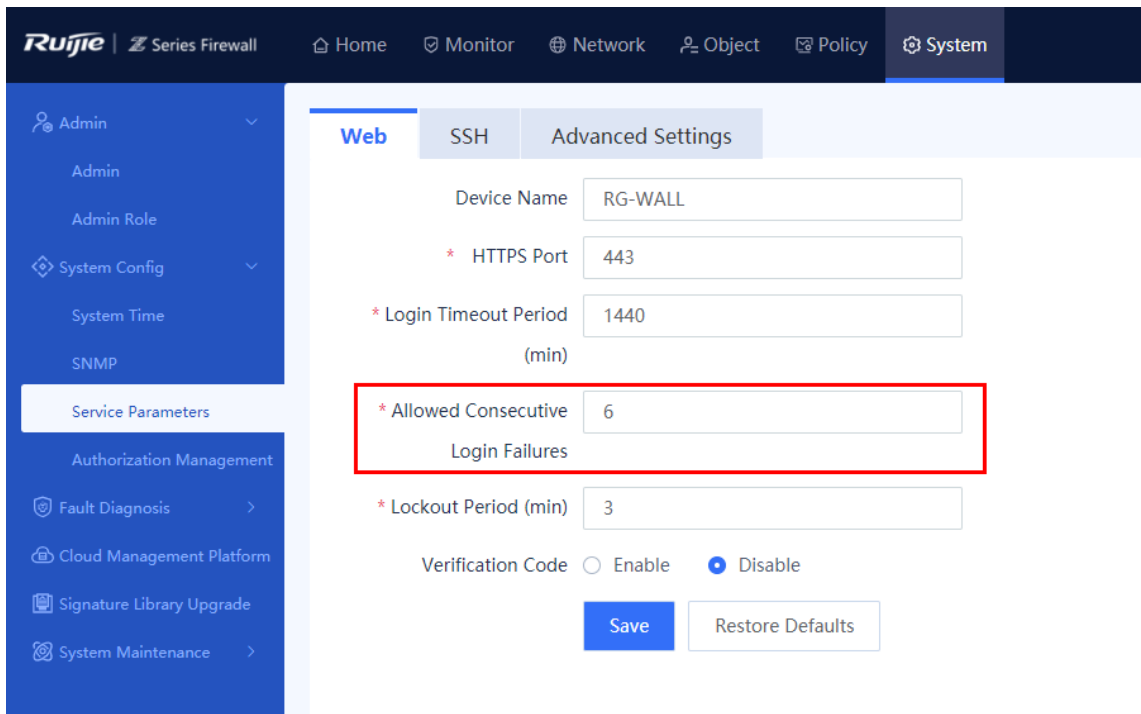
- Administrator login timeout period

Log in to the web management page and choose **System > System Config > Service Parameters**.



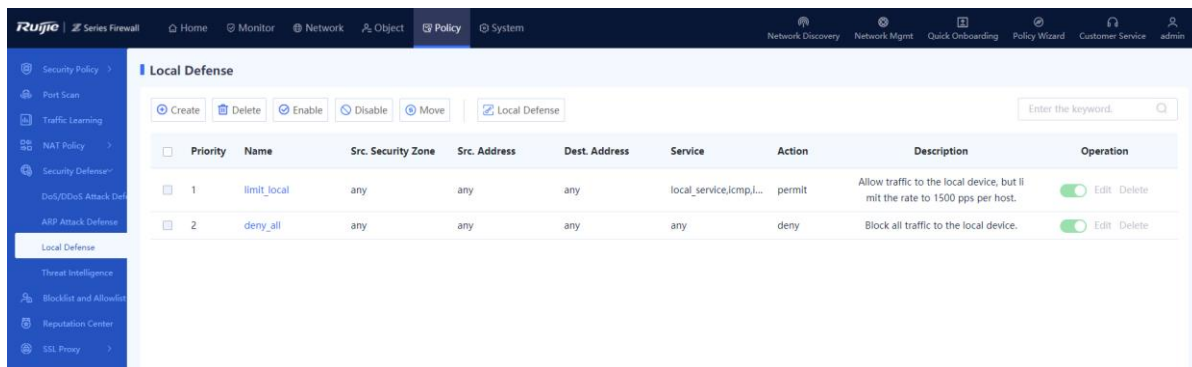
- Limit on administrator login failures

Log in to the web management page and choose **System > System Config > Service Parameters**.



(3) Management host settings

Log in to the web management page and choose **Policy > Security Defense > Local Defense**.



## 12.3 Checking Firewall Policies

### Standards

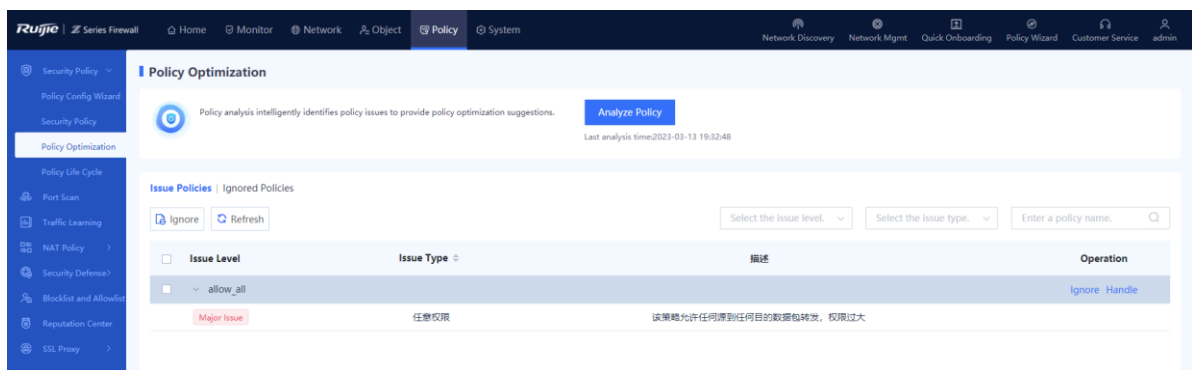
- An any-to-any policy makes the firewall meaningless and cannot achieve the purpose of access control. Administrators must know the data flow direction of customer services and implement access control based on the IP address and port number.
- All policies must be enabled. If a policy is not matched 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.)



## 12.4 Checking the Operation Status

### Standards

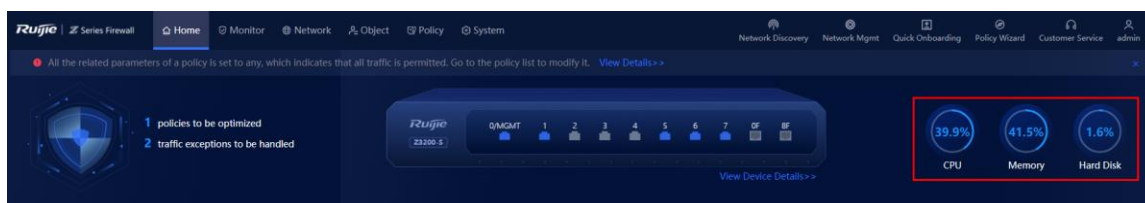
- Ensure that the CPU usage is lower than 75% during the service peak period. If the CPU usage of the firewall is too high, it may be encountered with attacks or abnormal traffic. In this case, the firewall stops forwarding data or discards packets and the firewall cannot be managed.
- Ensure that the 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.



## 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.

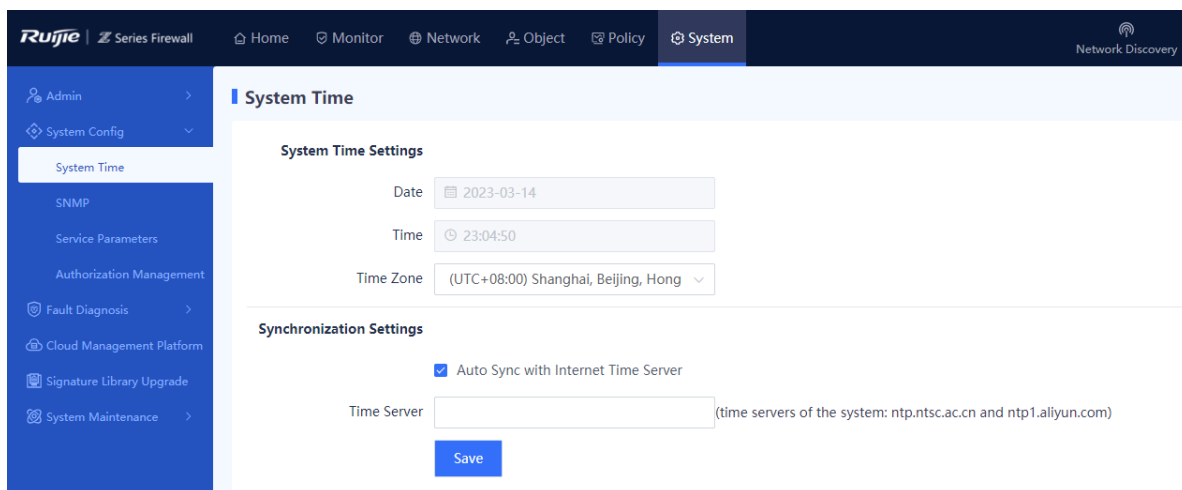
### Precautions

Confirm that the customer has purchased the relevant license.

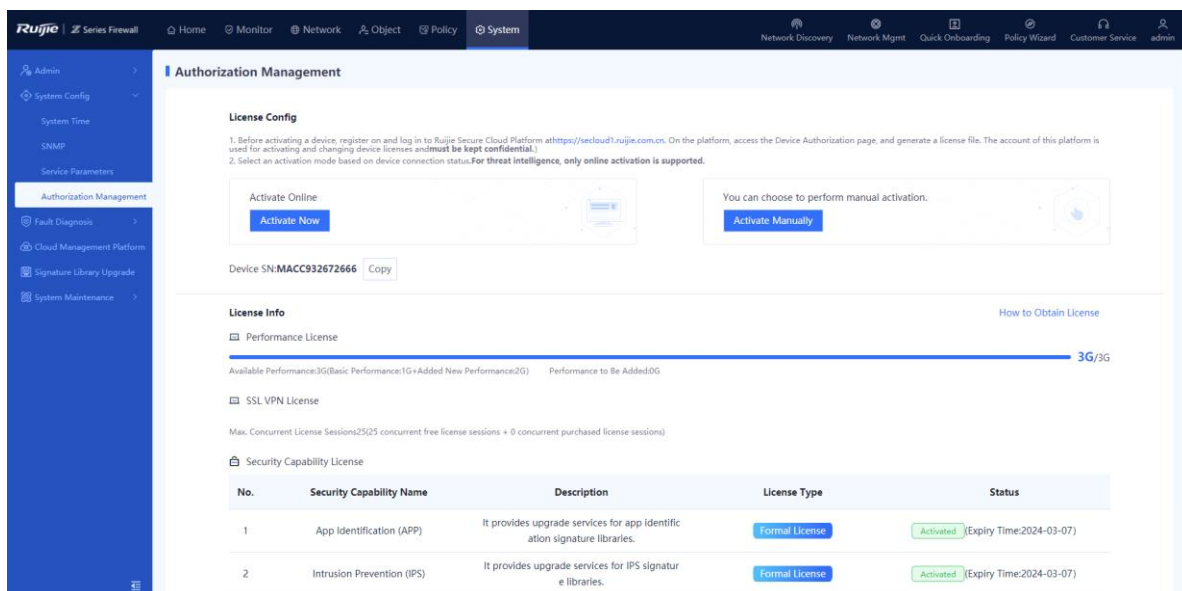
### Method

(1) Check whether the system time is accurate.

Log in to the web management page and choose **System > System Config > System Time**.



(2) Check the license status to confirm that the purchased license for the upgrade service is still valid.



## 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**.

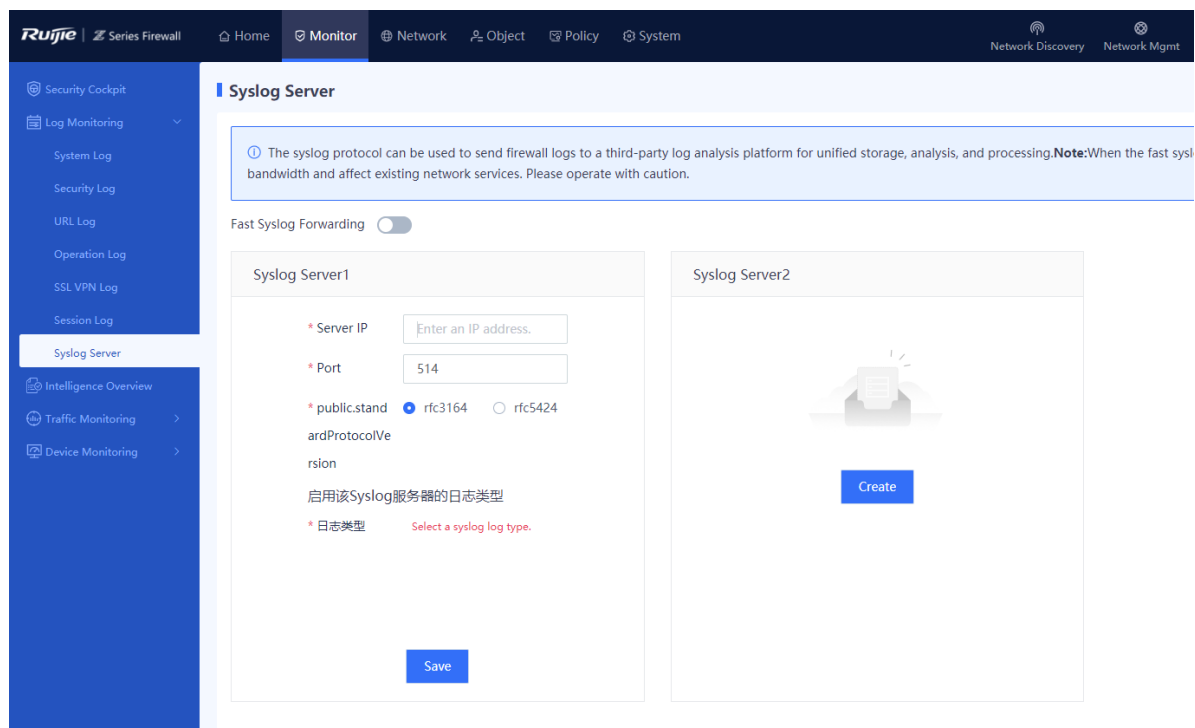


- Run the **firewall> show state system linux** command in the CLI.

```
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**.



## 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.

---

### **i** Note

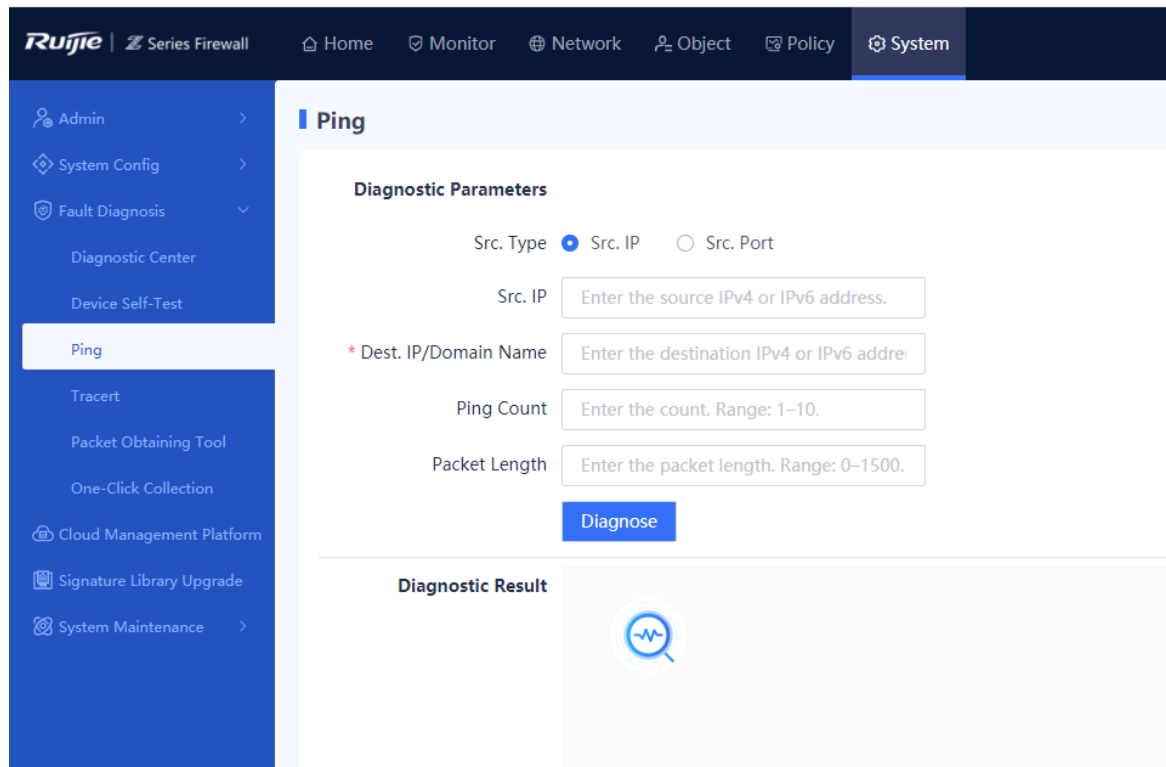
ICMP filtering is enabled on some network devices by default. When you perform the preceding operations on these devices, packet loss may occur periodically. You are advised not to set the destination address to the device IP address during the execution.

---

### 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.



## 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.