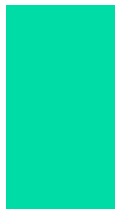
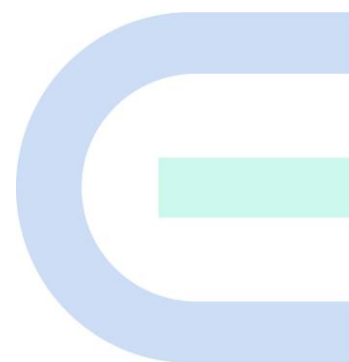


RG-WALL 1600-Z-S Series Cloud-Managed Firewall

V5.2-NGFW_NTOS1.0R6 User Manual



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 will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

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

Conventions

1. GUI Symbols

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

2. Signs

The signs used in this document are described as follows:

Danger

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

Warning

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

Caution

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

 Note

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

 Specification

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

3. Note

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

Contents

Preface	I
1 Overview	1
2 Quick Start Guide for the Web UI	2
2.1 Login on the Web UI	2
2.2 Web UI Layout	3
2.3 Operations on the Web UI	4
2.3.1 Changing Login User Password	4
2.3.2 Logging Out.....	6
3 Quick Deployment.....	7
3.1 Deployment Planning.....	7
3.1.1 Planning Device Locations and IP Addresses	7
3.1.2 Planning Networking Mode.....	7
3.1.3 Determining the Service Traffic Access Relationship	8
3.2 Deployment.....	9
3.2.1 Performing Quick Onboarding	9
3.2.2 Configuring Security Policies Using the Wizard	26
4 Integrated Deployment on Ruijie Cloud.....	35
4.1 Firewall Deployment (Routing Mode)	35
4.2 NBR Deployment (Transparent Mode).....	40
4.3 Deployment Using Ruijie Cloud App (Routing Mode)	45
4.4 Deployment Using Ruijie Cloud App (Transparent Mode)	56
5 Policy Configuration and Management.....	66
5.1 Security Policy	66

5.1.1 Overview	66
5.1.2 Manually Configuring Security Policies	66
5.1.3 Conducting Simulation Run	70
5.1.4 Importing Configuration Files to Configure Security Policies	72
5.1.5 Exporting Security Policies	75
5.1.6 Adjusting Security Policy Order	75
5.1.7 Optimizing Security Policies	76
5.1.8 Viewing Policy Life Cycle	78
5.1.9 Enabling Basic Protocol Packet Control	79
5.2 Enabling Port Scan	80
5.3 Enabling Traffic Learning	85
5.4 Traffic Control Policy	89
5.4.1 Overview	89
5.4.2 Configuring Traffic Control Policies	90
5.5 NAT Policy	95
5.5.1 NAT Overview	95
5.5.2 NAT Types	95
5.5.3 Working Principle	97
5.5.4 Configuring NAT	101
5.5.5 Configuring NAT46	113
5.5.6 Configuring NAT64	118
5.5.7 Configuring NAT66	122
5.5.8 Enabling the ALG Function	128
5.5.9 Configuring an Address Pool	129

5.5.10 Configuring NAT64 Prefixes	130
5.6 Security Defense.....	131
5.6.1 Overview	131
5.6.2 Attack Types.....	132
5.6.3 Configuring DoS/DDoS Attack Defense	133
5.6.4 Configuring ARP Attack Defense	139
5.6.5 Configuring Local Defense	143
5.7 Threat Intelligence	147
5.7.1 Overview	147
5.7.2 Enabling Threat Intelligence	147
5.7.3 Customizing Threat Intelligence	150
5.7.4 Configuring an Excluded Threat	154
5.7.5 Viewing Threat Intelligence Logs.....	155
5.7.6 Upgrading a Threat Intelligence Signature Library.....	156
5.8 Blocklist and Allowlist.....	156
5.8.1 Overview	156
5.8.2 Creating an IPv4 Allowlist	157
5.8.3 Creating an IPv6 Allowlist	158
5.8.4 Creating an IPv4 Blocklist.....	160
5.8.5 Creating an IPv6 Blocklist.....	161
5.8.6 Creating a Temporary IPv4 Blocklist.....	163
5.8.7 Creating a Temporary IPv6 Blocklist.....	164
5.9 SSL Proxy	166
5.9.1 Overview	166

5.9.2	Configuring an SSL Proxy Template	166
5.9.3	Configuring an SSL Proxy Policy	168
5.9.4	Configuring an SSL Proxy Allowlist.....	172
6	Object Configuration and Management	175
6.1	Address Object	175
6.1.1	Overview	175
6.1.2	Creating an IPv4 Address Object.....	175
6.1.3	Creating an IPv4 Address Group Object	177
6.1.4	Creating an IPv6 Address Object.....	179
6.1.5	Creating an IPv6 Address Group Object	180
6.2	Application	182
6.2.1	Overview	182
6.2.2	Viewing Application Information in a Signature Library	182
6.2.3	Creating a Custom Application	184
6.2.4	Creating a Custom Application Group	185
6.2.5	Upgrading an Application Identification Signature Library.....	187
6.3	URL Category	187
6.3.1	Overview	187
6.3.2	Viewing Predefined URL Categories	187
6.3.3	Configuring a Custom URL Category	188
6.4	Services	189
6.4.1	Overview	189
6.4.2	Configuring a Custom Service	190
6.4.3	Creating a Service Group	193

6.5 Time Plan	194
6.5.1 Overview	194
6.5.2 Creating a Cyclic Time Plan.....	195
6.5.3 Creating a One-Off Time Plan	196
6.6 ISP Address Library	197
6.6.1 Overview	197
6.6.2 Creating an ISP Address Library Manually.....	198
6.6.3 Creating an ISP Address Library by Importing an Address File	199
6.6.4 Upgrading an ISP Address Library	200
6.7 User Authentication	200
6.7.1 Overview	200
6.7.2 User Management	201
6.7.3 User Import	207
6.7.4 Online User	208
6.7.5 Authentication Domain Management.....	209
6.7.6 Authentication Policies	211
6.7.7 Authentication Settings	213
6.7.8 Authentication Server.....	220
6.8 Certificate Management.....	222
6.8.1 Overview	222
6.8.2 Local Certificate	222
6.8.3 SSL Certificate	223
6.9 Content Template	230
6.9.1 Virus Protection.....	230

6.9.2	Intrusion Prevention	235
6.9.3	URL Filtering	241
6.10	Security Rule Base	243
7	Network Configuration.....	245
7.1	Interface	245
7.1.1	Configuring a Physical Interface	245
7.1.2	Configuring a Subinterface	251
7.1.3	Configuring a Bridge Interface	256
7.1.4	Configuring an Aggregate Interface	260
7.1.5	Configuring a Tunnel interface	264
7.2	Security Zone	267
7.2.1	Overview	267
7.2.2	Creating a Security Zone	267
7.3	Route Management	269
7.3.1	Overview	269
7.3.2	Creating a Static Route.....	270
7.3.3	Creating an Intelligent Routing Policy.....	272
7.3.4	Viewing Address Library Routes.....	275
7.3.5	Viewing Route Tables	276
7.4	Outbound Interface Load Balancing	276
7.4.1	Overview	276
7.4.2	Configuring Source IP-based Load Balancing	277
7.4.3	Configuring Bandwidth-based Load Balancing	279
7.4.4	Viewing Load Balancing Session Information	281

7.5 SSL VPN.....	281
7.5.1 Overview	281
7.5.2 Creating an SSL VPN Gateway.....	282
7.5.3 Hardware Signature Management.....	293
7.5.4 Operation Monitoring	294
7.6 IPsec VPN.....	295
7.6.1 Overview	295
7.6.2 Principles.....	296
7.6.3 Configuring an IPsec Tunnel Using the Wizard.....	297
7.6.4 Custom Tunnel	313
7.6.5 Advanced Settings	326
7.6.6 Tunnel Monitoring	328
7.6.7 Viewing IPsec VPN Logs	330
7.7 DNS Server.....	330
7.7.1 Overview	330
7.7.2 Creating a DNS Server	331
7.8 DHCP Management.....	332
7.8.1 Overview	332
7.8.2 Configuring a DHCP Server.....	332
7.8.3 Address Management List	337
7.9 Link Detection	338
7.9.1 Link Detection	338
7.9.2 Detection Log.....	340
7.10 VRRP	340

7.10.1 Overview	340
7.10.2 Working Process	341
7.10.3 Configuring a VRRP Group	342
7.10.4 Viewing VRRP Logs.....	345
8 System Management	346
8.1 Administrators	346
8.1.1 Overview	346
8.1.2 Enabling Default Accounts.....	346
8.1.3 Creating an Administrator Account	348
8.1.4 Modifying the Administrator Password Security Policy	353
8.1.5 Modifying the Administrator Password	354
8.2 System Configuration	355
8.2.1 Setting System Time	355
8.2.2 Configuring SNMP	357
8.2.3 Configuring Service Parameters.....	361
8.3 Activating the License	365
8.4 Fault Diagnosis	367
8.4.1 Diagnostic Center	367
8.4.2 Device Self-Test	370
8.4.3 Ping	371
8.4.4 Tracert	372
8.4.5 Packet Obtaining Tool	373
8.4.6 One-Click Fault Information Collection	375
8.5 Signature Library Upgrade.....	375

8.6 System Maintenance	378
8.6.1 Checking Device Information.....	378
8.6.2 Managing Configuration Backup.....	378
8.6.3 Upgrading the System	380
8.6.4 Installing Patches.....	383
8.6.5 Restarting the Device.....	385
8.6.6 Restoring to Factory Settings	385
9 Security Monitoring Management	387
9.1 Security Cockpit.....	387
9.2 Log Monitoring Management.....	388
9.2.1 Log Overview	388
9.2.2 Querying Logs.....	388
9.2.3 Configuring the Syslog Server	395
9.3 Intelligence Overview.....	398
9.4 Traffic Monitoring	400
9.4.1 Interface Traffic	400
9.4.2 Real-Time Traffic.....	401
9.4.3 Traffic Statistics	402
9.5 Session Monitoring	403
9.5.1 Overview	403
9.5.2 Session Change Trend	403
9.5.3 Real-Time Session Information	405
9.6 Device Hardware Monitoring	407
10 Ruijie Cloud Connection.....	410

10.1 Overview	410
10.2 Connecting to Ruijie Cloud	410
10.2.1 Starting Ruijie Cloud	410
10.2.2 Binding Devices	410
10.3 Operations on Ruijie Cloud.....	412
10.3.1 Viewing Device Information	412
10.3.2 Managing Tunnels.....	414
10.3.3 Upgrading Device Software	415
10.3.4 Viewing Network Topology.....	417
11 Typical Configuration Examples.....	418
11.1 Configuring Extranet Users to Access Intranet Servers.....	418
11.2 Configuring Intranet Users to Access Intranet Servers Through a Public IP Address	421
11.3 Configuring DDoS Attack Defense	426
12 FAQs.....	431
12.1 What Can I Do If I Fail to Log In to the Web Page?	431
12.2 What Can I Do If I Fail to Log In to the System Through SSH?	432

1 Overview

The RG-WALL 1600-Z-S series cloud management firewall (the Z-S series firewall for short) is the next-generation firewall for all industry users. With cloud-network synergy, the Z-S series firewall continuously enhances its security detection capabilities, transforming passive defense to active defense based on rapid detection and proactive processing.

The Z-S series firewall provides proactive asset discovery, quick onboarding, and one-click fault analysis, simplifying product launch and O&M. It also supports rich security features, including intrusion prevention, antivirus, port scan, DoS/DDoS attack defense, and threat intelligence. This product can be widely used on networks in low-end and mid-range industries that require a simple network structure and diverse applications, such as primary and secondary schools, county hospitals, and small and medium-sized businesses (SMBs).

2 Quick Start Guide for the Web UI

The Z-S series firewall provides a graphical web UI for management, enabling efficient configuration and management.

2.1 Login on the Web UI

Application Scenario

After logging in to the web UI through HTTPS, the administrator can configure and manage firewalls on the UI.

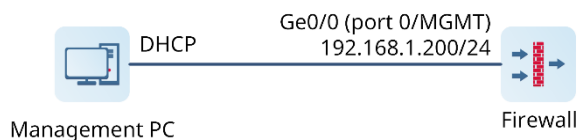
Prerequisites

- 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.

Table 2-1 Default Web Configurations

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

- 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.



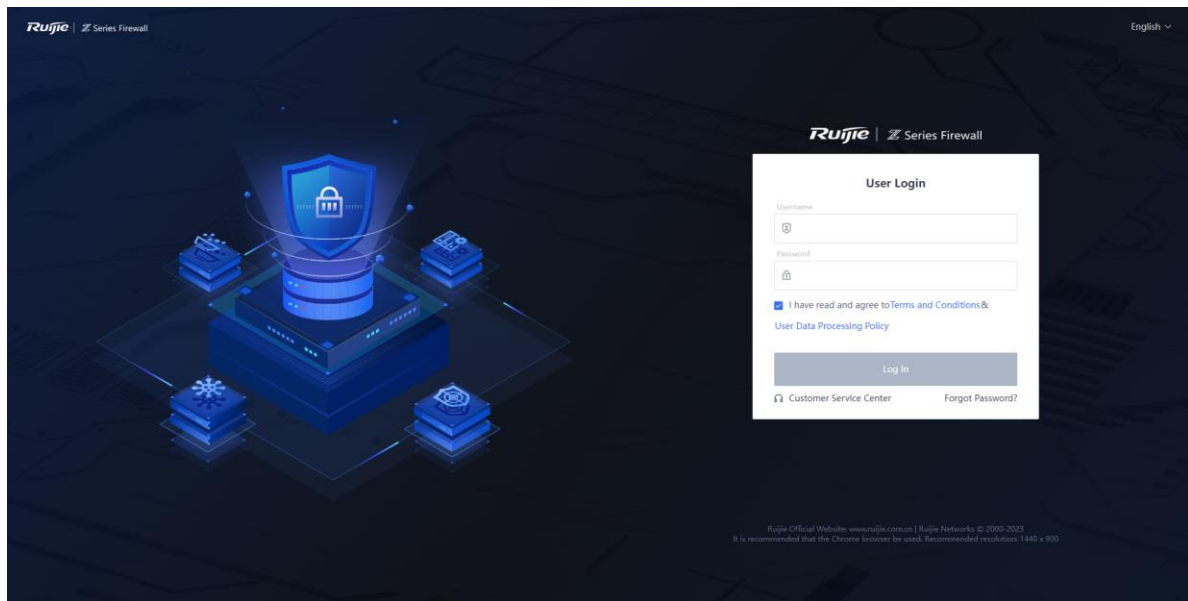
- The DHCP server is enabled for port 0/MGMT by default so that the local NIC of the management PC can automatically obtain an IP address from and communicate with the firewall. No manual IP address configuration is required.
- The management PC meets relevant requirements on the browser and resolution.
 - Browsers: Internet Explorer 11.0, Google Chrome, Firefox, and some Internet Explorer kernel-based browsers are supported. If other browsers are used for login, 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 interface, affecting the use experience.

Procedure

- (1) Open a browser on the management PC.

(2) Enter **https://192.168.1.200** in the address bar and press **Enter**.

The login page is displayed.



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

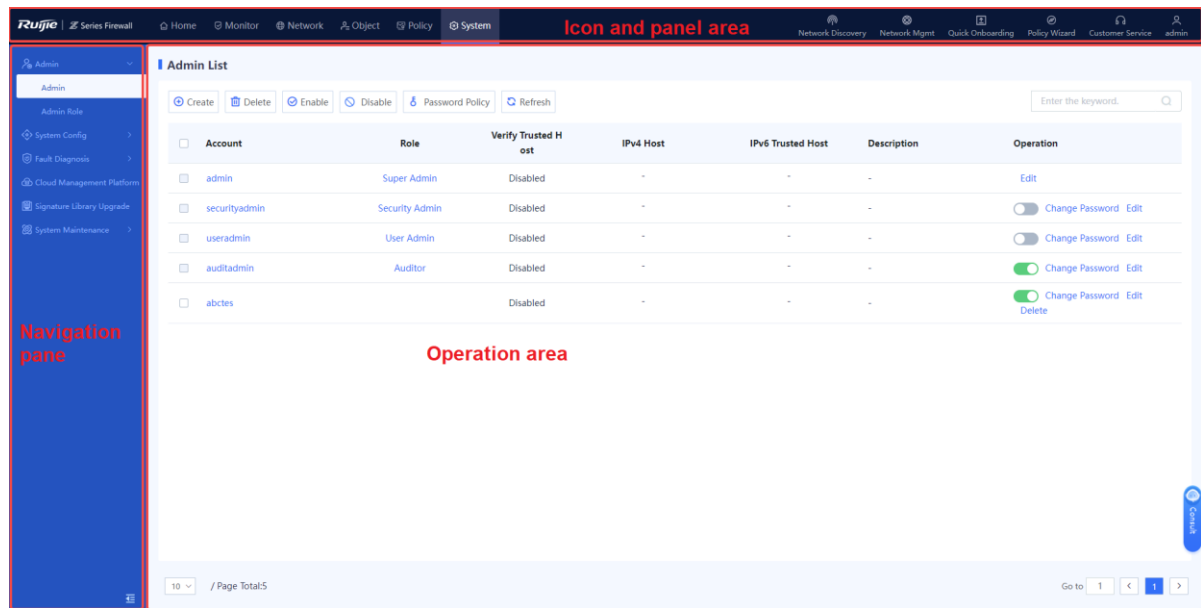
i Note

Verification code sending is enabled for the web service by default. If this function is disabled, you do not need to enter the verification code for login.

2.2 Web UI Layout

After login, the web UI is displayed, as shown in [Figure 2-1](#).

Figure 2-1 Web UI Layout



Area	Description
Icon and panel area	<ul style="list-style-type: none"> This area displays the company logo, device name, and function panel. This area supports new network discovery, network-wide management, quick onboarding, policy configuration wizard, and customer service, helping users quickly complete deployment operations. This area displays the current login user and allows you to change the password and log out.
Navigation pane	This area displays the web function menus of the device in the tree structure. You can click a function menu in the navigation pane to access the corresponding configuration page, which is displayed in the operation area.
Operation area	In this area, you can perform configuration operations and view information and the operation results.

2.3 Operations on the Web UI

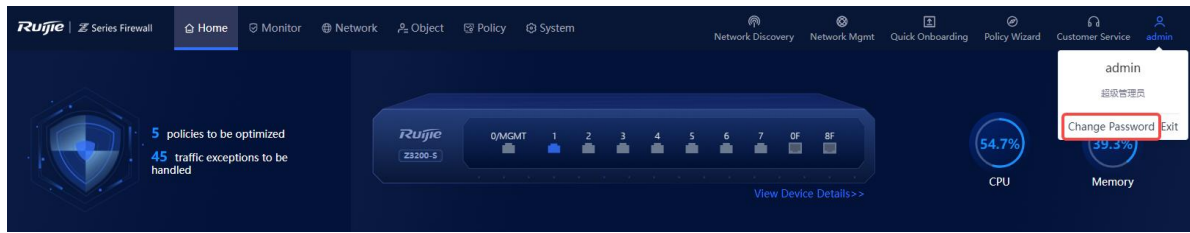
2.3.1 Changing Login User Password

Application Scenario

After login using a default account, change your password to ensure account security.

Procedure

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



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

Change Password ⊗

* Old
Password

* ① New
Password

* Confirm
Password

Confirm
Cancel

Item	Description	Remarks
Old Password	Old password of the login user.	You need to obtain the password of the login user in advance.
New Password	Password after change.	Password description: <ul style="list-style-type: none"> ● 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	Password after change that is entered again.	The value of Confirm Password must be the same as that of New Password .

(3) Click **Confirm** to save the new password.

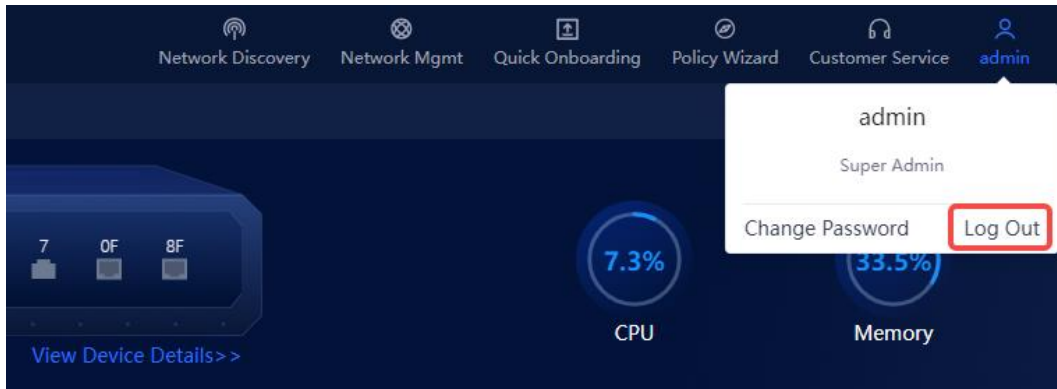
2.3.2 Logging Out

Application Scenario

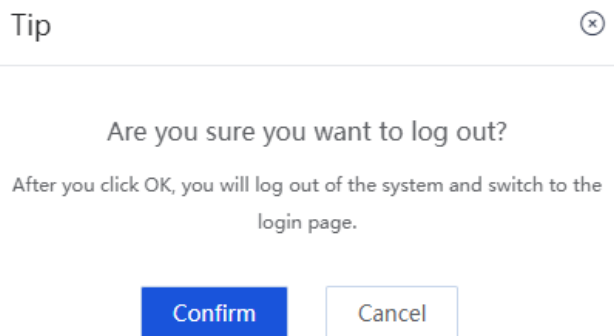
If no operation is performed on the web UI within a period of time, the administrator should log out to ensure account security.

Procedure

- (1) In the icon and panel area, click the name of the login user and choose **Log Out** from the short-cut menu.



A dialog box is displayed.



- (2) Click **Confirm**.

The login page is displayed.

3 Quick Deployment

3.1 Deployment Planning

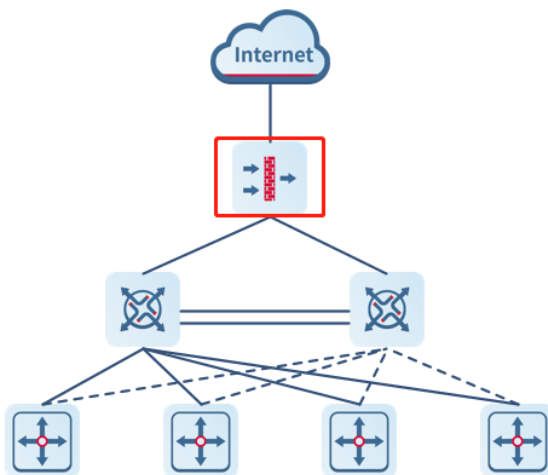
3.1.1 Planning Device Locations and IP Addresses

Determine the firewall location, for example, intranet demilitarized zone (DMZ), core/aggregation, or egress, based on network planning.

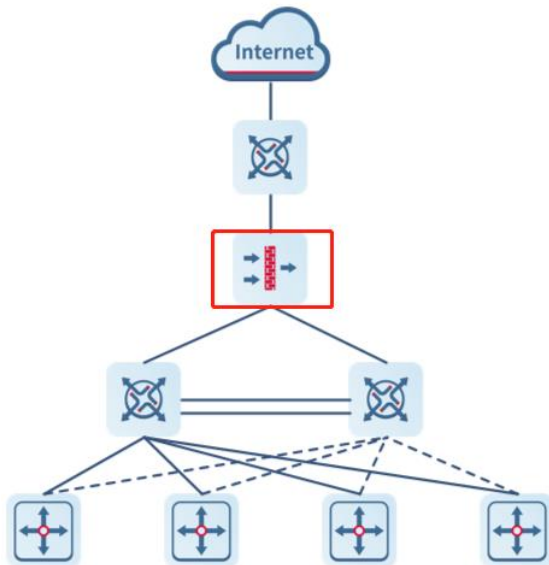
3.1.2 Planning Networking Mode

After determining the firewall location, select the corresponding networking mode.

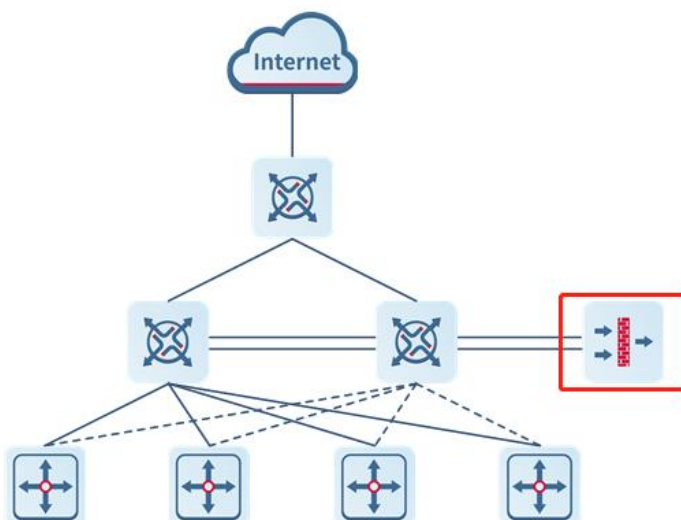
- At the network egress: Select the routing mode for the firewall to provide both security defense and some router functions, such as network address translation (NAT) and multi-ISP network access. Before configuring the routing mode, verify the Internet access mode. If the access mode is not configured according to the requirements of the local ISP, Internet access may fail.



- Between the core switches and egress router: Select the transparent mode for the firewall to enable security defense.



- Next to a core switch: Select the off-path mode for the firewall to detect traffic mirrored from the switch and enable security defense.



3.1.3 Determining the Service Traffic Access Relationship

When traffic on a network becomes more complex, security policy deployment should be optimized based on the service traffic access relationship.

Generally, you do not need to specify applications or time ranges in security policies. However, source/destination IP addresses, source/destination security zones, and services should be specified.

Consider the following aspects when configuring security policies:

- (1) Determine the firewall location on the network and divide security zones. Obtain network resource distribution of the live network according to the topology and identify critical information assets, services, and security levels.

- (2) Identify authorized services that are running on the live network for creating an allowlist.
- (3) Determine the communication matrix and service access rules based on the information security policies of enterprises, user group structure, and service allowlist.
- (4) Identify high-risk applications and unauthorized services (prohibited by the information security policies of enterprises) for creating a blocklist and determining service deny rules.
- (5) Create an all-permit policy from any to any first. Then, enable port scan and traffic learning to record policy hit logs. Optimize security policies based on the port scan and traffic learning results.

3.2 Deployment

3.2.1 Performing Quick Onboarding

Use the quick onboarding wizard on the web UI to quickly enable Internet access for firewalls.

1. Quick Onboarding (Routing Mode)

Application Scenario

When the routing mode is planned for a firewall, perform the following operations to quickly bring the firewall online.

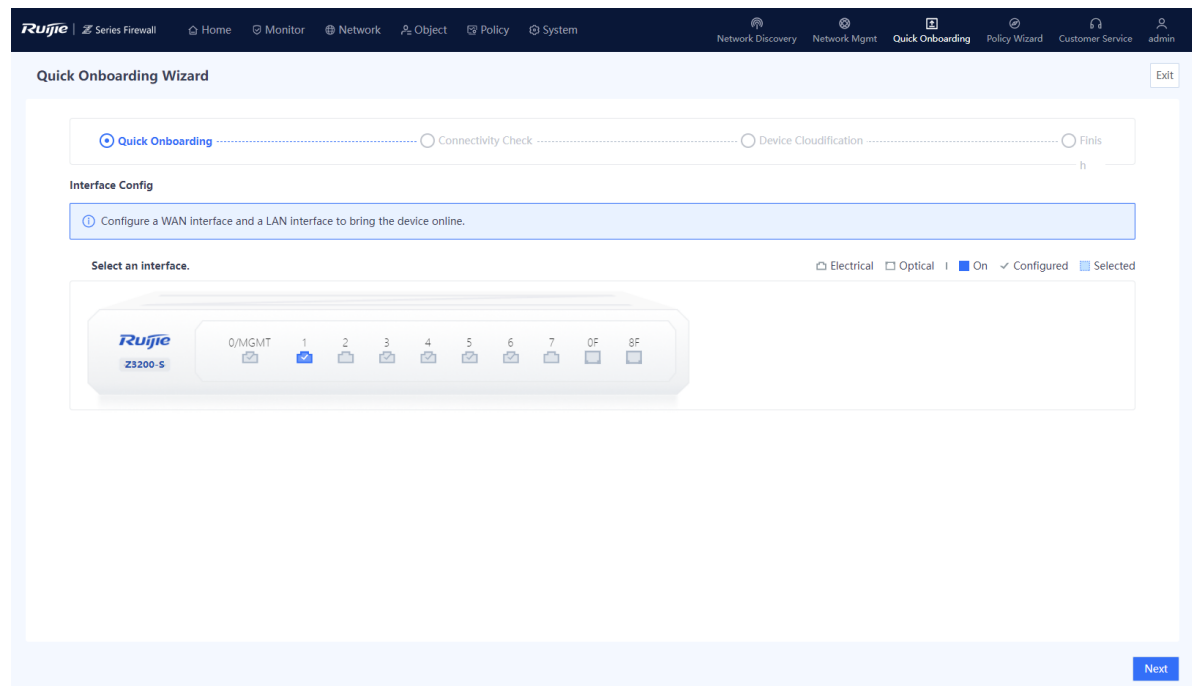
Prerequisites

You have planned the physical interfaces that function as one LAN interface and one WAN interface separately for quick Internet access.

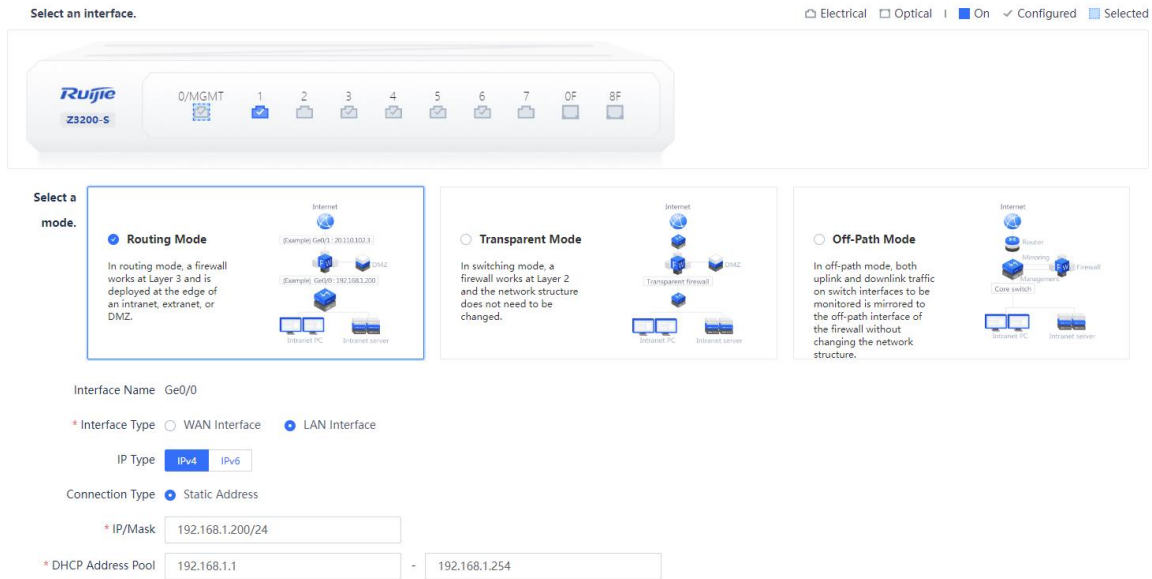
Procedure

- (1) On the right of the icon and panel area, click **Quick Onboarding**.

The **Quick Onboarding Wizard** page is displayed.



- (2) Configure the LAN interface.

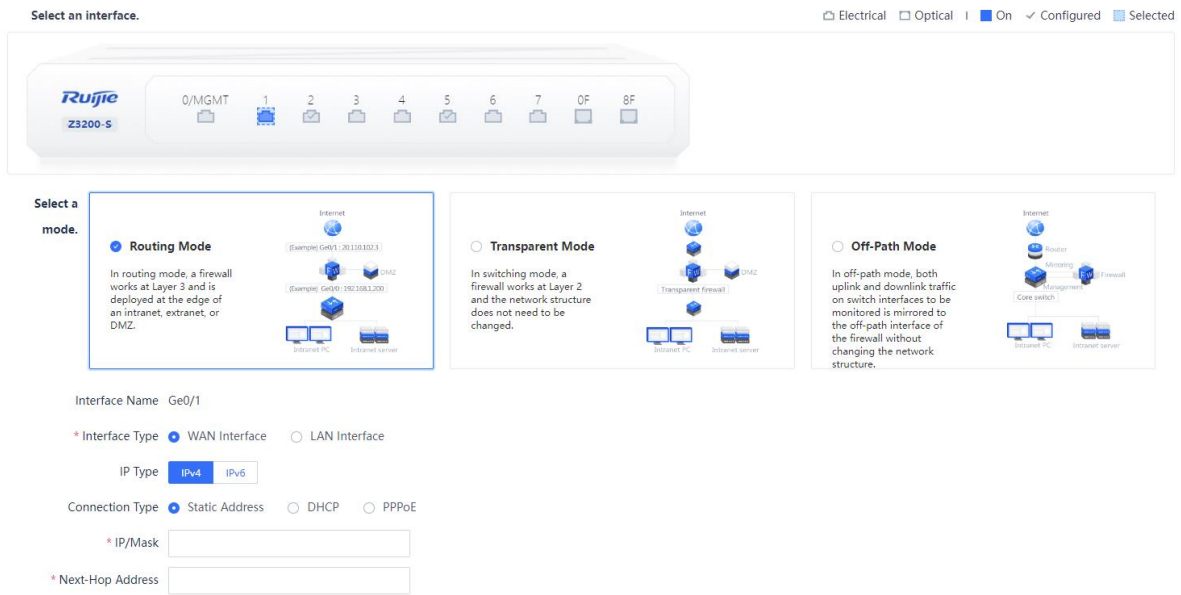


- a In the **Selecting Interface** area, select the interface that functions as the LAN interface.
- b In the Selecting Mode area, click Routing Mode.
- c Set parameters for the LAN interface.

Item	Description	Remarks
Interface Name	Name of the interface to be configured.	The system automatically displays the interface name. [Example] Ge0/6
Interface Type	LAN Interface: applicable for connection to LAN devices, such as PCs, switches, and printers.	[Example] LAN Interface
IP Type	Set the interface address type based on the network environment. Valid values: IPv6 and IPv4 . Both IPv4 and IPv6 addresses can be configured for an interface.	[Example] IPv4
IP Type: IPv4		
Connection Type	Connection type of the interface. The options are as follows: <ul style="list-style-type: none"> ● 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 must be configured. 	[Example] Static Address

Item	Description	Remarks
IP/Mask	IP address and mask of the interface.	You need to set this parameter when Connection Type is set to Static Address . [Example] 192.168.20.1/24
DHCP Address Pool	Set the range of IP addresses that can be assigned to downstream DHCP clients.	This configuration item is available only for port 0/MGMT. [Example] 192.168.110.17-192.168.110.254
IP Type: IPv6		
IPv6	Whether to enable the IPv6 function on the interface. When you set IP Type to IPv6 , you must enable IPv6 . Otherwise, the IPv6 address does not take effect.	[Example] Enabled
Connection Type	Connection type of the interface. The options are as follows: <ul style="list-style-type: none"> ● Static Address: Manually specify an IPv6 address for the interface. This configuration mode is applicable when the network administrator specifies an IPv6 address for the device based on the predefined IPv6 address planning. The IP address/prefix length must be configured. ● ND-RA: The interface automatically obtains an IPv6 address through the Neighbor Discovery-Router Advertisement (ND-RA) mode. 	[Example] Static Address
IP/Prefix Length	IPv6 address and address prefix length of the interface.	You need to set this parameter when Connection Type is set to Static Address . [Example] 2000::1/96
Advertise RA	Whether to allow the device to send RA packets on the interface. When this function is enabled, the device periodically sends RA packets, including prefix information options and information about certain flag bits, to advertise its presence.	[Example] Enabled

(3) Configure the WAN interface.



- a In the **Selecting Interface** area, select the interface that functions as the WAN interface.
- b In the Selecting Mode area, click Routing Mode.
- c Set parameters for the WAN interface.

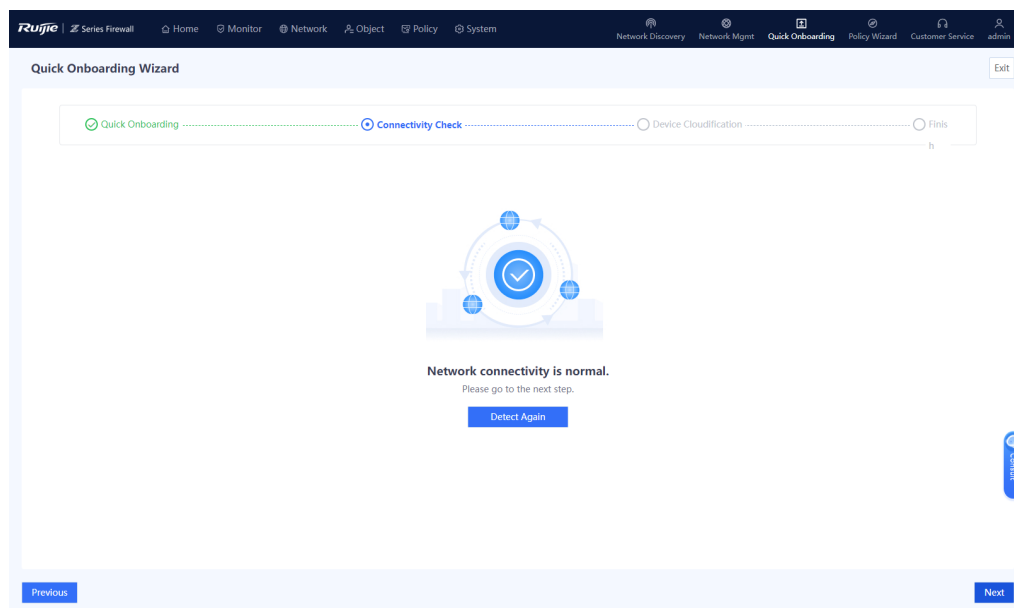
Item	Description	Remarks
Interface Name	Name of the interface to be configured.	The system automatically displays the interface name. [Example] Ge0/7
Interface Type	WAN Interface: Applicable to Internet access to connect the firewall to the Internet. Generally, the WAN interface is directly connected to the fiber to the home (FTTH) Optical Network Unit (ONU) of the ISP.	[Example] WAN Interface
IP Type	Set the interface address type based on the network environment. Valid values: IPv6 and IPv4 . Both IPv4 and IPv6 addresses can be configured for an interface.	[Example] IPv4
IP Type: IPv4		

Item	Description	Remarks
Connection Type	<p>Connection type of the interface. The options are as follows:</p> <ul style="list-style-type: none"> ● 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 the network administrator is not professional. The interface on the firewall automatically obtains an IP address from the connected ISP network or upper-layer DHCP server for Internet access. ● PPPoE: Applicable for dialup access to the ISP network. The username and password of the dialup user must be configured. 	<p>[Example]</p> <p>Static Address</p>
IP/Mask	IP address and mask of the interface.	<p>You need to set this parameter when Connection Type is set to Static Address.</p> <p>[Example]</p> <p>192.168.20.1/24</p>
Next-Hop Address	Next router address to reach the router with the destination address.	<p>You need to set this parameter when Connection Type is set to Static Address.</p> <p>[Example]</p> <p>192.168.20.2/24</p>
Account/Password	<p>Username and password for dialup access.</p> <p>Typically, they are assigned by the ISP.</p>	<p>You need to set this parameter when Connection Type is set to PPPoE.</p> <p>[Example]</p> <p>Admin/Ruijie@123</p>
IP Type: IPv6		
IPv6	Whether to enable the IPv6 function on the interface. When you set IP Type to IPv6 , you must enable IPv6 . Otherwise, the IPv6 address does not take effect.	<p>[Example]</p> <p>Enabled</p>

Item	Description	Remarks
Connection Type	<p>Connection type of the interface. The options are as follows:</p> <ul style="list-style-type: none"> ● Static Address: Manually specify an IPv6 address for the interface. This configuration mode is applicable when the network administrator specifies an IPv6 address for the device based on the predefined IPv6 address planning. The IP address/mask and next-hop address must be configured. ● ND-RA: The interface automatically obtains an IPv6 address through the Neighbor Discovery-Router Advertisement (ND-RA) mode. 	<p>[Example]</p> <p>Static Address</p>
IP/Prefix Length	IPv6 address and address prefix length of the interface.	<p>You need to set this parameter when Connection Type is set to Static Address.</p> <p>[Example]</p> <p>2001:1::1/64</p>
Advertise RA	Whether to allow the device to send RA packets on the interface. When this function is enabled, the device periodically sends RA packets, including prefix information options and information about certain flag bits, to advertise its presence.	<p>[Example]</p> <p>Enabled</p>

d After completing the configuration, click **Next**.

(4) The system automatically checks whether the firewall is connected to the Internet. If so, click **Next**.



i Note

If the firewall cannot connect to the Internet, click **Previous** to modify the interface configuration.

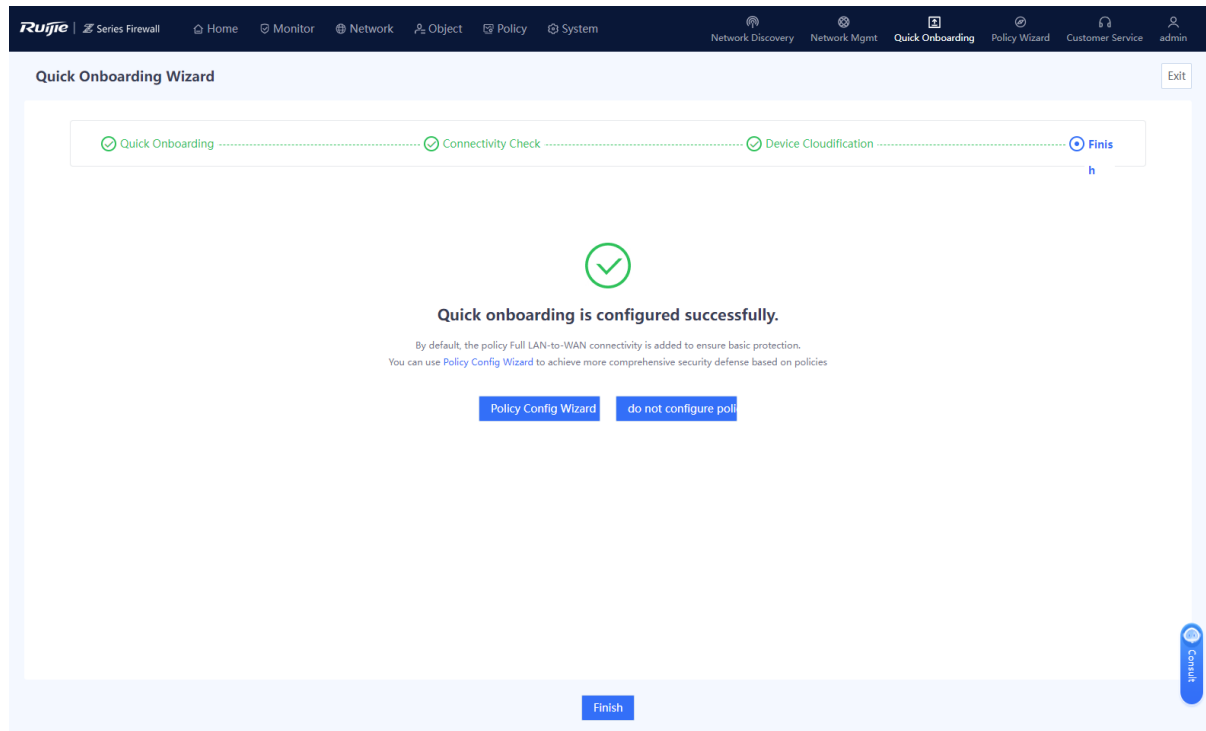
- (5) On the **Device Cloudification** page, enable the cloud management platform function and bind the device as prompted.

i Note

If the device cannot connect to the Internet, connect it to the cloud management platform according to 10 Ruijie Cloud Connection.

The screenshot displays the 'Quick Onboarding Wizard' interface. At the top, a progress bar shows four steps: 'Quick Onboarding' (completed), 'Connectivity Check' (completed), 'Device Cloudification' (current step), and 'Finish' (pending). Below the progress bar, the 'Enable Ruijie Cloud-based Management' section contains a blue box with the text: '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.' Below this, a toggle switch for 'Ruijie Cloud-based Management' is turned on. The 'Bind Device' section contains a blue box with the text: 'Use an account to manage gateways. Ruijie Cloud link: <http://cloud.ruijie.com.cn/>' and a note: '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.' Below the text is a QR code with the instruction: 'Bind the device by scanning the QR code on WeChat.' The interface includes an 'Exit' button in the top right corner and a 'Cancel' button in the bottom right corner.

- (6) After completing the configuration, click **Next**. Click **Finish** to complete quick onboarding configuration.



Verification

Connect the WAN interface of the device to the optical modem (or ONU), log in to the device through the management port, and choose **System > Fault Diagnosis > Ping**. Then, configure diagnostic parameters, as shown in [Figure 3-1](#), and click **Diagnose**.

Figure 3-1 Ping Example

Ping

Diagnostic Parameters

Src. Type Src. IP Src. Port

Src. IP

* Dest. IP/Domain Name

Ping Count

Packet Length

In the **Diagnostic Result** area, check whether the device can access the Internet properly. If so, quick onboarding is complete successfully.

Diagnostic Result



```

PING www.a.shifen.com (163.177.151.109) 56(84) bytes of data.
64 bytes from 163.177.151.109 (163.177.151.109): icmp_seq=1 ttl=52 time=19.5 ms
64 bytes from 163.177.151.109 (163.177.151.109): icmp_seq=2 ttl=52 time=18.9 ms
64 bytes from 163.177.151.109 (163.177.151.109): icmp_seq=3 ttl=52 time=18.8 ms
64 bytes from 163.177.151.109 (163.177.151.109): icmp_seq=4 ttl=52 time=19.3 ms
64 bytes from 163.177.151.109 (163.177.151.109): icmp_seq=5 ttl=52 time=19.0 ms

--- www.a.shifen.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 18.755/19.105/19.478/0.269 ms
    
```

2. Quick Onboarding (Transparent Mode)

Application Scenario

When the transparent mode is planned for a firewall, perform the following operations to quickly bring the firewall online.

Prerequisites

You have planned the physical interfaces that function as one LAN interface and one WAN interface separately for quick Internet access.



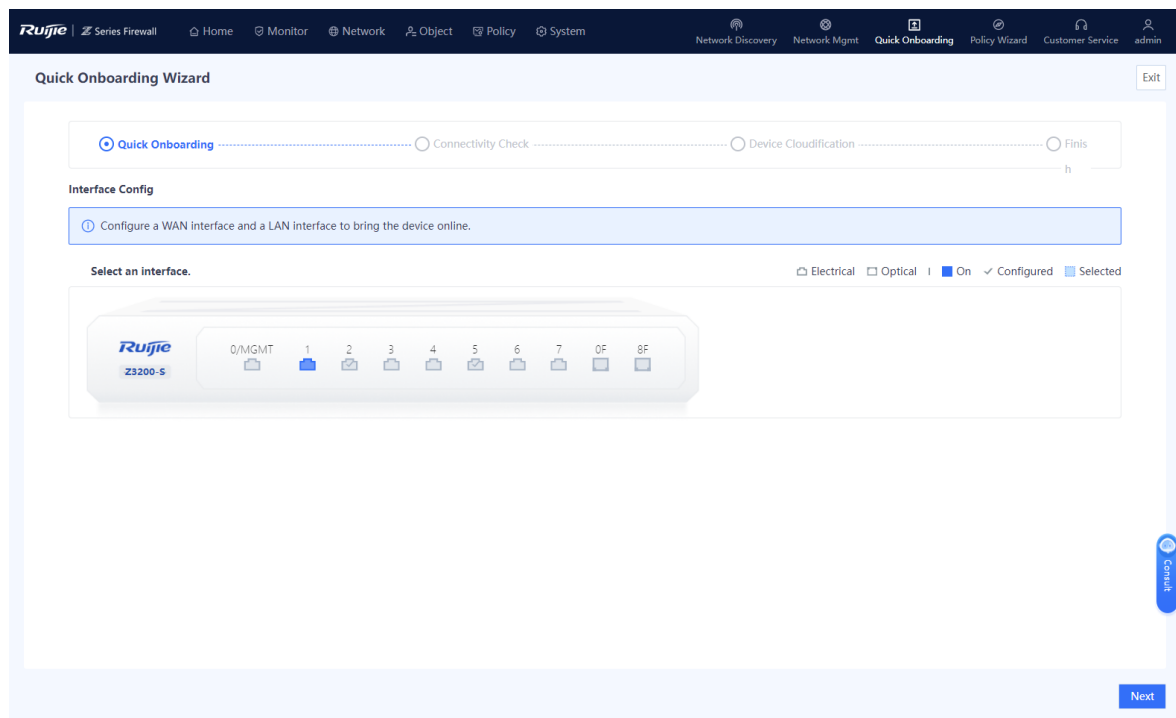
Note

Port 0/MGMT cannot be set to the transparent mode.

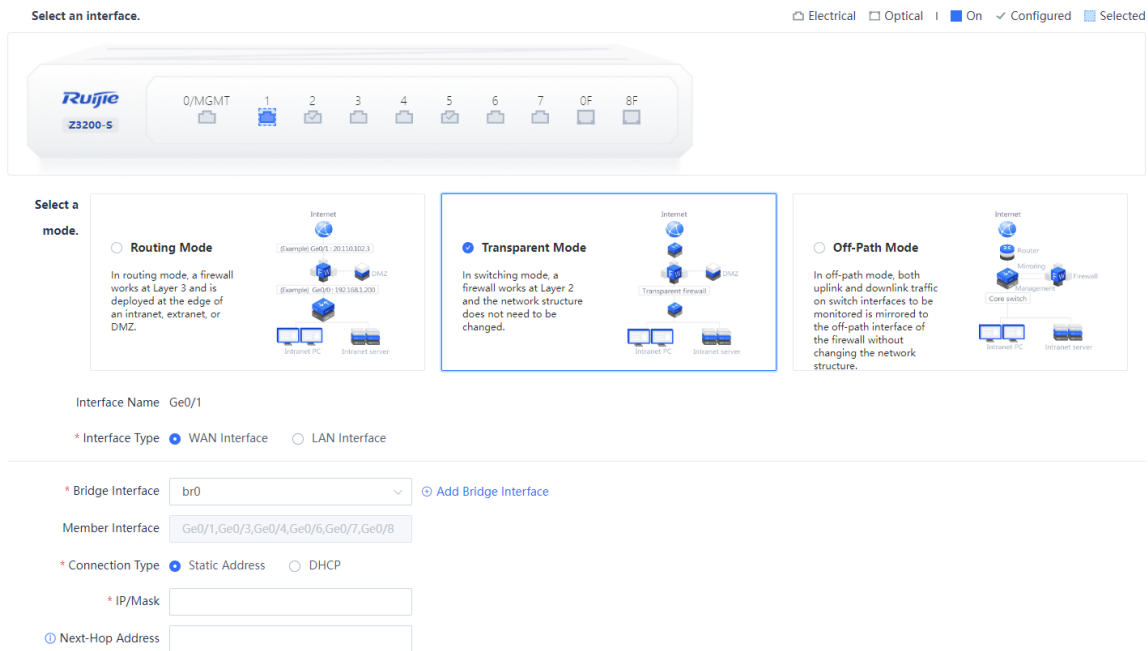
Procedure

- (1) On the right of the icon and panel area, click **Quick Onboarding**.

The **Quick Onboarding Wizard** page is displayed.

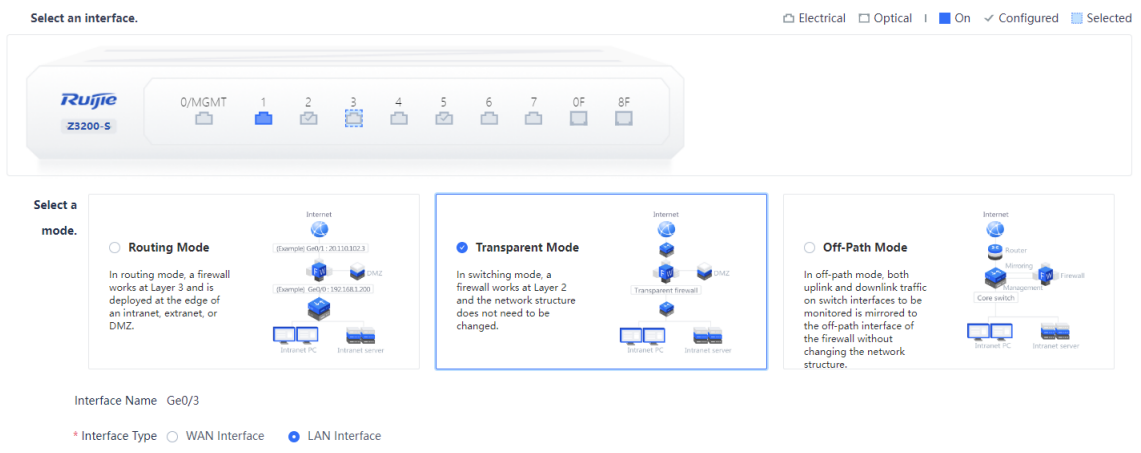


(2) Configure the WAN interface.



- a In the **Selecting Interface** area, select the interface that functions as the WAN interface.
- b In the **Selecting Mode** area, click **Transparent Mode**.
The system automatically displays the interface name.
- c Set **Interface Type** to **WAN Interface**.

(3) Configure the LAN interface.



- a In the **Selecting Interface** area, select the interface that functions as the LAN interface.
- b In the **Selecting Mode** area, click **Transparent Mode**.
The system automatically displays the interface name.
- c Set **Interface Type** to **LAN Interface**.

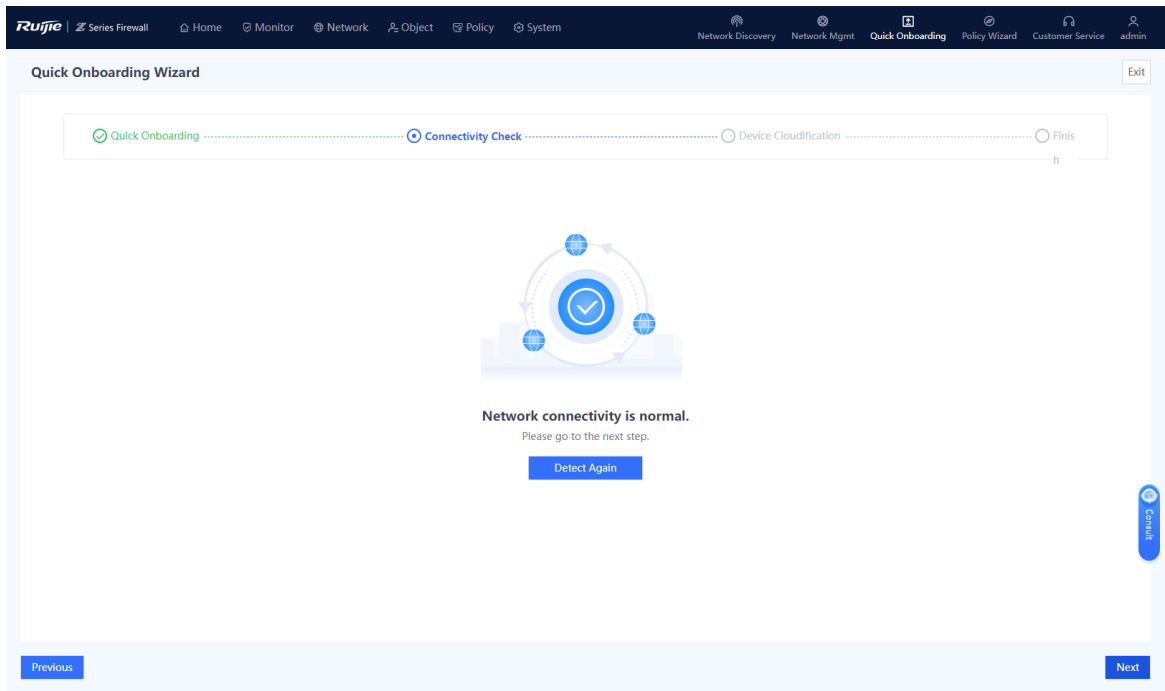
(4) Configure a bridge interface.

a Set parameters for the bridge interface.

Item	Description	Remarks
Bridge Interface	Bridge interface that the interface is added to.	The system has a default bridge interface br0 . To add a bridge interface, click Add Bridge Interface . For details, see 7.1.3 Configuring a Bridge Interface . [Example] br0
Member Interface	Member interface of the bridge interface. After an interface is added to a bridge interface, it becomes a member of the bridge interface.	[Example] Ge0/4,Ge0/5
Connection Type	Connection type of the interface. The options are as follows: <ul style="list-style-type: none"> ● 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 the network administrator is not professional. The bridge interface automatically obtains an IP address from the connected ISP network or upper-layer DHCP server for Internet access. 	[Example] Static Address
IP/Mask	IP address and mask of the interface.	You need to set this parameter when Connection Type is set to Static Address . [Example] 192.168.20.1/24
Next-Hop Address	Next router address to reach the router with the destination address.	You need to set this parameter when Connection Type is set to Static Address . [Example] 192.168.20.2/24

b After completing the configuration, click **Next**.

(5) The system automatically checks whether the firewall is connected to the Internet. If so, click **Next**.



Note

If the firewall cannot connect to the Internet, click **Previous** to modify parameters, and then check again.

- (6) (Optional) If the firewall can connect to the Internet, the **Enable Ruijie Cloud-based Management** page is displayed. Enable the cloud management platform function and bind the device as prompted.

Note

If the device cannot connect to the Internet, connect it to the cloud management platform according to 10 Ruijie Cloud Connection.

Enable Ruijie Cloud-based Management

Note 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

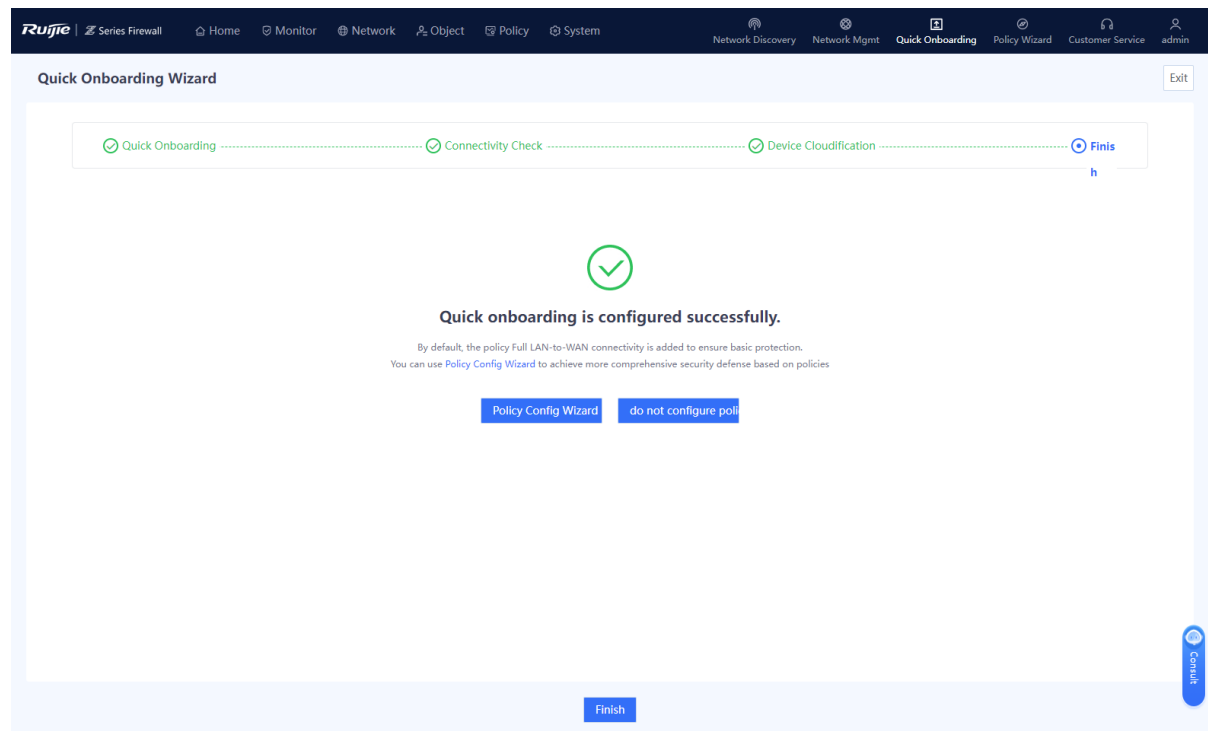
Bind Device

Note 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.

(7) After completing the configuration, click **Next**. Click **Finish** to complete quick onboarding configuration.



Verification

Connect the WAN interface of the device to the optical modem (or ONU), log in to the device through the management port, and choose **System > Fault Diagnosis > Ping**. Then, configure diagnostic parameters, as shown in [Figure 3-2](#), and click **Diagnose**.

Figure 3-2 Ping Example

Ping

Diagnostic Parameters

Src. Type Src. IP Src. Port

Src. IP

* Dest. IP/Domain Name

Ping Count

Packet Length

In the **Diagnostic Result** area, check whether the device can access the Internet properly. If so, quick onboarding is complete successfully.

Diagnostic Result

```
PING www.a.shifen.com (163.177.151.109) 56(84) bytes of data.  
64 bytes from 163.177.151.109 (163.177.151.109): icmp_seq=1 ttl=52 time=19.5 ms  
64 bytes from 163.177.151.109 (163.177.151.109): icmp_seq=2 ttl=52 time=18.9 ms  
64 bytes from 163.177.151.109 (163.177.151.109): icmp_seq=3 ttl=52 time=18.8 ms  
64 bytes from 163.177.151.109 (163.177.151.109): icmp_seq=4 ttl=52 time=19.3 ms  
64 bytes from 163.177.151.109 (163.177.151.109): icmp_seq=5 ttl=52 time=19.0 ms  
  
--- www.a.shifen.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4005ms  
rtt min/avg/max/mdev = 18.755/19.105/19.478/0.269 ms
```

3. Quick Onboarding (Off-Path Mode)

Application Scenario

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 structure of the live network or incur network interruption, the firewall can be deployed in off-path mode. In this mode, the firewall is connected to the switch in off-path mode to provide security defense for service traffic. This mode monitors the security of the customer network without changing the network structure or affecting data forwarding of the customer.

When the off-path mode is planned for a firewall, perform the following operations to quickly bring the firewall online.

Prerequisites

At least one off-path interface has been configured to mirror both uplink and downlink traffic on switch interfaces to be monitored to the off-path interface of the firewall. Corresponding physical interfaces have been planned.

To manage a firewall in off-path mode, you have connected port 0/MGMT to the extranet (for example, through a core switch) and configured the IP address and next-hop address for the port to enable extranet connectivity.

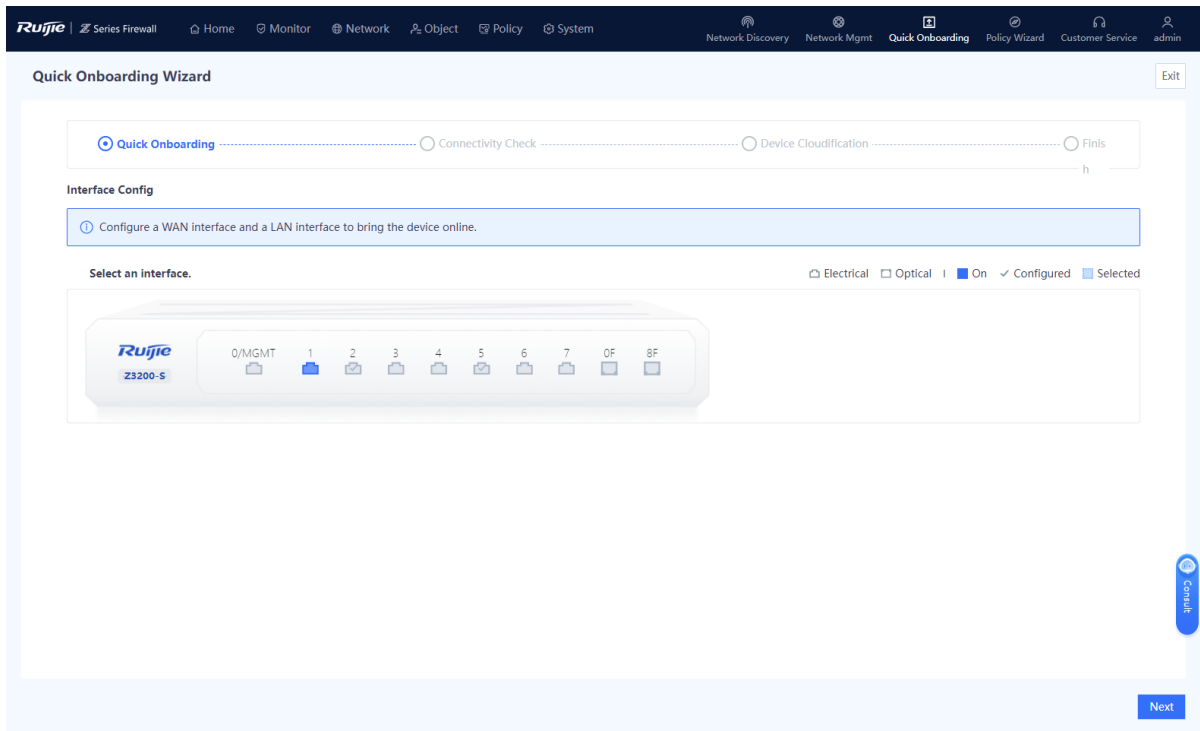
Note

Port 0/MGMT cannot be set to the off-path mode.

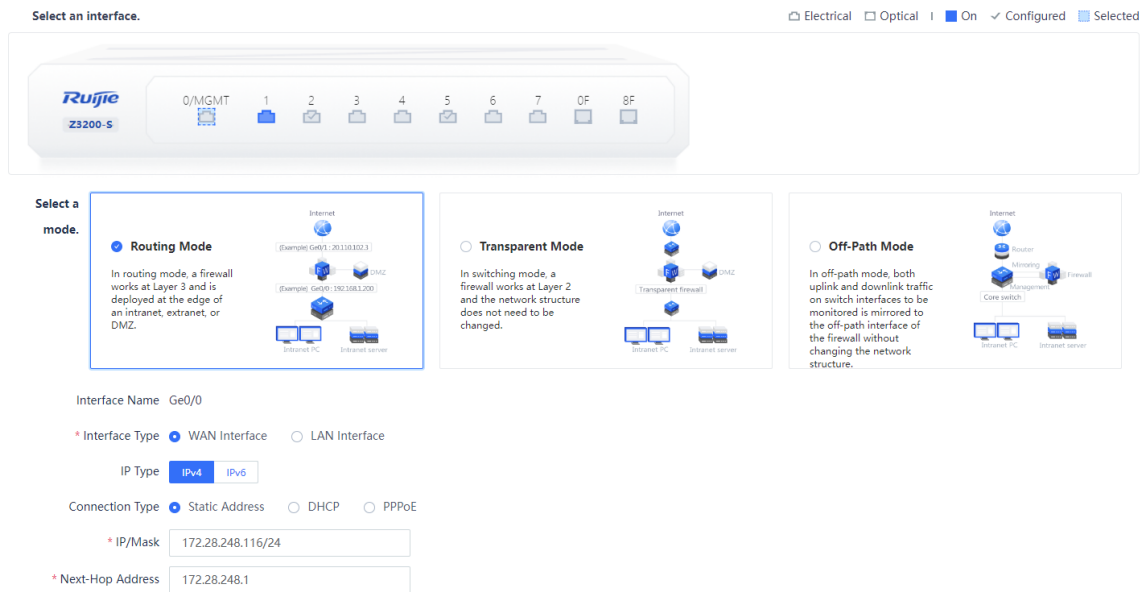
Procedure

(1) On the right of the icon and panel area, click **Quick Onboarding**.

The **Quick Onboarding Wizard** page is displayed.

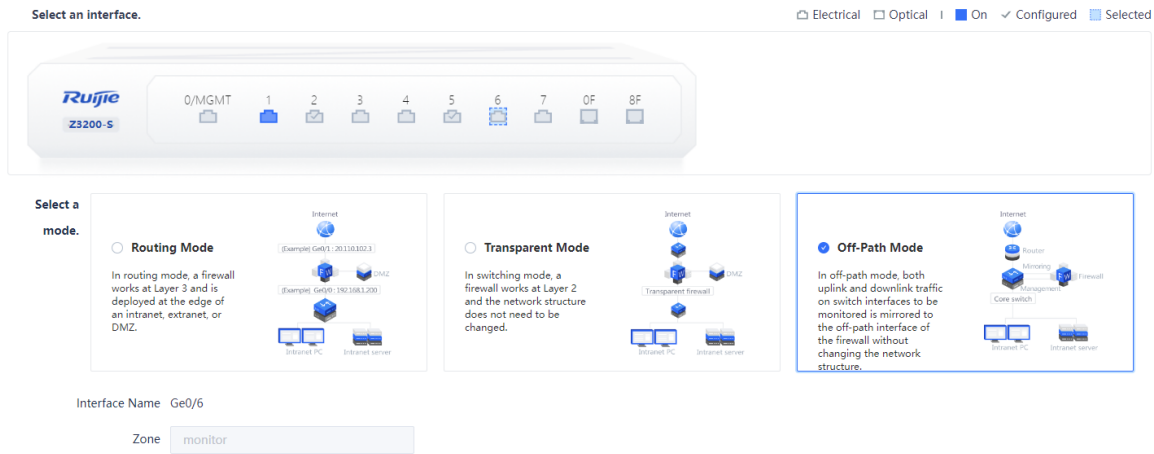


(2) Configure the management interface.

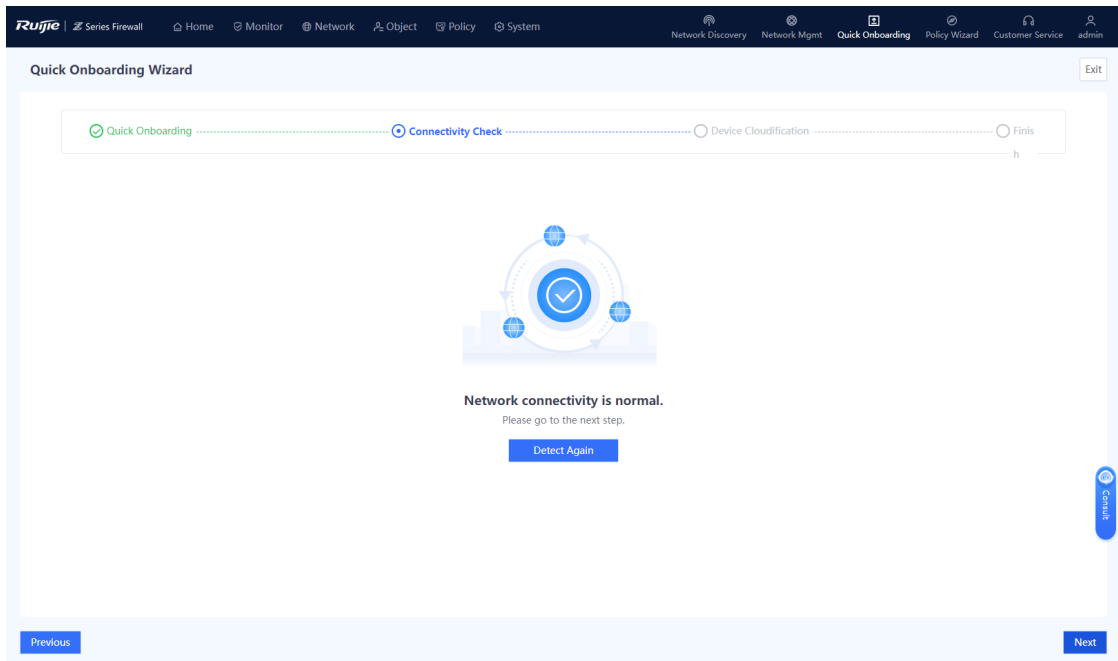


- a In the **Selecting Interface** area, click port 0/MGMT.
- b In the **Selecting Mode** area, click Routing Mode.
- c Set **Interface Type** to **WAN Interface** and configure the IP address and the next-hop address. (If the interface is connected to a switch, set the next-hop address to the management address of the switch.)

(3) Configure the off-path interface.



- a In the **Selecting Interface** area, select the interface that functions as the off-path interface for connecting to a switch.
 - b In the Selecting Mode area, click **Off-Path Mode**.
The system automatically displays the interface name. The default value of **Zone** is **monitor**.
 - c After completing the configuration, click **Next**.
- (4) The system automatically checks whether the firewall is connected to the Internet. If so, click **Next**.



Note

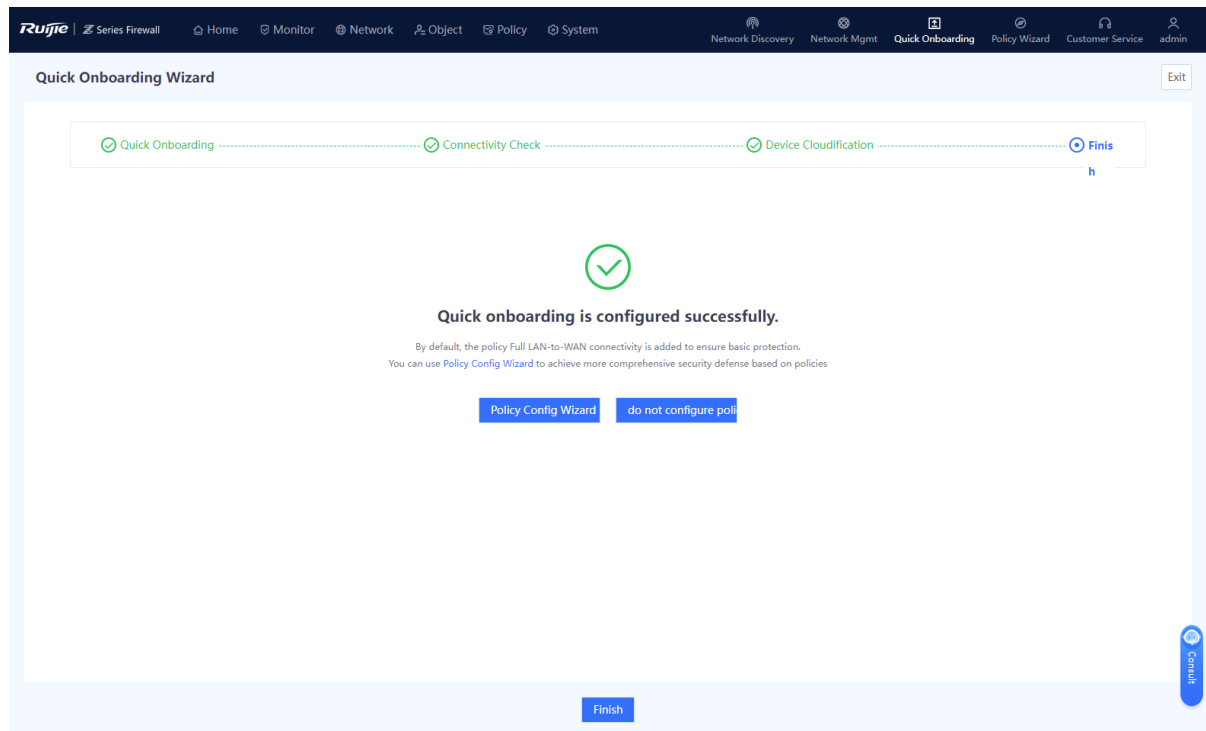
If the firewall cannot connect to the Internet, click **Previous** to modify management interface parameters, and then check again.

- (5) (Optional) If the firewall can connect to the Internet, the **Enable Ruijie Cloud-based Management** page is displayed. Enable the cloud management platform function and bind the device as prompted.

Note

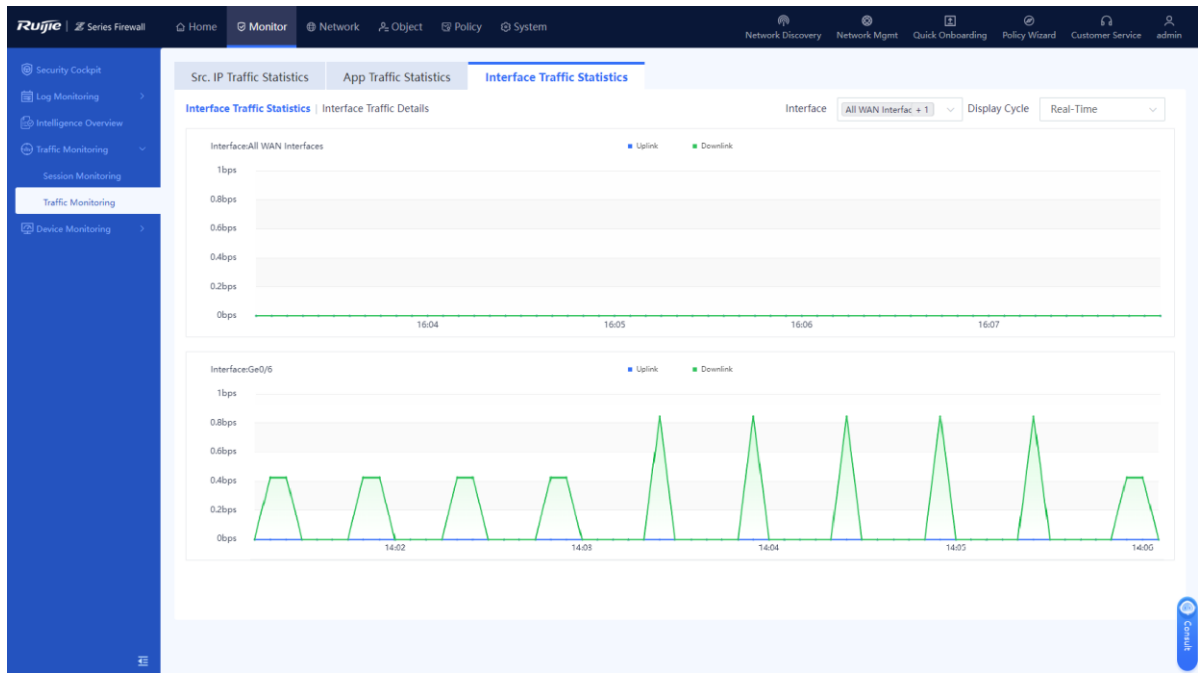
If the device cannot connect to the Internet, connect it to the cloud management platform according to 10 Ruijie Cloud Connection.

- (6) After completing the configuration, click **Next**. Click **Finish** to complete quick onboarding configuration.



Verification

Configure the switch to mirror traffic to be monitored to the off-path interface on the firewall. Then, log in to the firewall through the management interface, choose **Monitor > Traffic Monitoring > Traffic Monitoring > Interface Traffic Statistics**, and check traffic on the off-path interface.

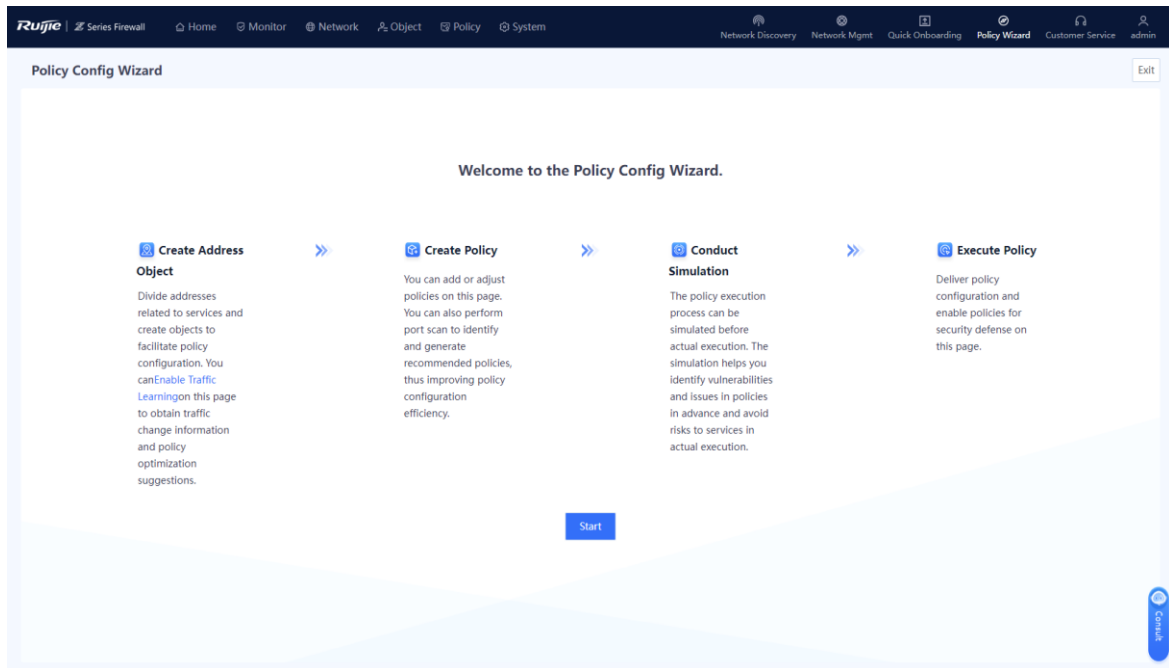


3.2.2 Configuring Security Policies Using the Wizard

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 the icon and panel area, click **Policy Wizard**.
- (2) Click **Start** to enter the **Policy Config Wizard** page. Perform the operations according to the wizard.



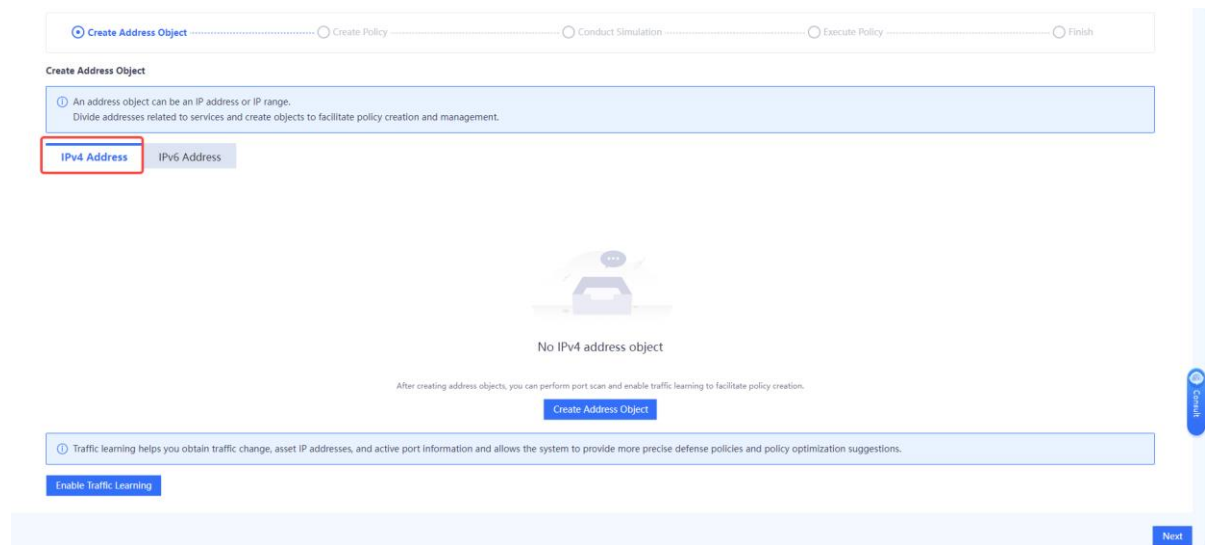
1. Creating Address Objects

Application Scenario

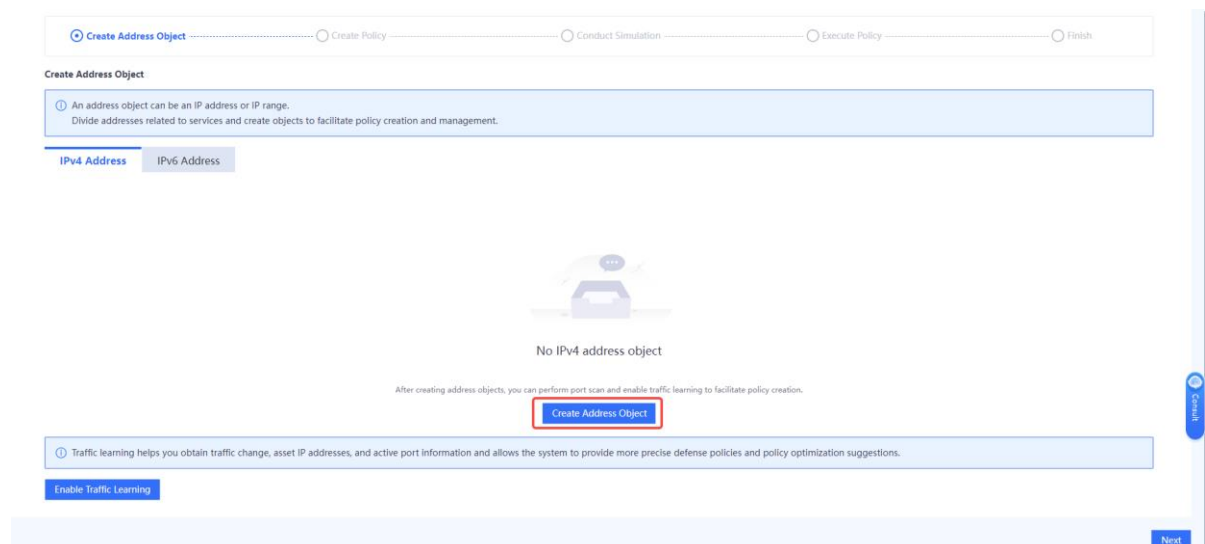
By using the address object, you can classify service-related IP addresses (including intranet or extranet IP addresses), facilitating management of traffic within the specified IP address range.

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) On the **Add IPv4 Address Object** or **Add IPv6 Address Object** page, enter the object names and IP addresses/ranges.

Add IPv4 Address Object



* Address Object Name * IP Address/Range

Create

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"> ● IP address: One or multiple IP addresses. Input an IP address per line. Press Enter to separate lines. <ul style="list-style-type: none"> ○ Example 1: 192.168.20.3 ○ Example 2: 1234::100 ● IP range: A contiguous range of addresses. Connect the start IP address and end IP address with a hyphen (-). <ul style="list-style-type: none"> ○ Example 1: 192.168.20.1-192.168.20.3 ○ Example 2: 1234::100-2345::100 ● Subnet: IP range. <ul style="list-style-type: none"> ○ Example 1: 192.168.1.0/24 or 192.168.1.0/255.255.255.0 ○ Example 2: 1234::100/100

Note

To add multiple address objects, click **Create**.

(4) Click **Confirm Creation**.

(5) Select address objects, and click **Next**.

Follow-up Procedure

- You can choose **Object > Address** to view, add, edit, and delete address objects.
- You can only delete the address with no reference.

2. Configuring Security Policies

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 extranet. A security policy is configured to establish a designated channel between the intranet and extranet to filter sensitive data access.

Prerequisites

The security zone, service, service group, application group, time plan, intrusion protection policy, and virus protection policy have been created according to service requirements.

- For details on how to create a security zone, see [7.2 Security Zone](#).
- For details on how to create a service, see [6.4.2 Configuring a Custom Service](#).
- For details on how to create a service group, see [6.4.3 Creating a Service Group](#).
- For details on how to create an application zone, see [6.2 Application](#).
- For details on how to create a time plan, see [6.5 Time Plan](#).
- For details on how to create an intrusion protection policy, see [6.9.2 Intrusion Prevention](#).
- For details on how to create a virus protection policy, see [6.9.1 Virus Protection](#).

Procedure

- (1) On the **Create Policy** page, click **Create**.

The screenshot shows the 'Policy Config Wizard' interface. At the top, there is a progress bar with five steps: 'Create Address Object', 'Create Policy' (selected), 'Conduct Simulation', 'Execute Policy', and 'Finish'. Below the progress bar, the 'Create Policy' section contains a blue box with instructions: 'You can manually create policies or perform port scan to guide policy creation. Next, you can choose to conduct simulation before executing policies or directly execute policies.' There are two buttons: 'View Simulation Result' and 'Scan Port - Create Policy'. Below this, there is a 'Policy Group' section with a list of actions: 'Create', 'Delete', 'Enable', 'Disable', 'Refresh', and 'More'. A 'Type' dropdown menu is set to 'All', and there is a search box 'Enter a keyword.'. A table of policy groups is displayed below, with columns: Priority, Name, Type, Src. Security Zone, Src. Address, Dest. Security Zone, Dest. Address, Service, App, Time Range, and Operation. The table shows two rows under the 'Default Policy Group'.

Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time Range	Operation
1	allow_all	-	any	any	any	any	any	any	any	<input checked="" type="checkbox"/> Edit Delete
2	Default Po..	-	any	any	any	any	any	any	any	Edit Delete

- (2) Set parameters related to the security policy.
 - a Configure basic information about the 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 initiating the target data connection.	Click the drop-down list, and select a source address in the To-be-selected area. The selected address is automatically added to the Selected area. [Example] any

Item	Description	Remarks
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.	Click the drop-down list, and select a destination address in the To-be-selected area. The selected address is automatically added to the Selected area. [Example] any

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 to permit or deny the target data connection.

Action Settings

Action Option Permit Deny

Action Option	Description
Permit	<p>If the action is set to Permit, 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.

Content Security

Intrusion Prevention Enable Disable [⊕ Add Intrusion Prevention Template](#)

Virus Protection Enable Disable [⊕ Add Virus Protection Template](#)

URL Filtering Enable Disable [⊕ Add URL Filtering](#)

Advanced
Settings

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. ▼

Cancel
Confirm

h Click **Save**.

3. Conducting Simulation Run

Application Scenario

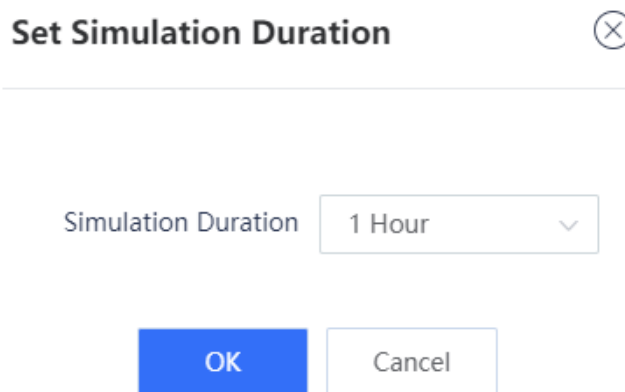
After you create a security policy, you can conduct simulation run to discover vulnerabilities or problems of the policy in advance to avoid risks to services in actual implementation.

Procedure

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

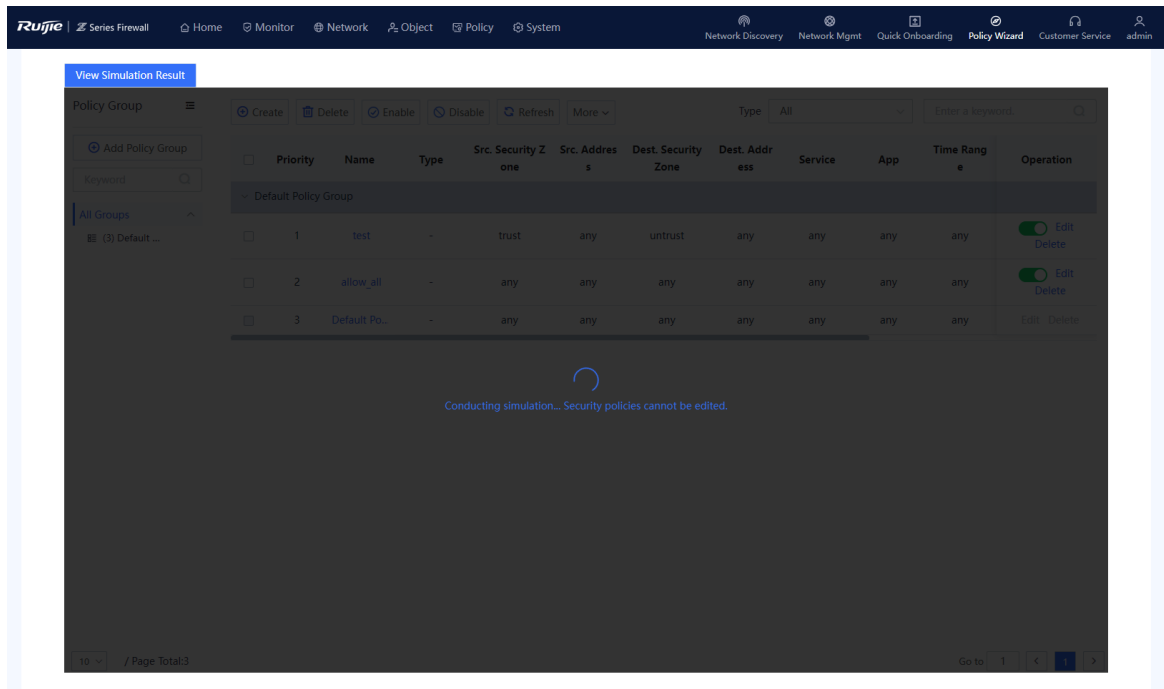


- (2) In the **Set Simulation Duration** dialog box, set the duration of simulation run.



- (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:

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

(5) Analyze whether the simulation results differ from actual execution results.

Simulation Results That Differ from Actual Execution Results

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

Refresh Clear Result

Src. Address	Actual Execution Result	Simulation Result	Hit Count in Actual Execution	Hit Count in Simulation	Details
--------------	-------------------------	-------------------	-------------------------------	-------------------------	---------



The actual execution result is the same as the simulation result.

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.

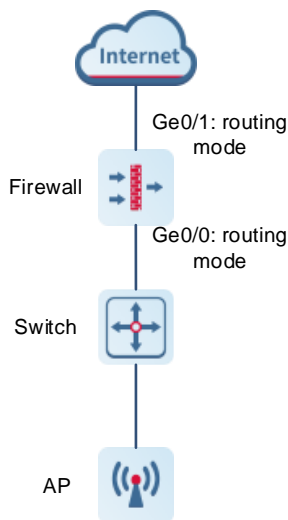
4 Integrated Deployment on Ruijie Cloud

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.

4.1 Firewall Deployment (Routing Mode)

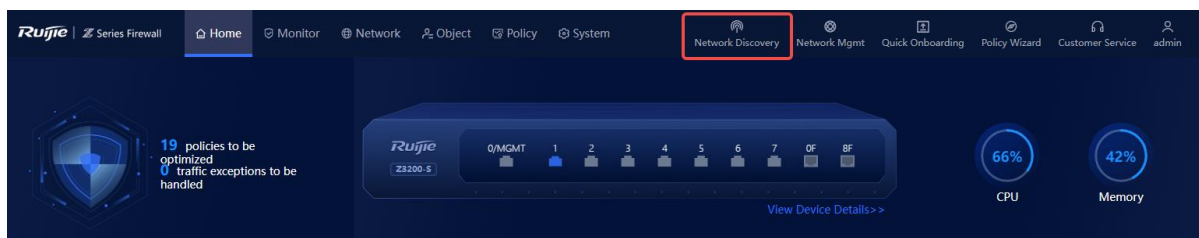
1. Application Scenario

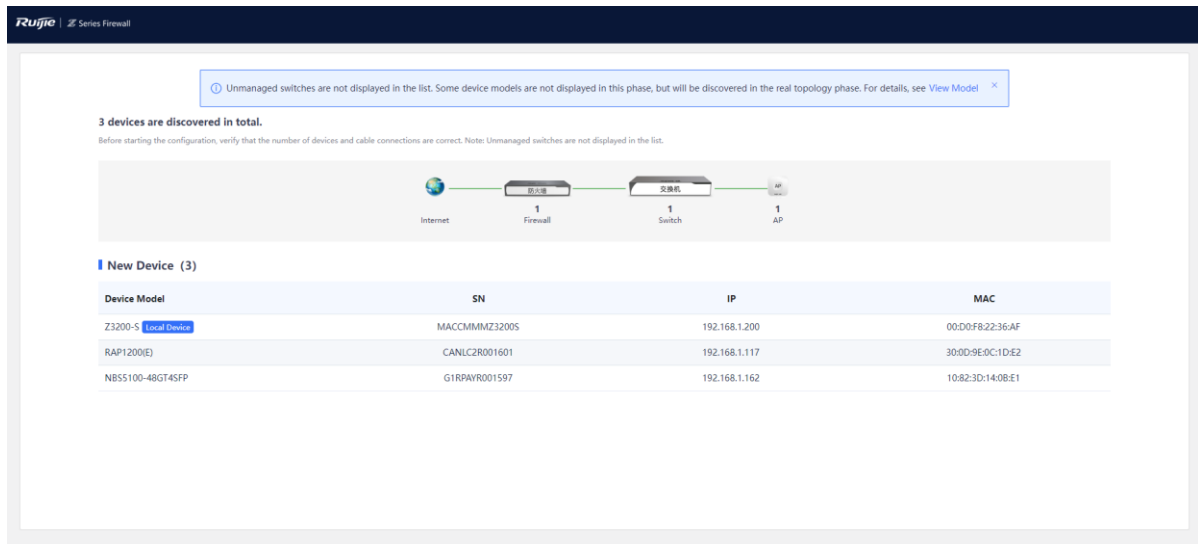
The firewall functions as an egress gateway and it is uplinked to the Internet and downlinked to a switch. You are advised to deploy the firewall in routing mode. The uplink interface is configured to work in routing mode to access the Internet and the downlink interface is configured to work in routing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



2. Procedure

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

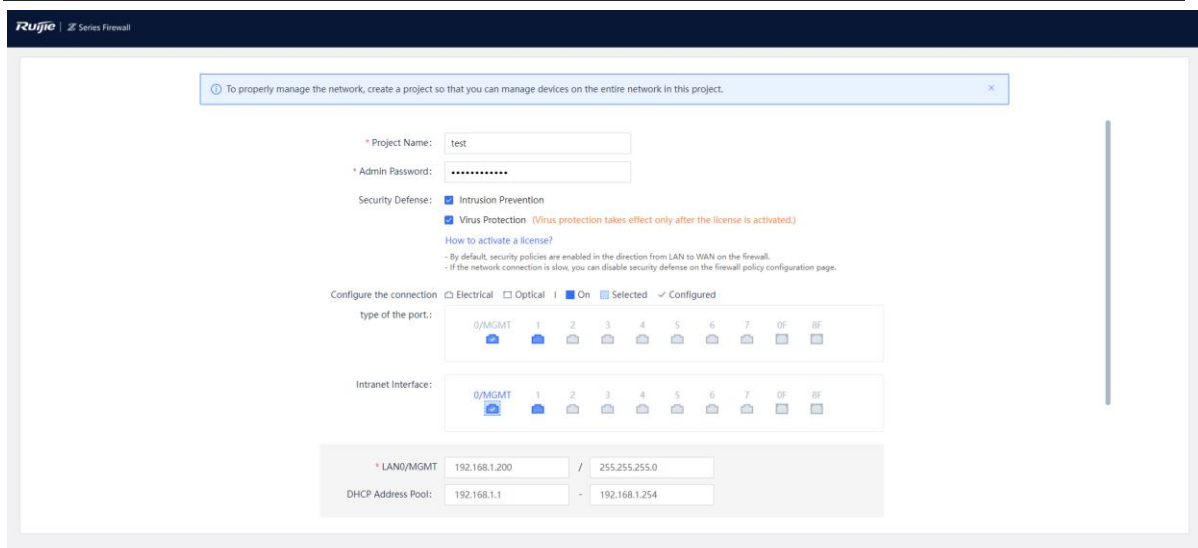


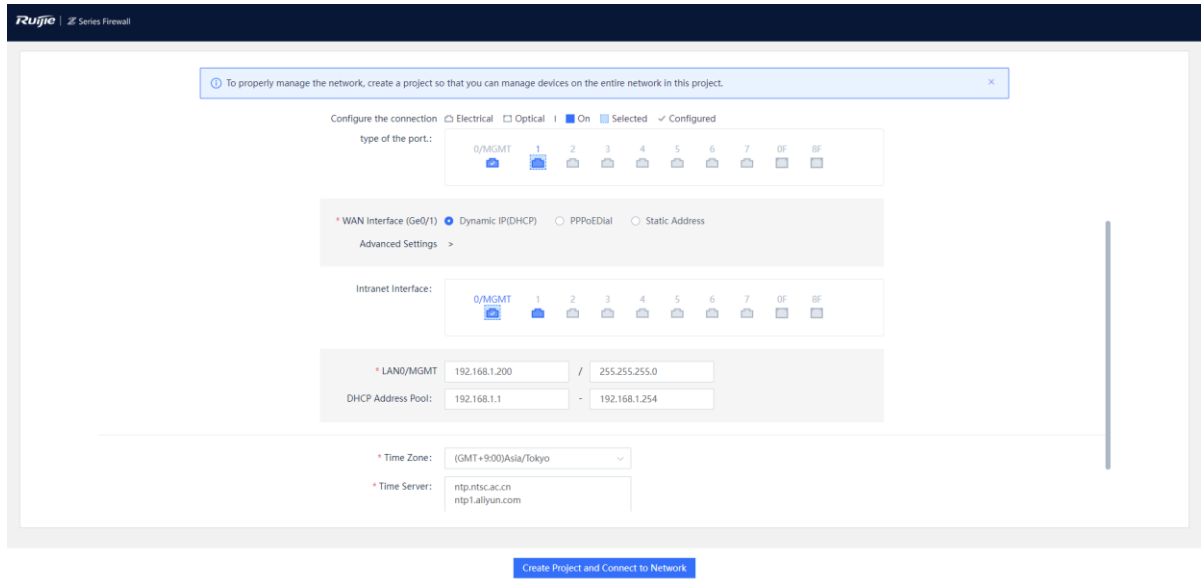


(2) Click **Start**. Enter the network project name and configure a port IP address as prompted.

i Note

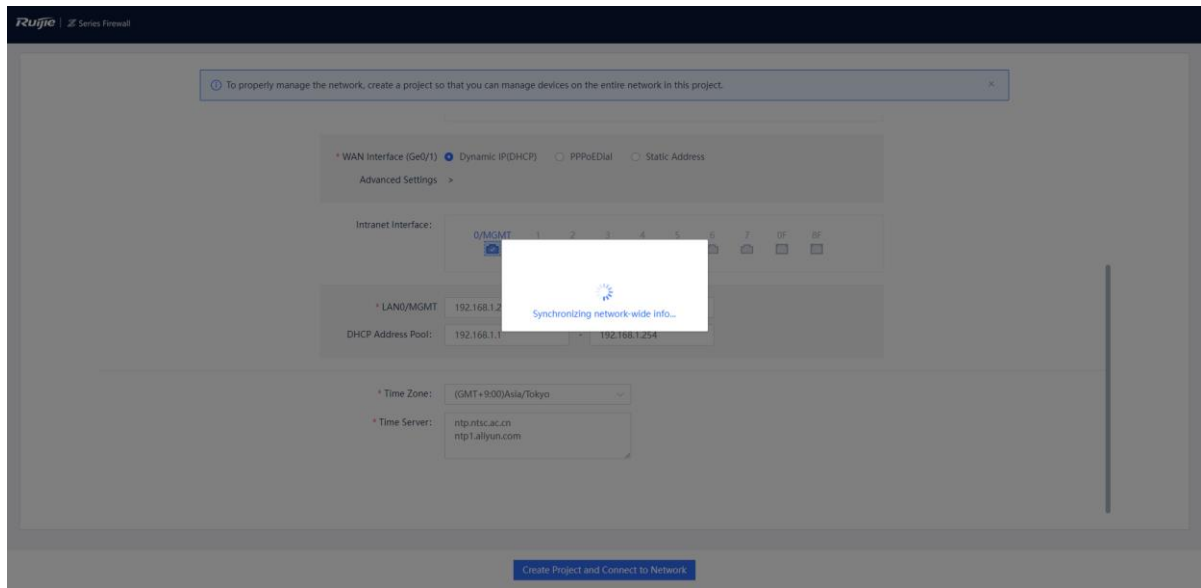
- The DHCP server function is enabled on the firewall by default, and the default DHCP address pool is configured on the management port.
- Intrusion prevention and virus protection are enabled on the firewall by default. You can choose to disable these functions based on actual needs. The virus protection 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.





Item	Description	Remarks
WAN Interface	<p>Connects the firewall to the Internet. Generally, the WAN interface is directly connected to the FTTH 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"> ● Dynamic IP (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. ● PPPoE: Applicable for dialup access to the ISP network. The username and password of the dialup user must be configured. ● Static Address: Applicable when the network administrator specifies an IP address for the device based on the predefined IP address planning. This connection type requires the network administrator to possess certain network knowledge. The IP address/mask and next-hop address must be configured. 	<p>[Example]</p> <p>Ge0/1</p> <p>Dynamic IP (DHCP)</p>
LAN Interface	<p>Connects to the LAN. The LAN interface IP address must be configured based on the predefined IP address planning.</p>	<p>[Example]</p> <p>192.168.1.1/24</p>

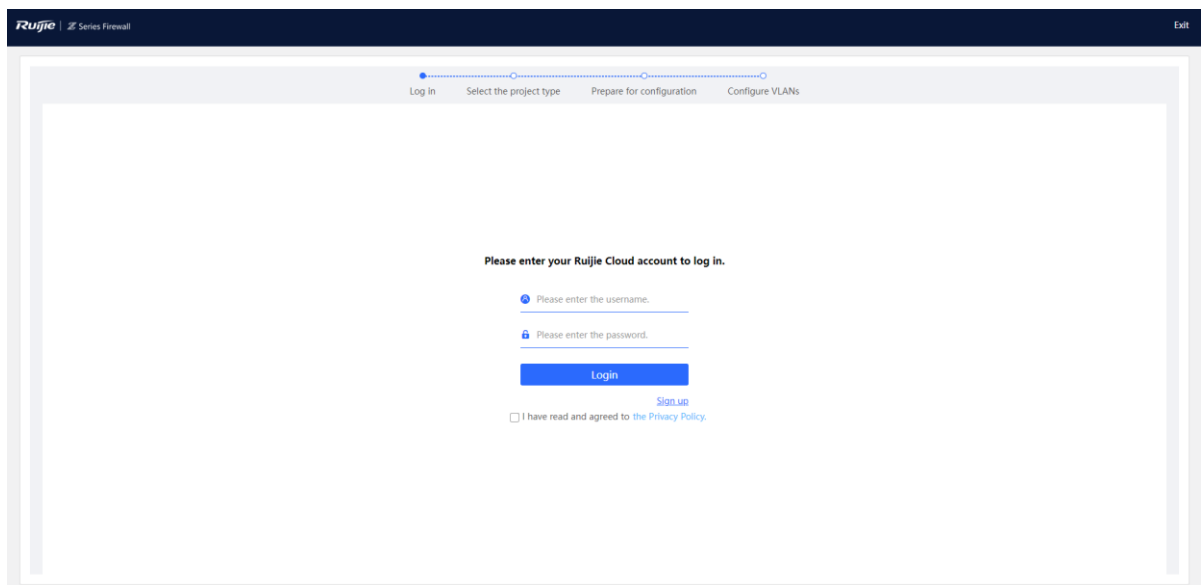
(3) Click **Create Project and Connect to Network**. The system delivers configuration information.



- (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.

i Note

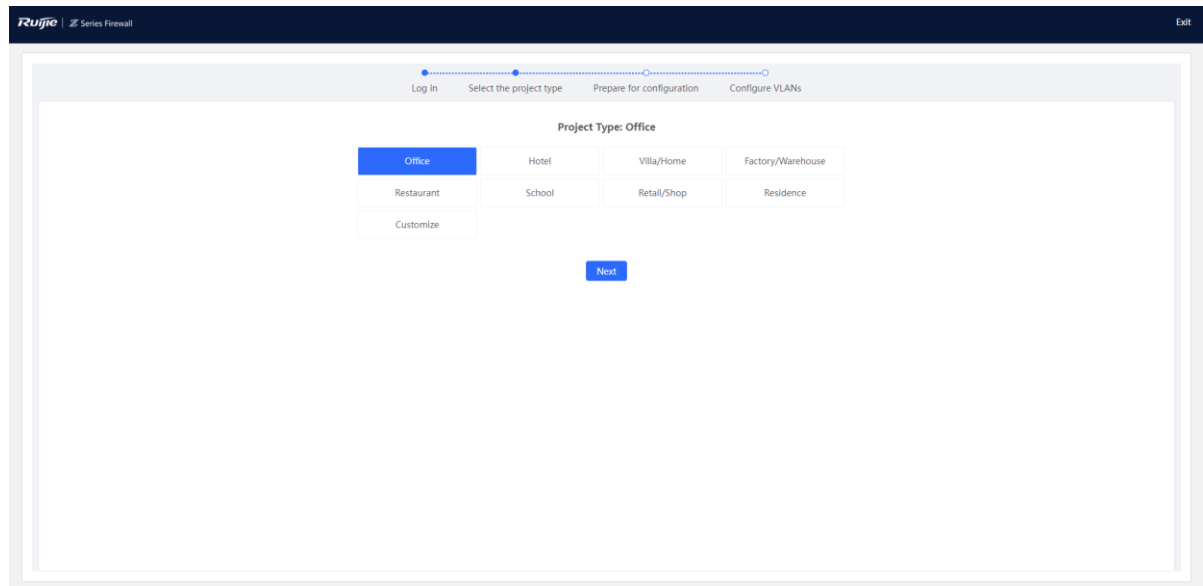
After successful configuration, the firewall automatically adds the IP address of the DHCP server in the networking to the allowlist and generates a security policy (with the name **trust-untrust** and enabled with intrusion prevention).



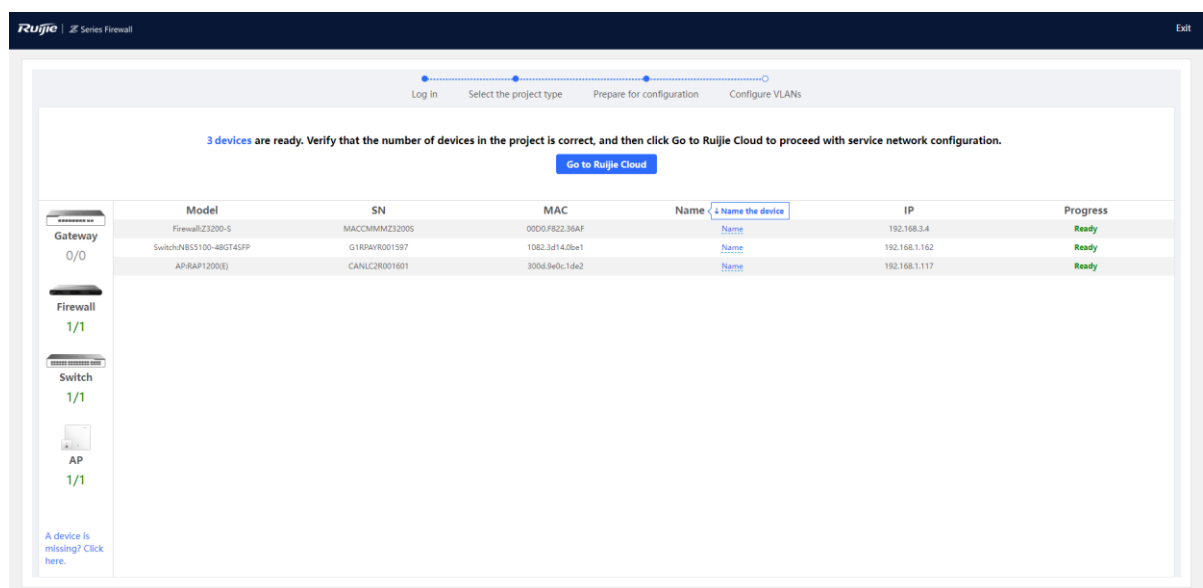
i Note

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.

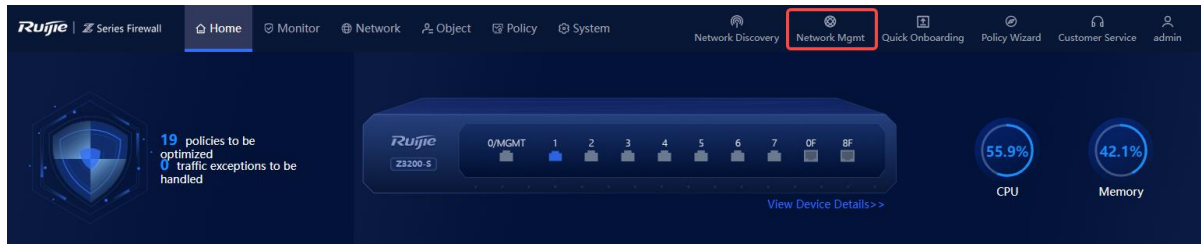
- (5) After successful login, select a project type based on the actual networking scenario and click **Next**. The initial configuration delivered varies by the project type, so the project type must be set based on the actual service scenario.



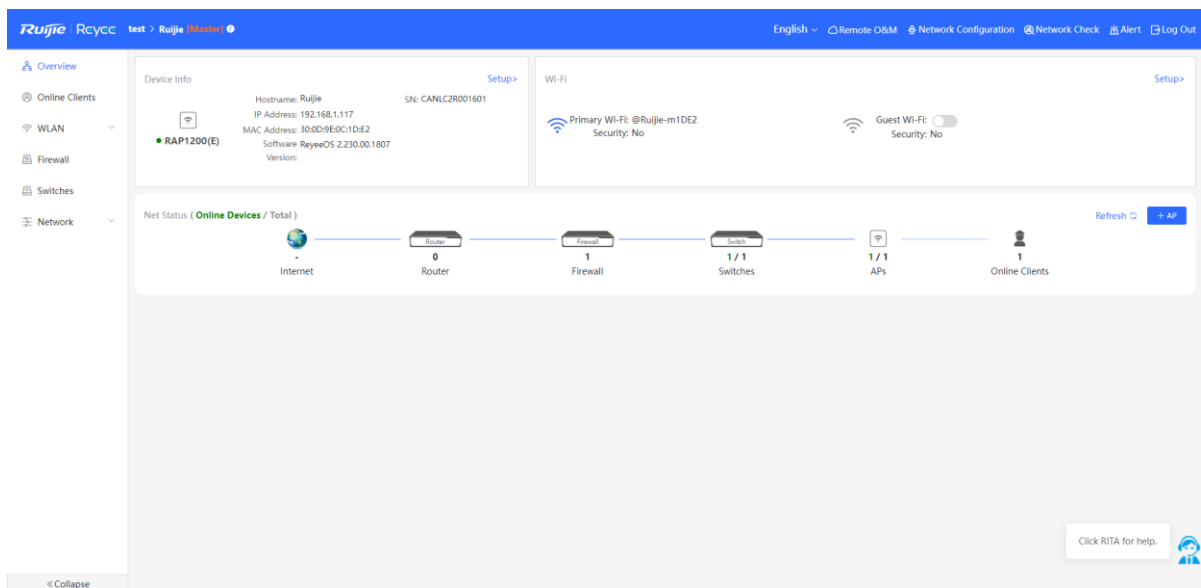
- (6) Wait until preparations before configuration are complete and then configure the service network.
- (7) After all devices go online, click **Go to the Cloud Platform** and perform service configuration on the Ruijie Cloud platform.



- (8) (Optional) After service configuration is complete, click **Network Mgmt** on the firewall to switch to the web UI 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.



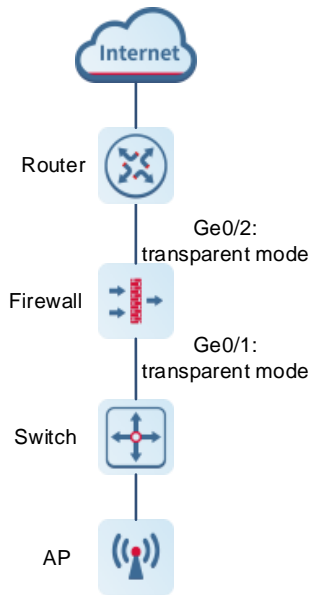
The following figure shows the **Overview** page of the master device.



4.2 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**.

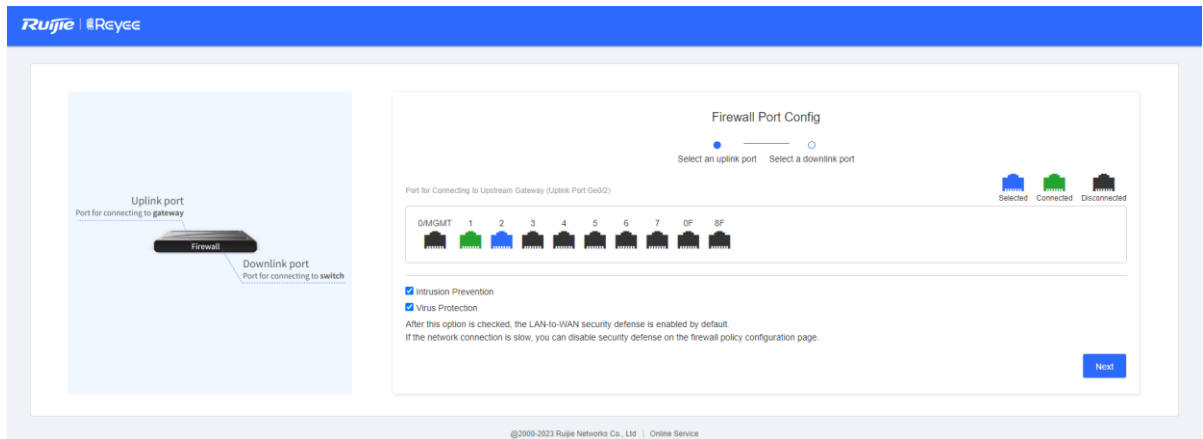
- (2) Log in to the web page of the NBR. The following page is displayed by default. Click **Start**.

The screenshot shows the Ruijie Cloud management interface. At the top, there is a notification: "5 devices are detected. 1 devices should be added manually." Below this, there is a network topology diagram showing the connection between Internet, Gateway, Firewall, Switch, AP, and Add Manually. Below the topology, there is a table titled "My Network(4)" with columns for Model, SN, IP, and MAC. The table contains the following data:

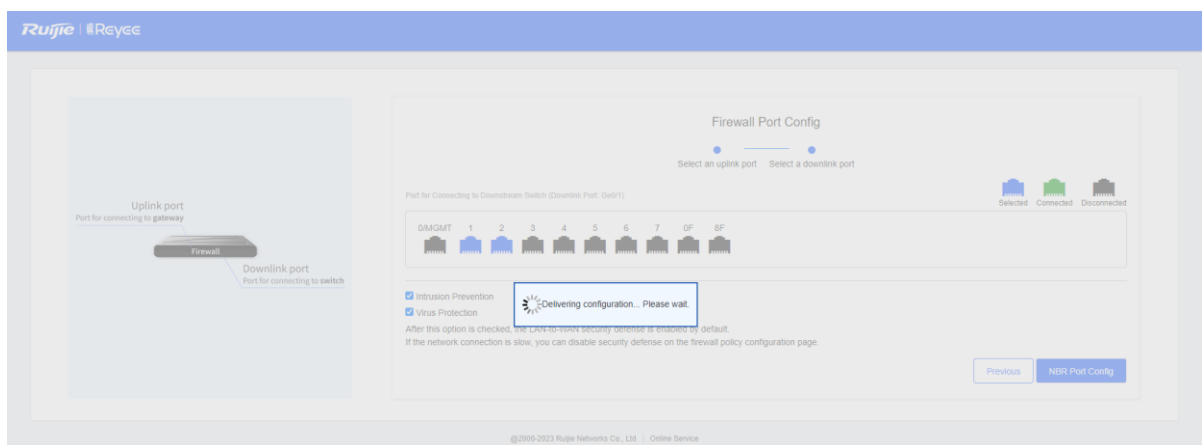
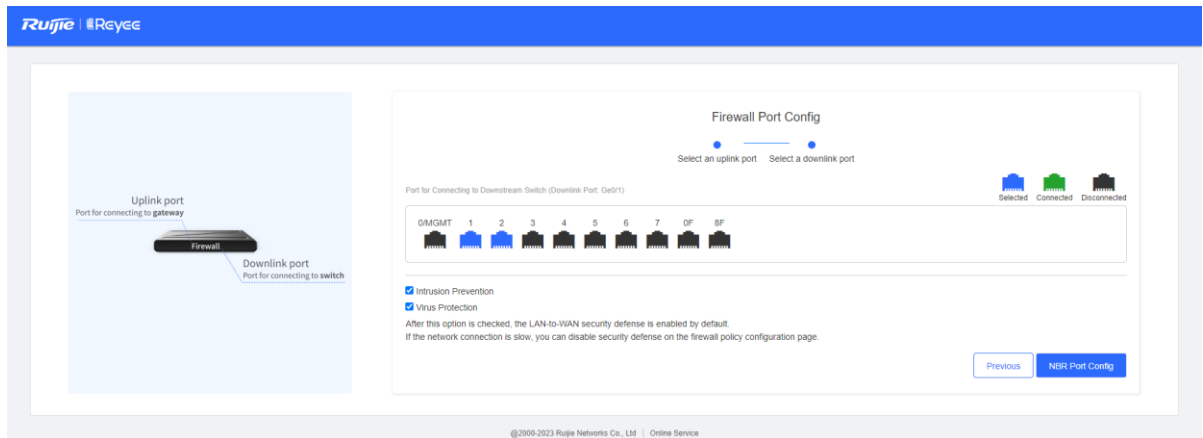
Model	SN	IP	MAC
NBR6210-E	MACCHJG621001	192.168.1.1	00:D1:F8:22:93:59
Z3200-S	MACCHJQZ32831	192.168.1.5	00:d0:f8:22:36:ce
RAP2261(G)	G1RU708000836	192.168.1.2	28:D0:F5:F5:98:0E
NBS3200-48GT4XS-P	G1QH1AD000557	192.168.1.3	C0:B8:E6:B5:A8:C2

Below the table, there is a "Show No." dropdown set to 10, a "Total Count: 4" label, and navigation buttons: "First", "Pre", "Next", "Last", and "GO". At the bottom, there are "Detect again" and "Start Config" buttons.

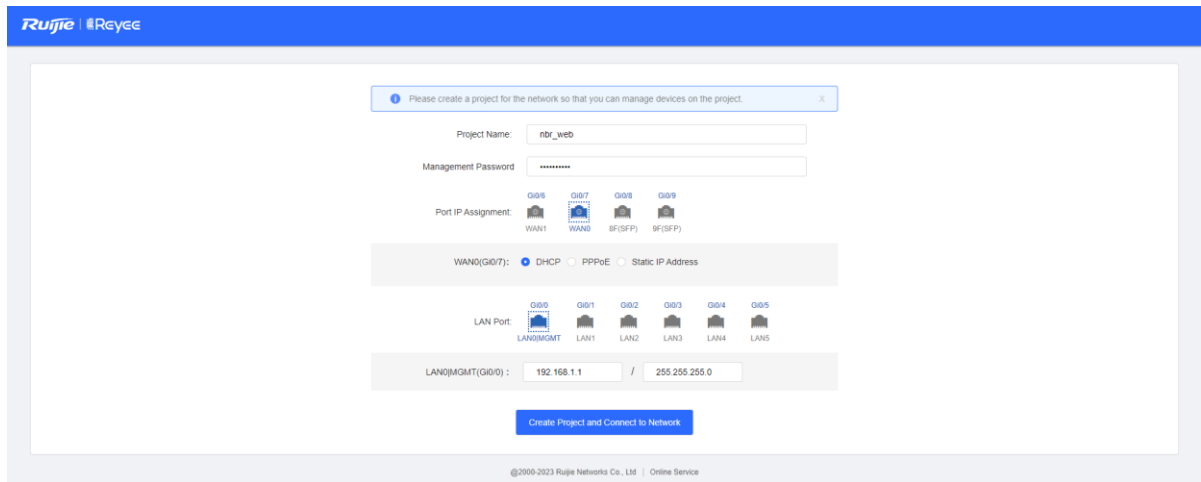
- (3) Select the WAN interface (interface connected to the gateway, Ge0/2 in this example) of the firewall based on the actual networking and click **Next**.



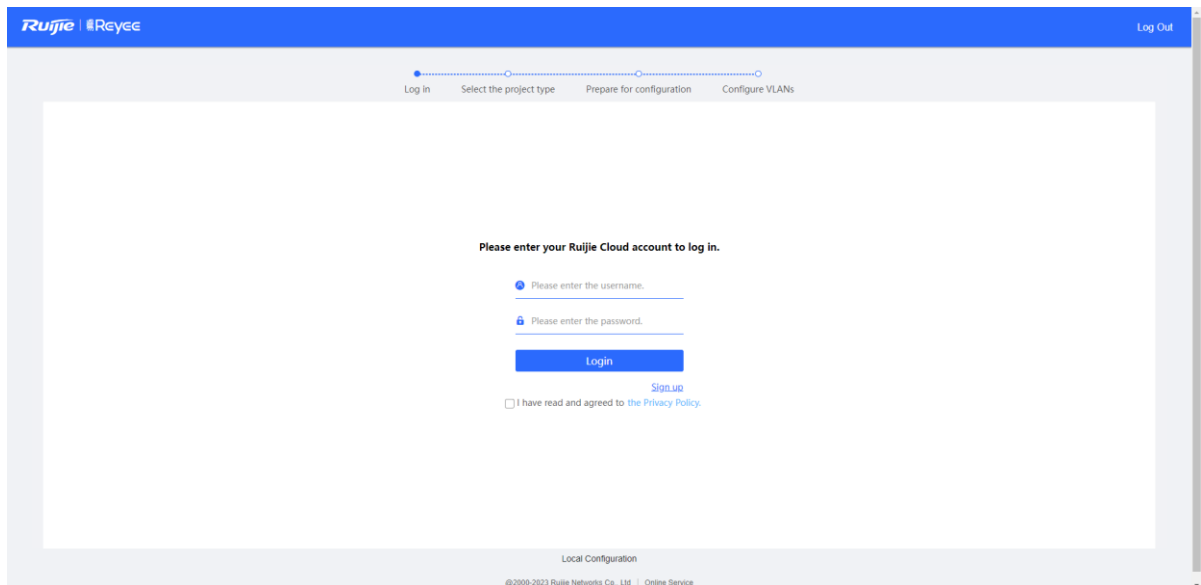
(4) Select the LAN interface (interface connected to the switch, Ge0/1 in this example) of the firewall based on the actual networking and click **NBR Port Config**.



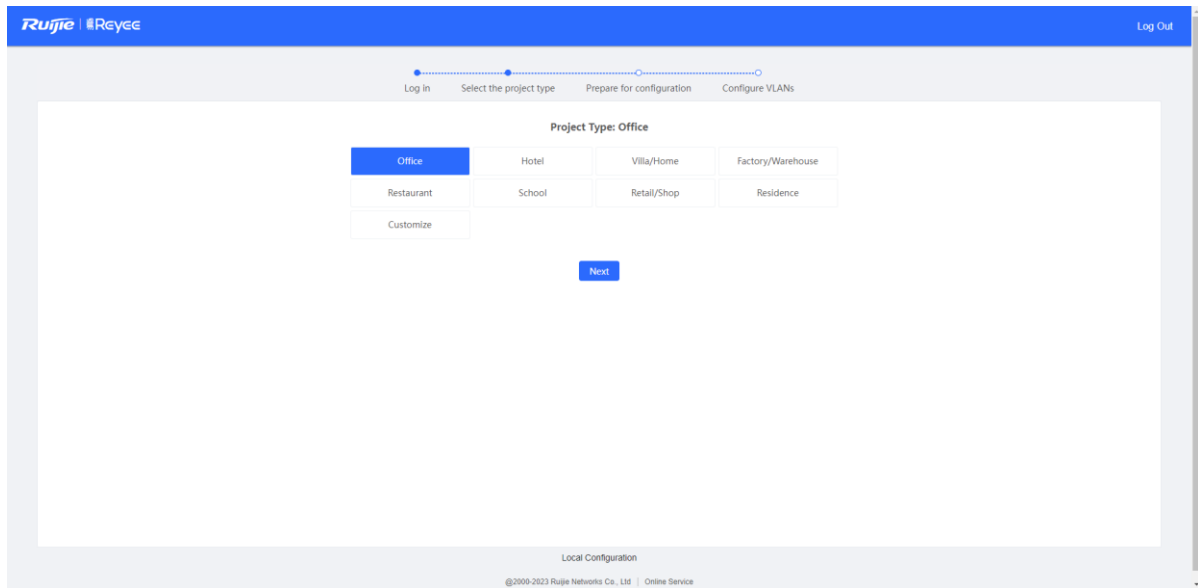
(5) After successful configuration delivery, the following page is displayed. On this page, enter the project name and management password and click **Create Project and Connect to Network**.



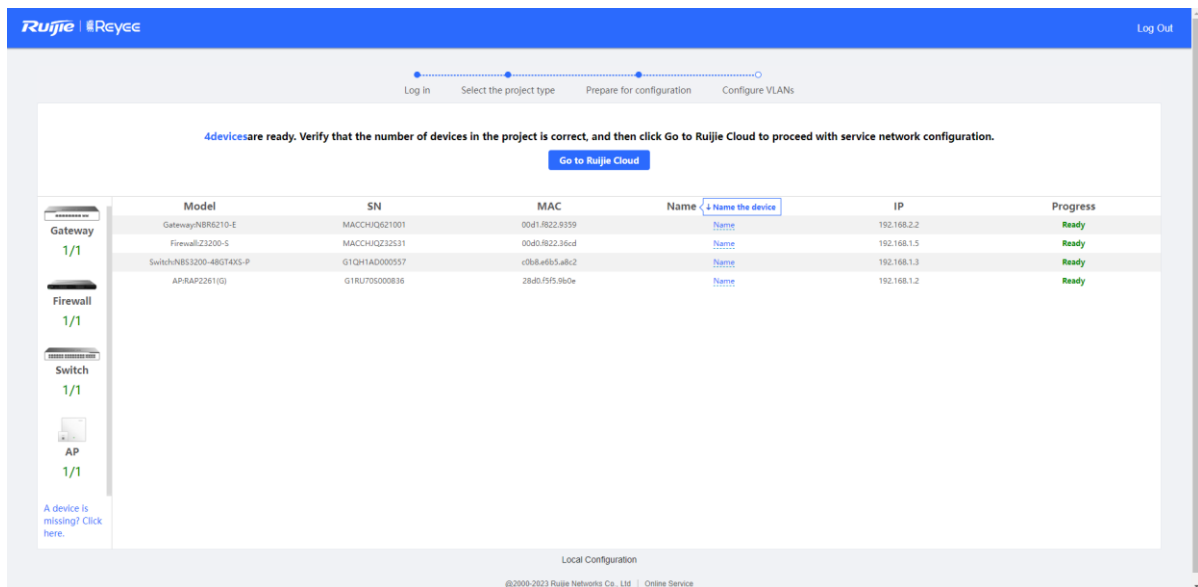
- (6) Check the system prompt. A prompt indicating successful configuration is displayed after the configurations are completed. You can scan the username and password to log in to Ruijie Cloud and migrate the firewall to the cloud.

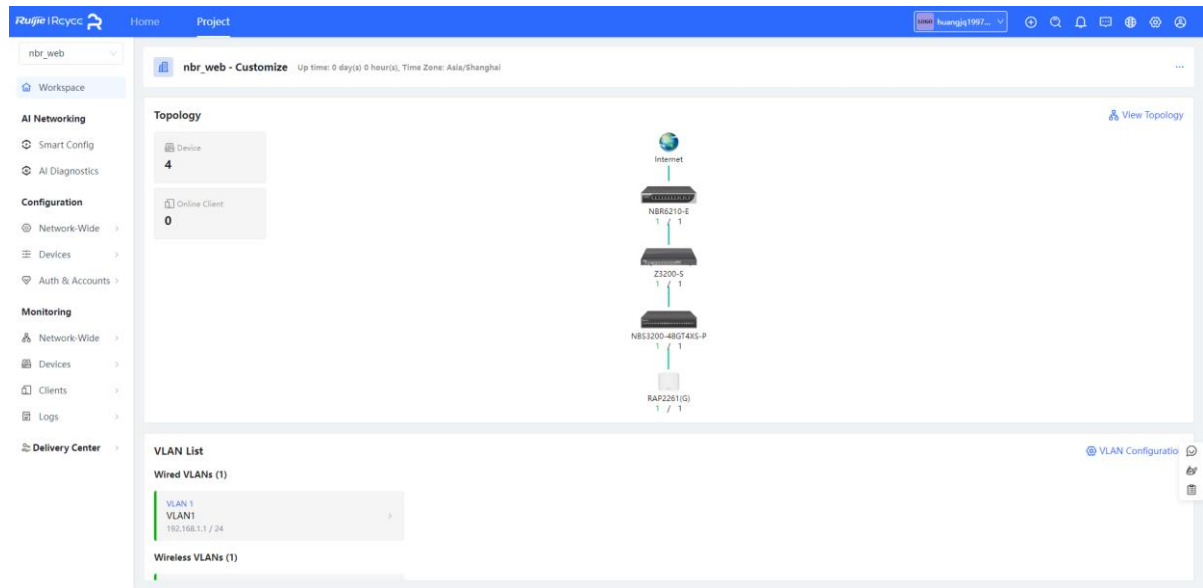


- (7) After successful login, select a project type based on the actual networking scenario (**Other** in this example) and click **Next**. The initial configuration delivered varies by the project type, so the project type must be set based on the actual service scenario.



- (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** and perform service configuration such as ports and routes on the Ruijie Cloud platform.

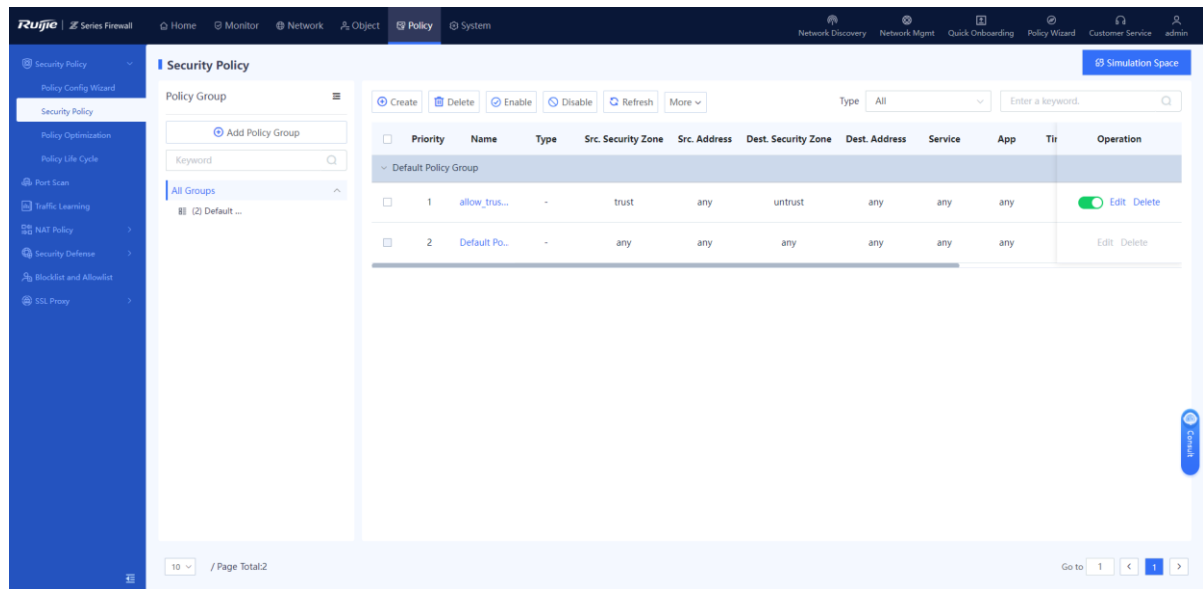




Note

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.



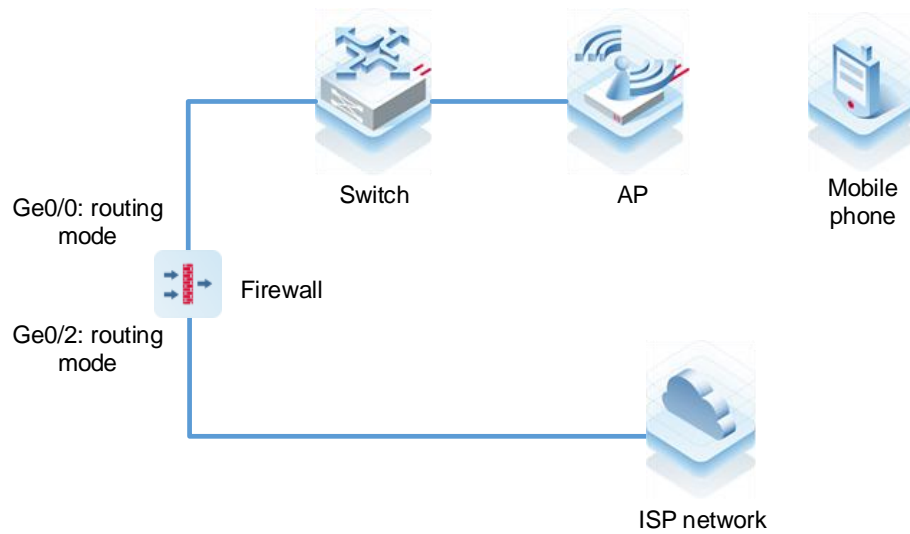
4.3 Deployment Using Ruijie Cloud App (Routing Mode)

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.

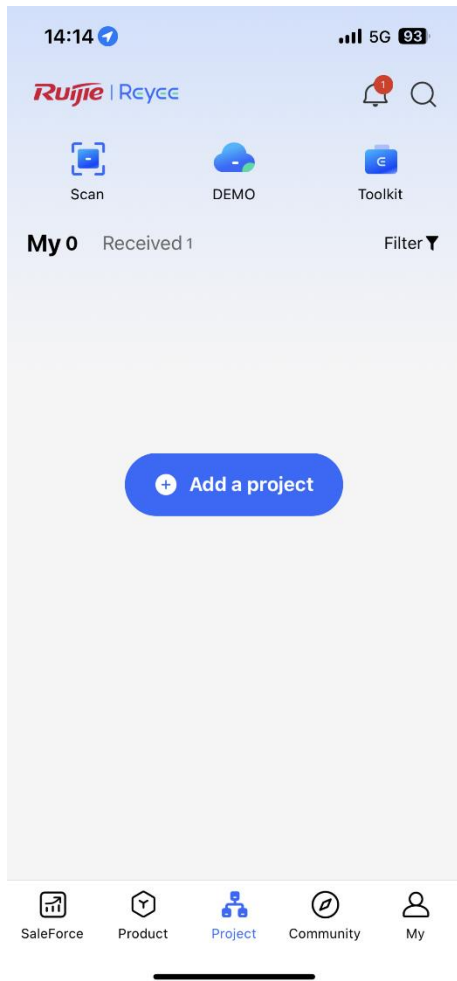
i Note

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

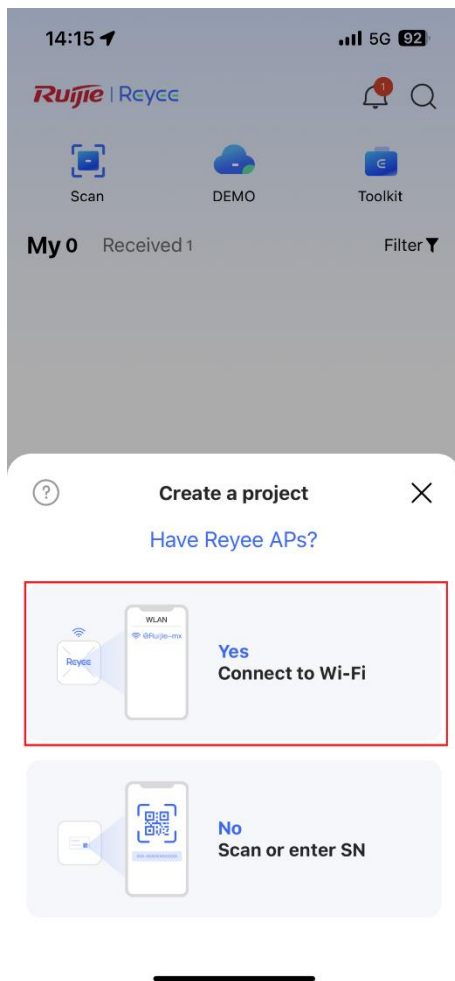


2. Procedure

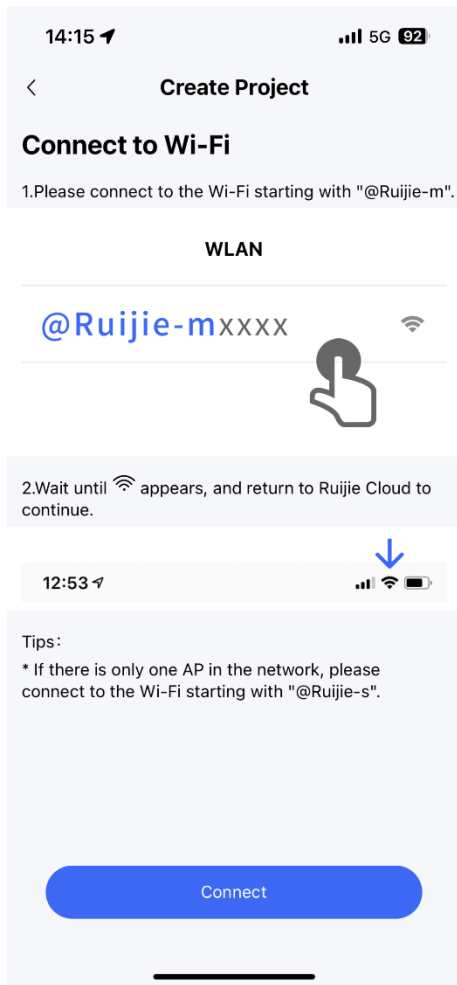
- (1) After the network environment is established according to the preceding figure, start the Ruijie Cloud app and choose **Project > Add a project**.



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

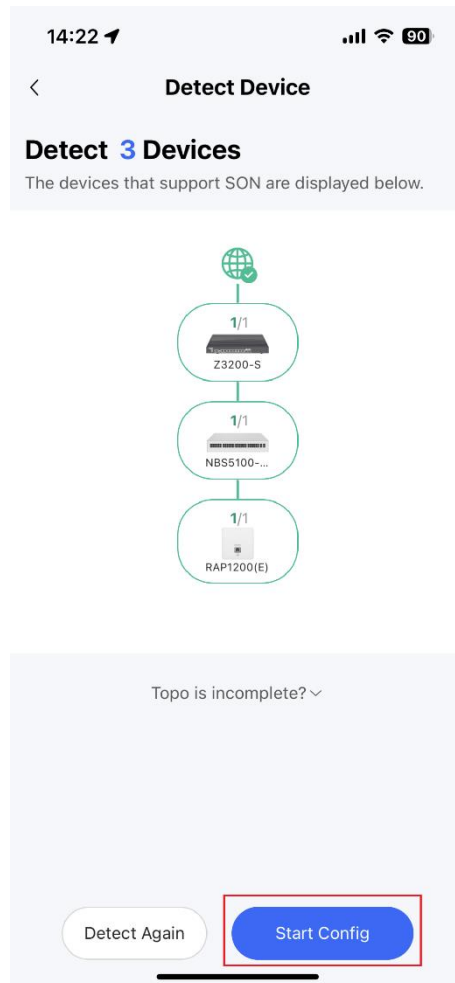
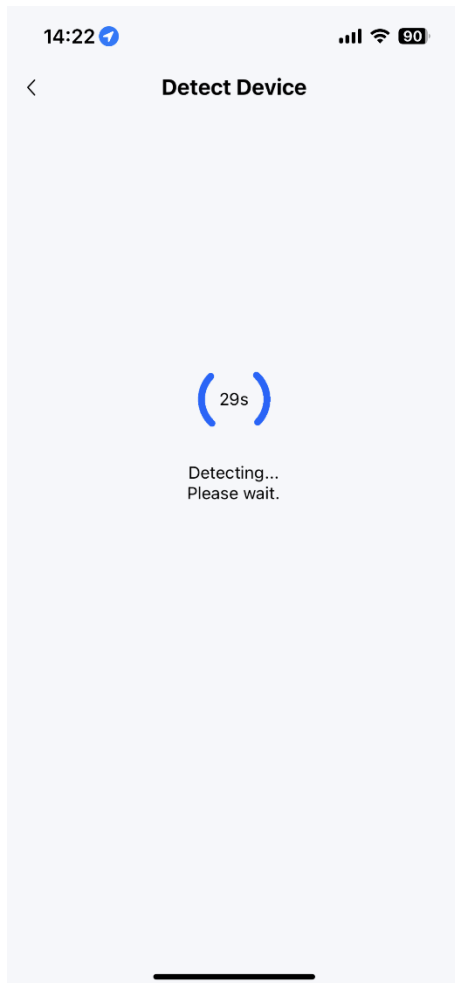


(3) Tap **Connect** to connect to the Wi-Fi signal of the Reycce AP.

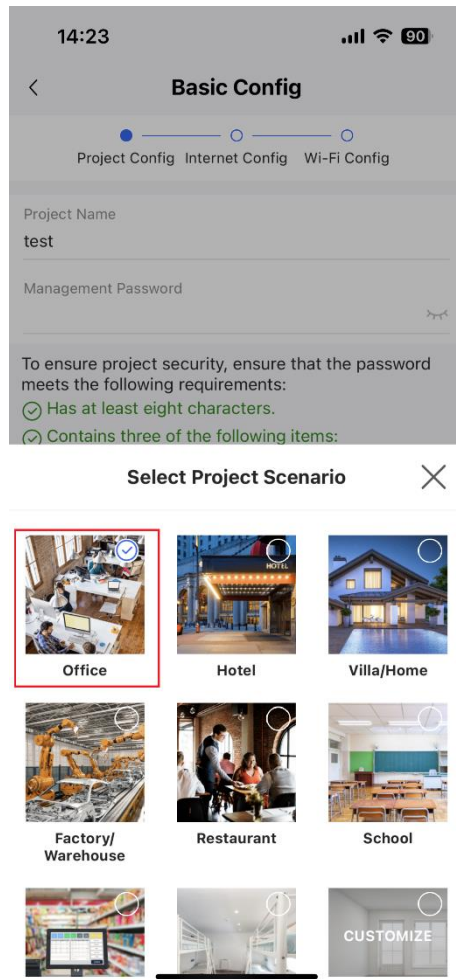
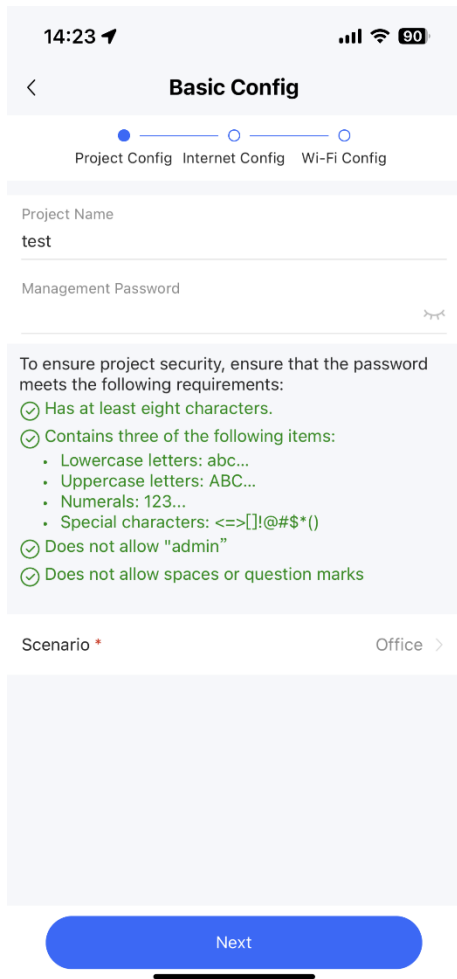




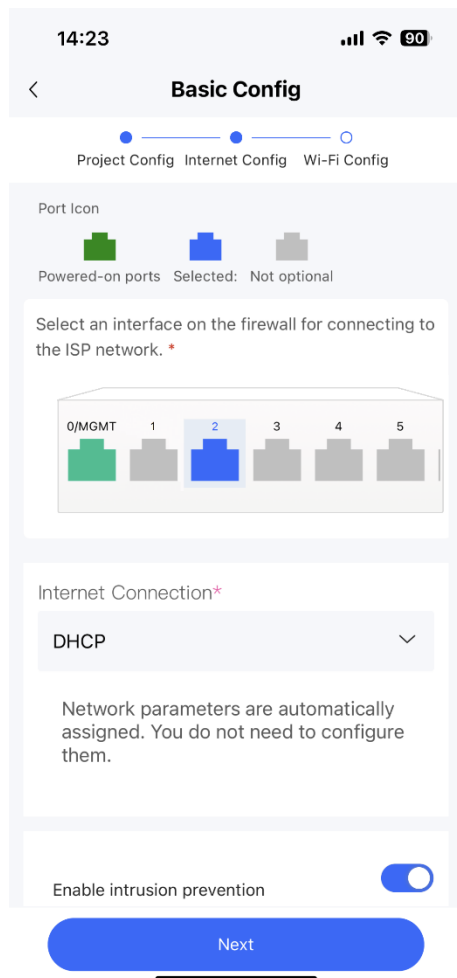
(4) Wait for about 30s until the system automatically generates the network topology. Then, tap **Start Config**.



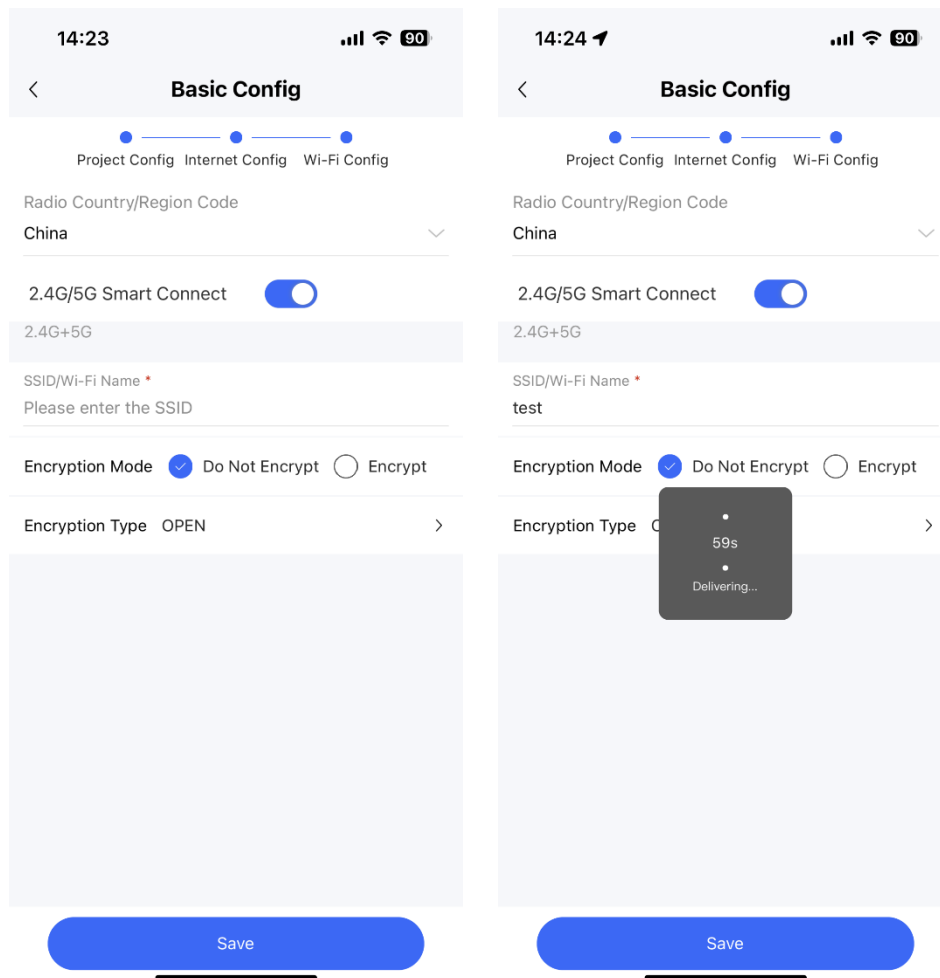
(5) Enter the project name and password and tap **Next**.



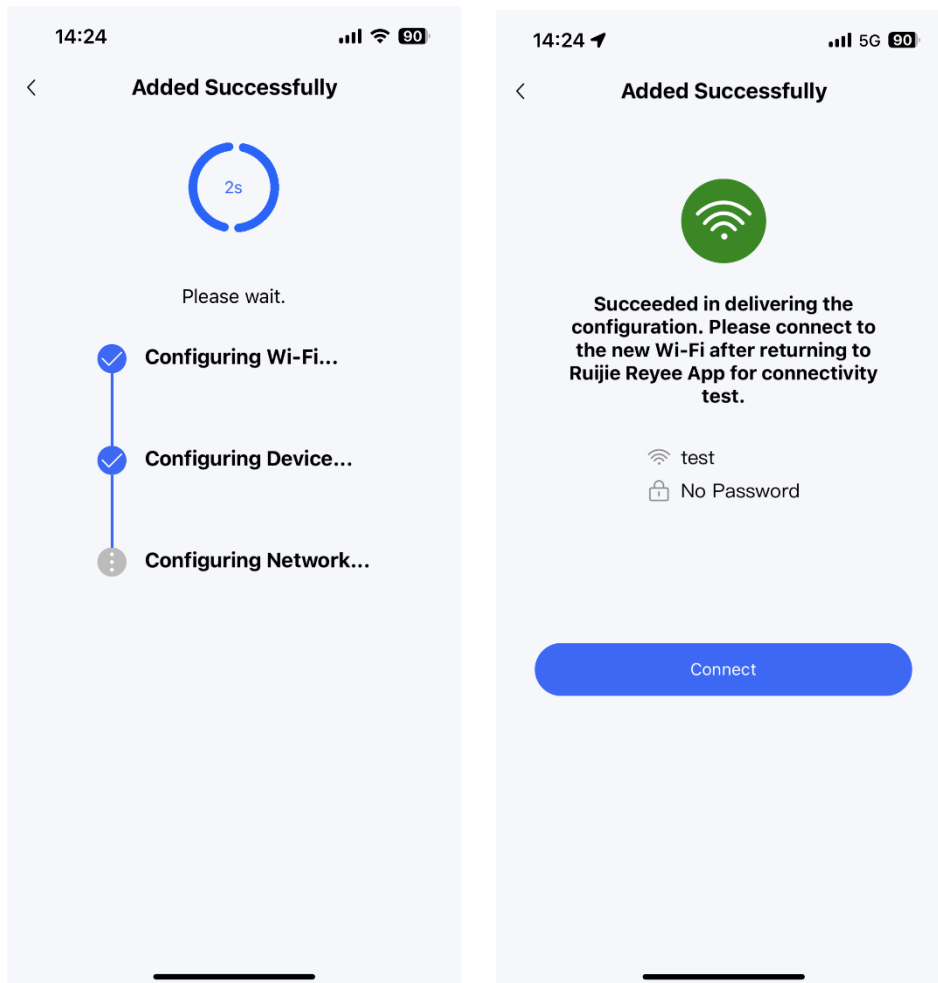
(6) Select the firewall interface (WAN interface) connected to the Internet, set an Internet access method, and tap **Next**.



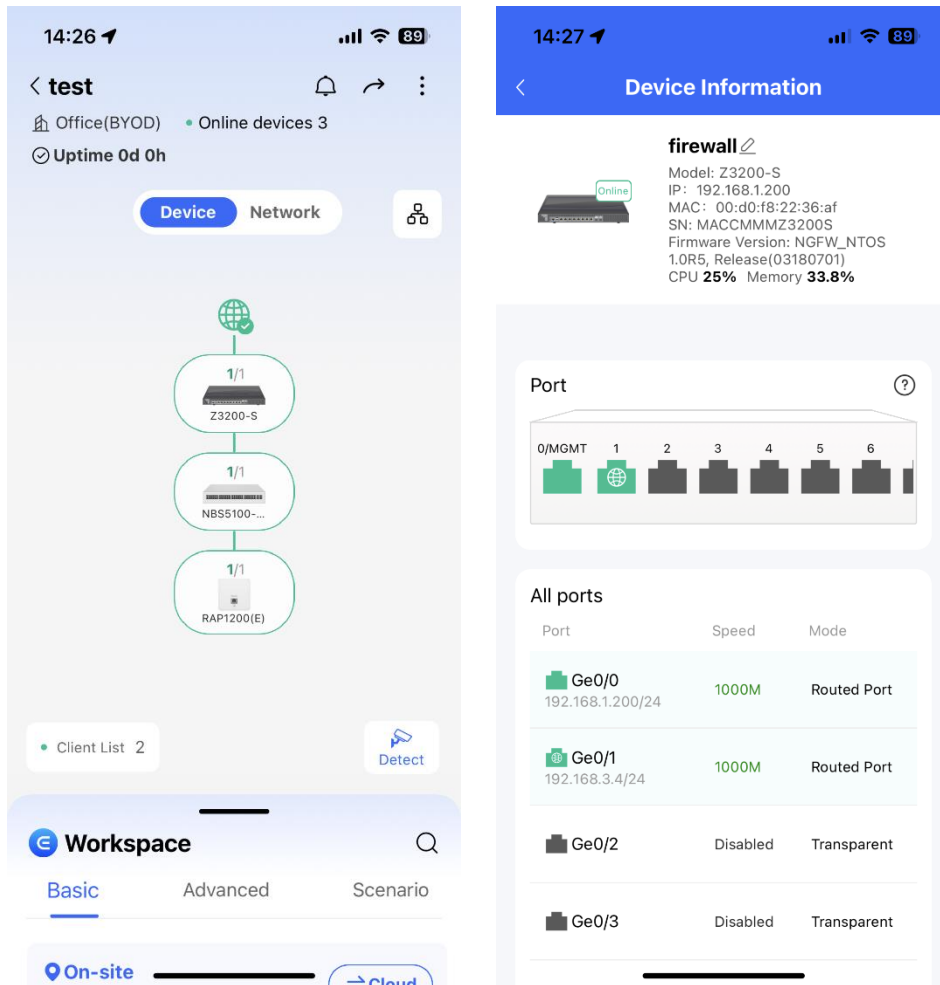
(7) Set the Wi-Fi name and password and tap **Save**.



(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.



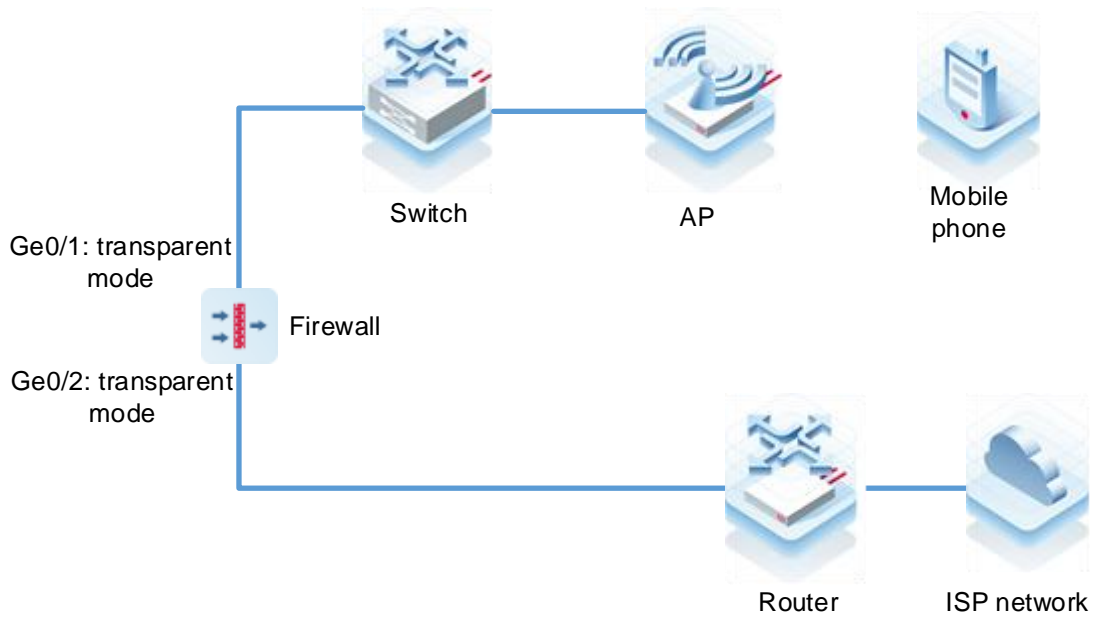
4.4 Deployment Using Ruijie Cloud App (Transparent Mode)

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.

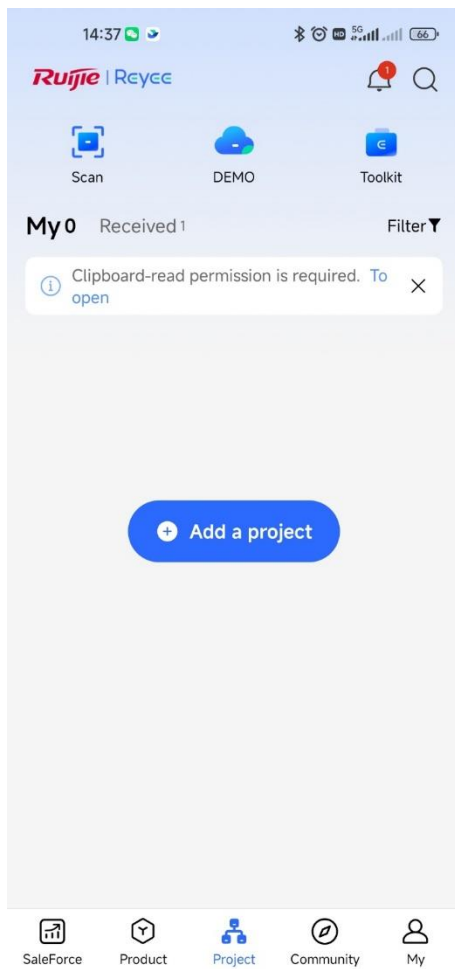
i Note

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

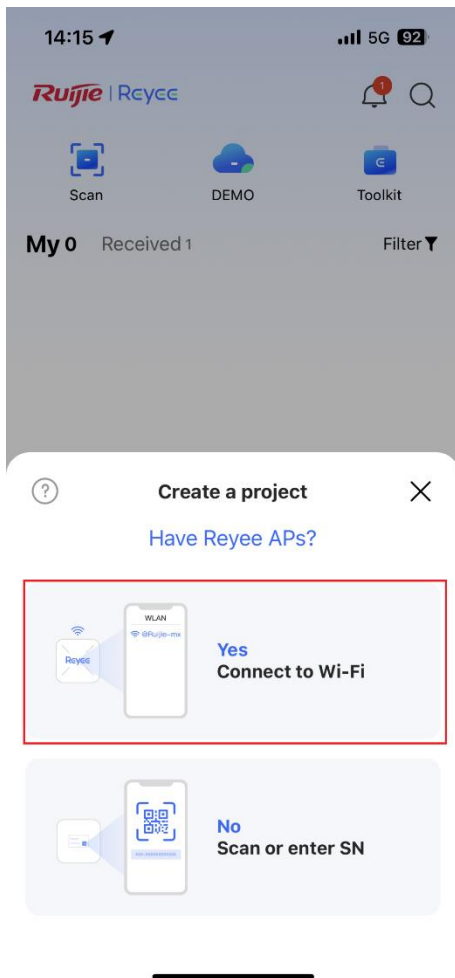


2. Procedure

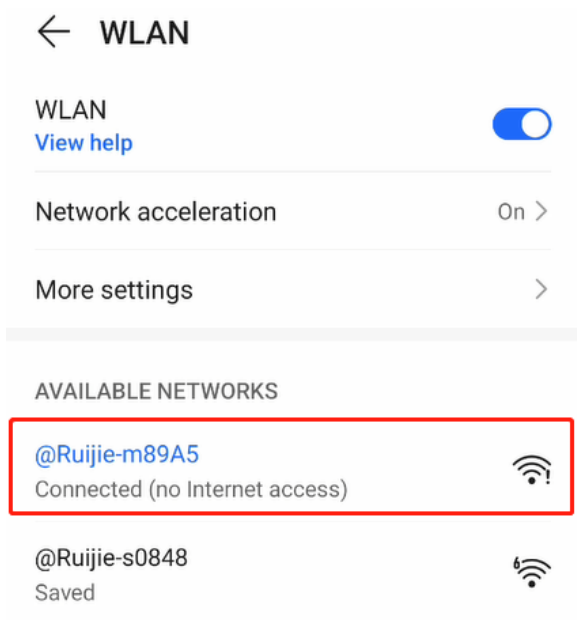
- (1) After the network environment is established according to the preceding figure, start the Ruijie Cloud app and choose **Project > Add a project**.



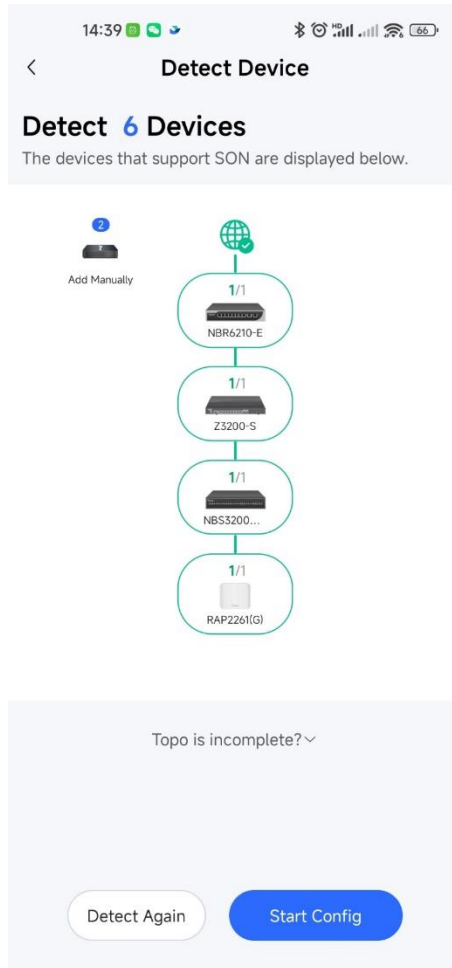
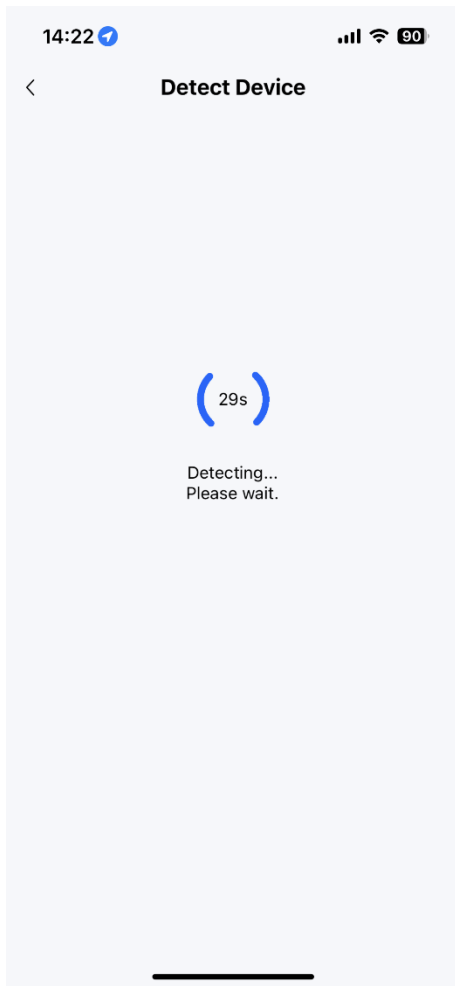
(2) Select **Connect to Wi-Fi** and add a project.



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

14:39

Basic Config

Project Config Internet Config Firewall Configuration Wi-Fi Config

Project Name
nbr_app

Management Password
ruijie@123

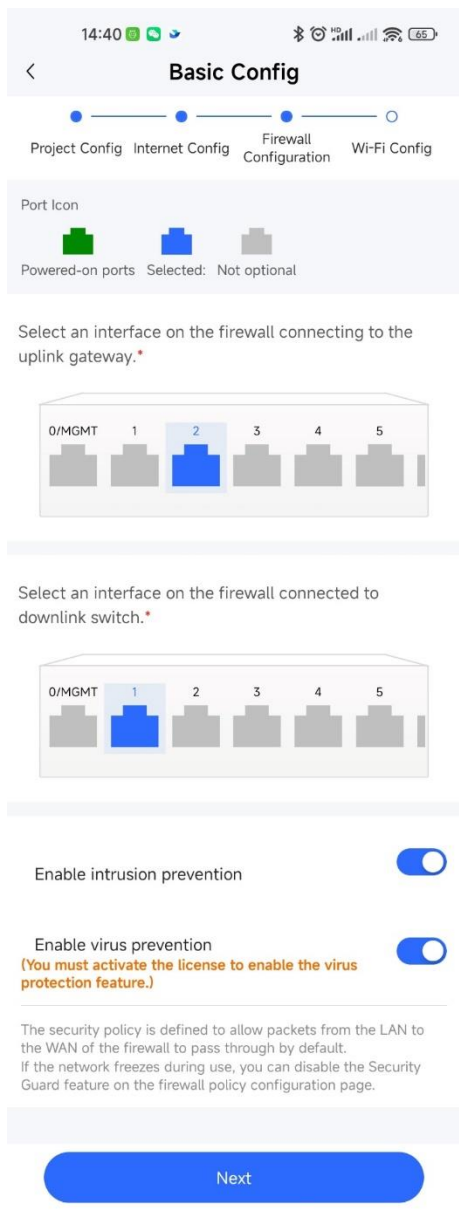
To ensure project security, ensure that the password meets the following requirements:

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

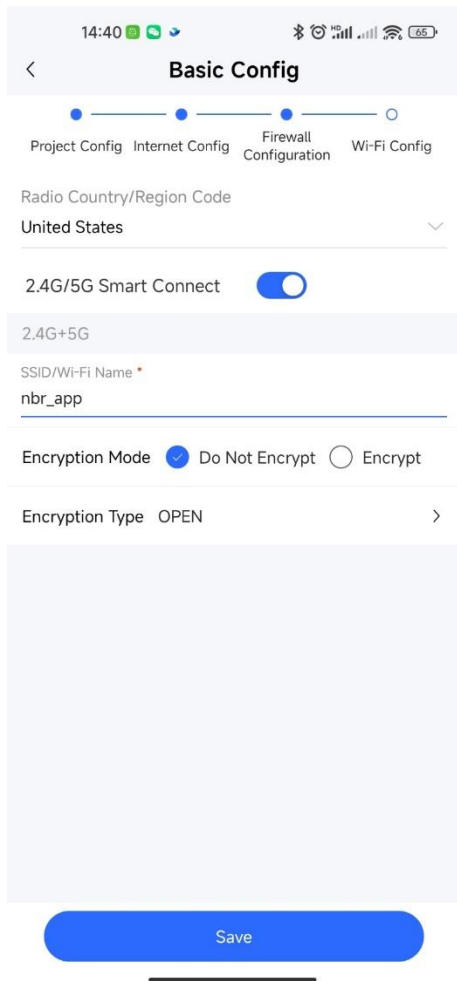
Scenario * Office

Next

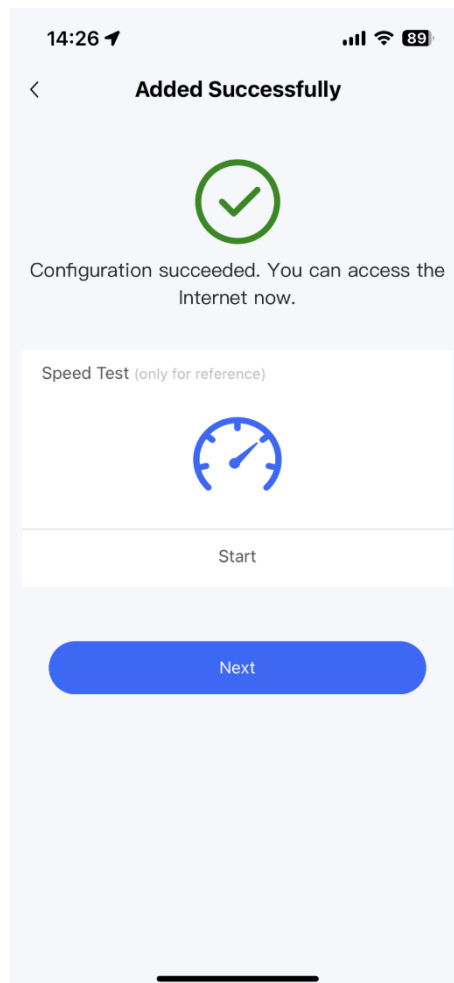
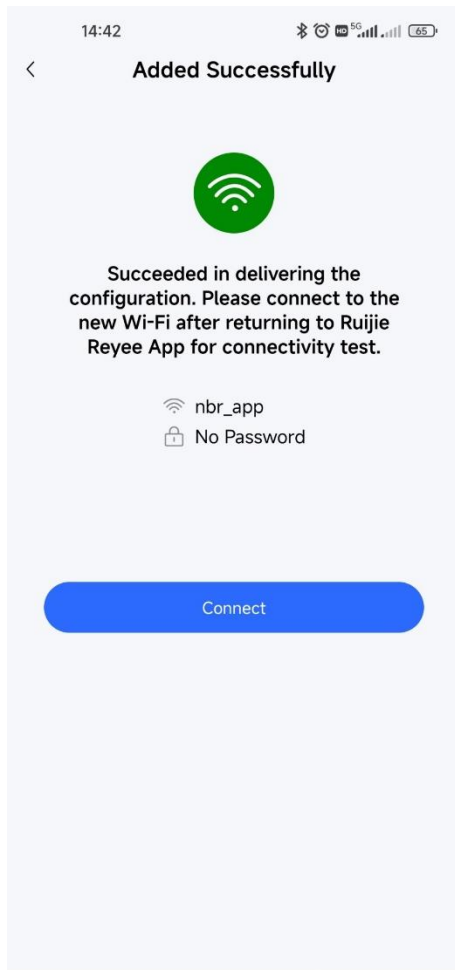
(6) Select the firewall interfaces connected to the router and switch, and tap **Next**.



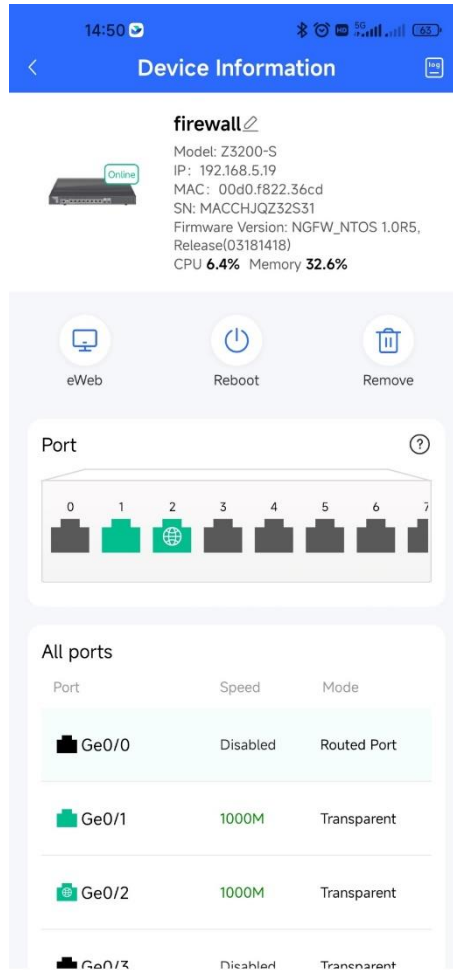
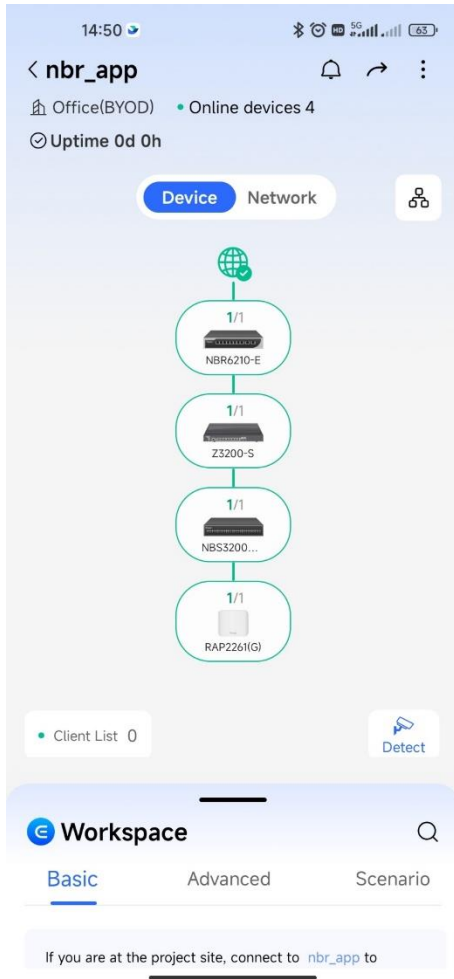
(7) Set the Wi-Fi name and password and tap **Save**.



(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.



5 Policy Configuration and Management

5.1 Security Policy

5.1.1 Overview

Security policies control packet forwarding based on packet attributes. In a security policy, filtering conditions (such as the source/destination security zone, source/destination IP address, service, and application), processing actions (permit or deny), and whether to perform content security checks (including intrusion defense and virus protection) can be set for packets.

After security policies are configured, the firewall will process received packets as follows:

- (1) Check whether packet attributes match the filtering conditions. Different filtering conditions are in an AND relationship. That is, a packet matches the security policy only when all the conditions are met. When multiple security policies are configured, they are matched one by one in the order of configuration until the packet matches a security policy successfully.
- (2) The matched packet is processed according to the processing action. If the action is permit, the packet is forwarded. If the action is deny, the packet is discarded and a security log is recorded.
- (3) If URL filtering, intrusion prevention, or virus protection is enabled in the security policy, the packet is forwarded to the corresponding module for content security check.
- (4) If a packet matches the URL filtering, intrusion prevention, or virus protection policy, it is processed according to the processing action. If the action is alarm, the packet is forwarded and a security log is recorded. If the action is block, the packet is discarded. Packets that do not match these policies are directly forwarded.

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

5.1.2 Manually Configuring Security Policies

Application Scenario

In addition to the wizard, 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**.

A tip dialog box is displayed.

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.

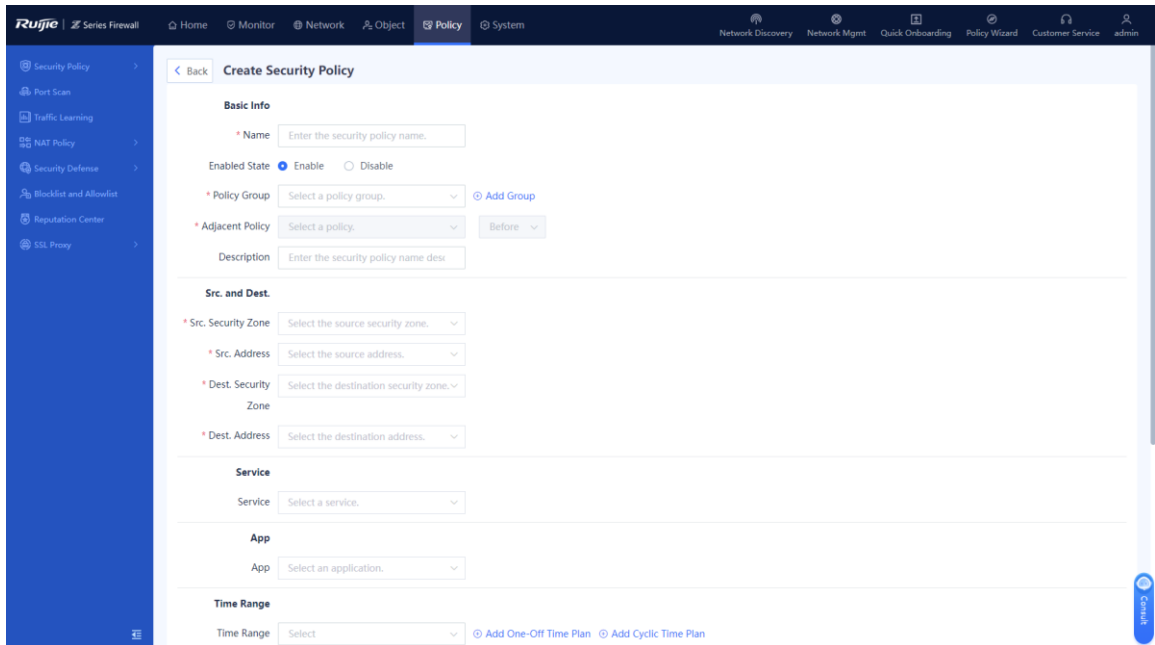
Do Not Show This Again

Simulation Space

Create

(3) Click **Create**.

The **Create Security Policy** page is displayed.



(4) Set the parameters for the security policy.

Item	Description	Remarks
Basic Info		
Name	Security policy name.	Characters such as `~!#%^&*+V0::"/<>?` and spaces are not allowed. [Example] Trust_to_untrust

Item	Description	Remarks
Enabled State	Whether to enable the new security policy.	[Example] Enable
Policy Group	Policy group to which the new security policy belongs.	<ul style="list-style-type: none"> ● Select from the drop-down list. ● Click Add Group to customize the new policy group. [Example] Default Policy Group
Adjacent Policy	Move the new security policy before or after the specified policy. The policy listed before has a higher matching priority.	N/A
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"> ● Click the drop-down list, and select a source security zone in the To-be-selected area. The selected zone is automatically added to the Selected area. ● Click Add Security Zone to add a custom security zone. [Example] trust
Src. Address	Source address initiating the target data connection.	Click the drop-down list, and select a source address in the To-be-selected area. The selected address is automatically added to the Selected area. [Example] any
Dest. Security Zone	Destination security zone of the target data connection.	<ul style="list-style-type: none"> ● Click the drop-down list, and select a destination security zone in the To-be-selected area. The selected zone is automatically added to the Selected area. ● Click Add Security Zone to add a custom security zone. [Example] trust

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

Item	Description	Remarks
Content Security	<p>Whether intrusion prevention, virus detection, and URL filtering are enabled for the target data connection.</p> <p>To enable content security checks, you must specify corresponding templates. For intrusion prevention and virus protection templates, 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"> ● Intrusion Prevention: Enable ● Virus Protection: Enable ● URL Filtering: Disable
Advanced	<p>Advanced settings of the security policy, including:</p> <p>Long-Lived Connection: applies to the special servers that require long-lived connections. After this function is enabled, the server's connection request is not restricted by the connection timeout setting of the firewall. The connection duration needs to be set.</p>	<p>Click Settings, and set parameters on the displayed Advanced Option page.</p> <p>[Example]</p> <p>Select Long-Lived Connection.</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

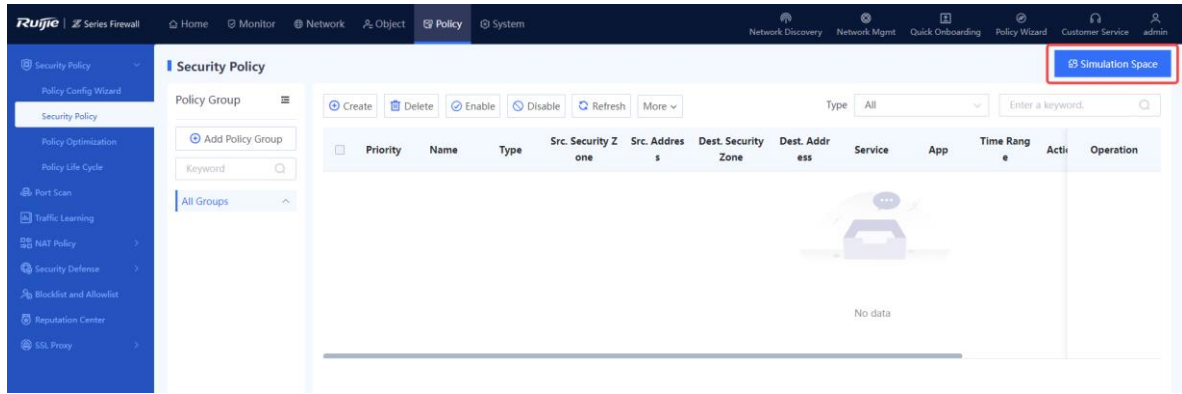
5.1.3 Conducting Simulation Run

Application Scenario

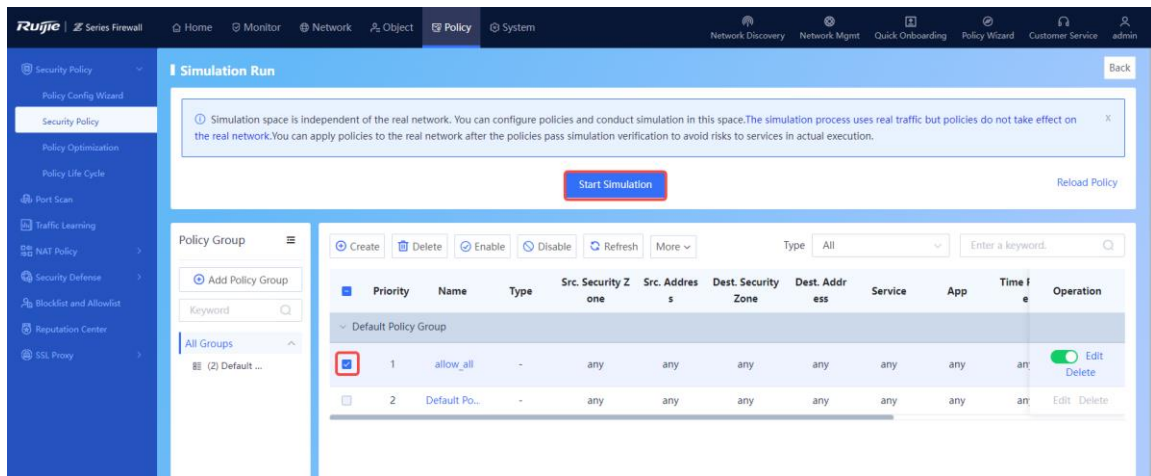
After you create a security policy, you can conduct simulation run to discover vulnerabilities or problems of the policy in advance to avoid risks to services in actual implementation.

Procedure

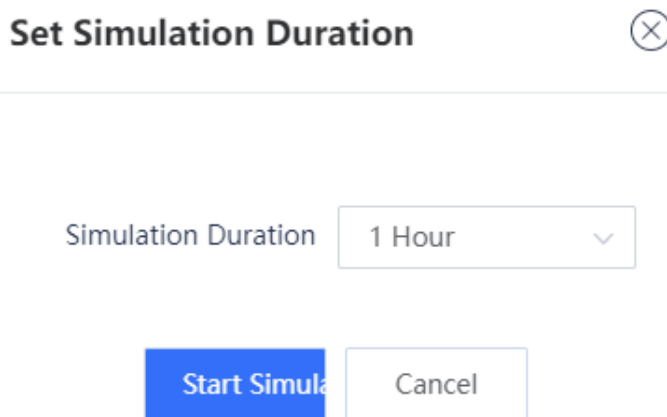
- (1) Choose **Policy > Security Policy**.
- (2) Click **Simulation Space** in the upper right corner of the operation area.



(3) Select the policy for which simulation run will be performed, and click **Start Simulation**.

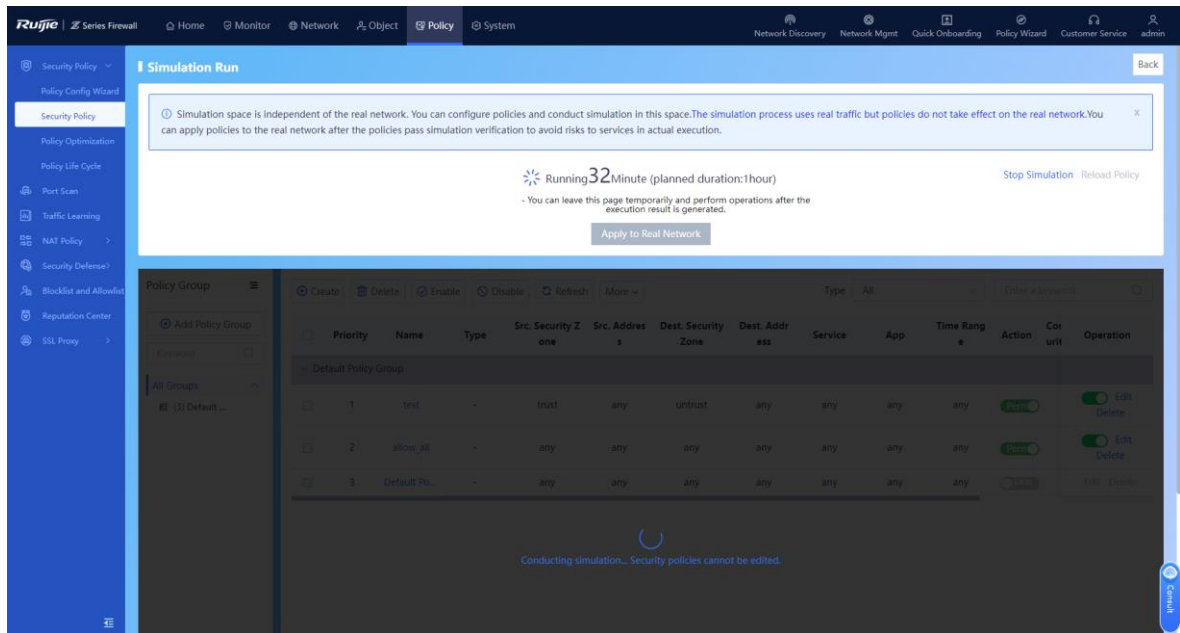


(4) In the **Set Simulation Duration** dialog box, set the duration of simulation run.



(5) Click Start Simulation.

The system automatically performs simulation run for the selected policies.



(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 ⊗

ⓘ 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; margin-top: 10px;">No data</p>					

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

5.1.4 Importing Configuration Files to Configure Security Policies

Application Scenario

Z-S series firewalls support fast generation of security policies by importing configuration files.

Caution

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

Prerequisites

The configuration files can be obtained in the following two ways:

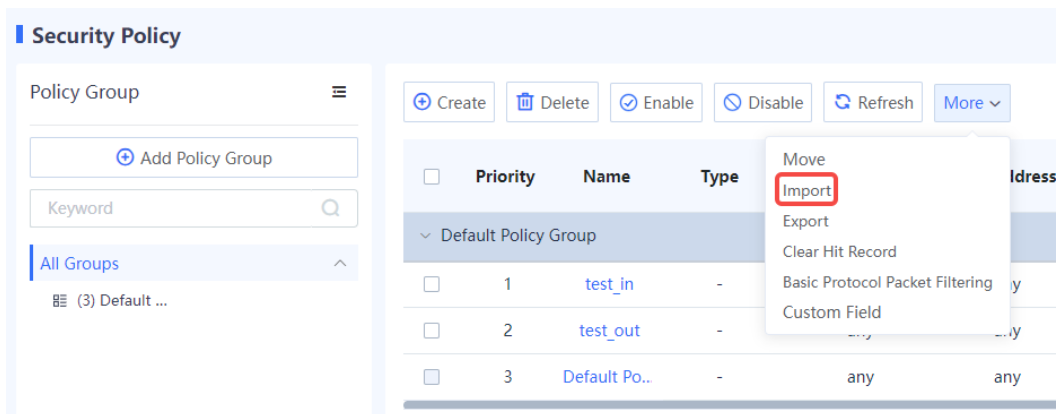
- The device provides the configuration file template. You can download the configuration file template, and modify it according to actual service situations.
- To import the configurations from another device to a Z-S series firewall, you can configure the policy migration tool to obtain the corresponding configuration file.

Note

For the usage of the policy migration tool, contact technical support engineers.

Procedure

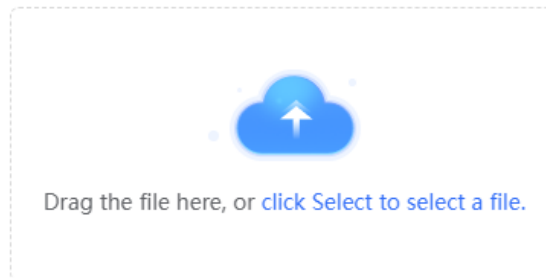
- (1) Choose **Policy > Security Policy**.
- (2) Click **More** in the operation area and select **Import** from the drop-down list.



- (3) A tip dialog box is displayed.

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

If imported configurations conflict with existing configurations,

- Display Conflicting Data Skip

OK

Cancel

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

Note

After modifying the configuration file, check whether the naming of the configuration file meets the system requirements. The naming format of the configuration file is: config-conversion-{yyyyMMddHHmmssSSS}.csv.

- (5) Drag the configuration file to the upload area or click **click Select to select a file** 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:

- **Display Conflicting Data:** 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.

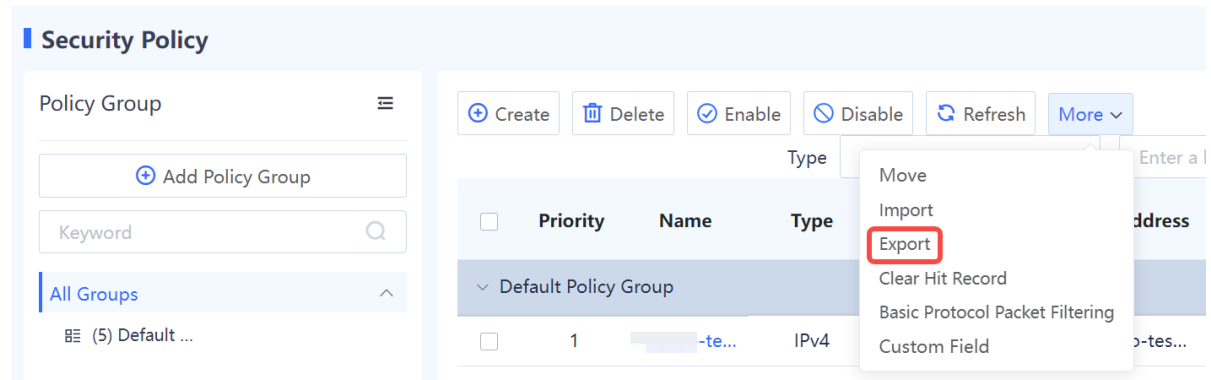
5.1.5 Exporting Security Policies

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.



5.1.6 Adjusting Security 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.

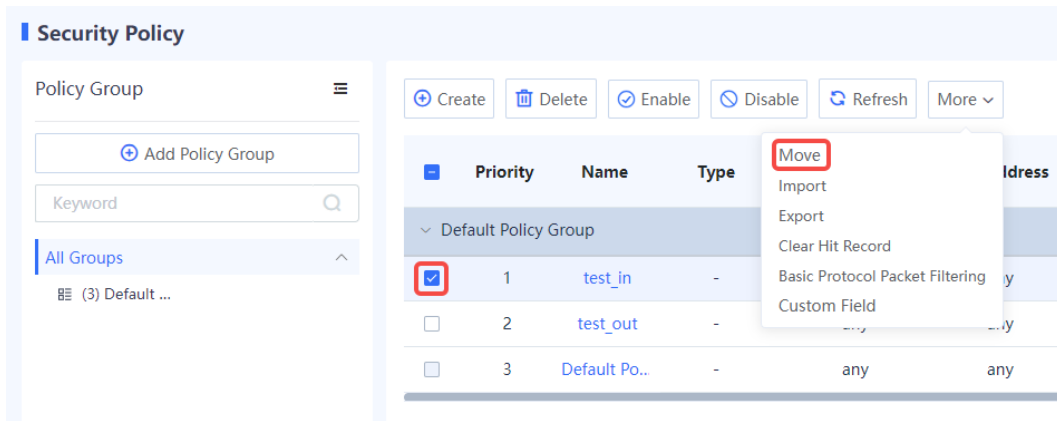
You can adjust the order of security policies to meet service requirements.

i Note

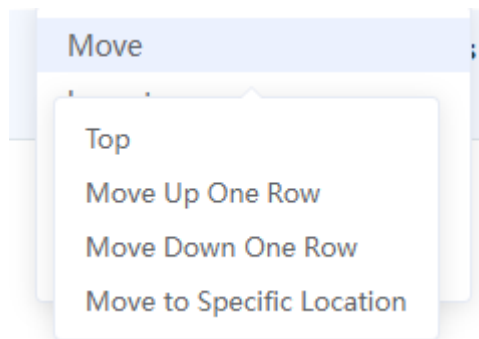
- There is a default security policy in the system that has the lowest priority. It blocks all data connections.
- When a data connection fails to hit a configured policy and hit the default policy, the data connection is blocked.

Procedure

- (1) Choose **Policy > Security Policy**.
- (2) Select the policy of which the priority needs to be adjusted.



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



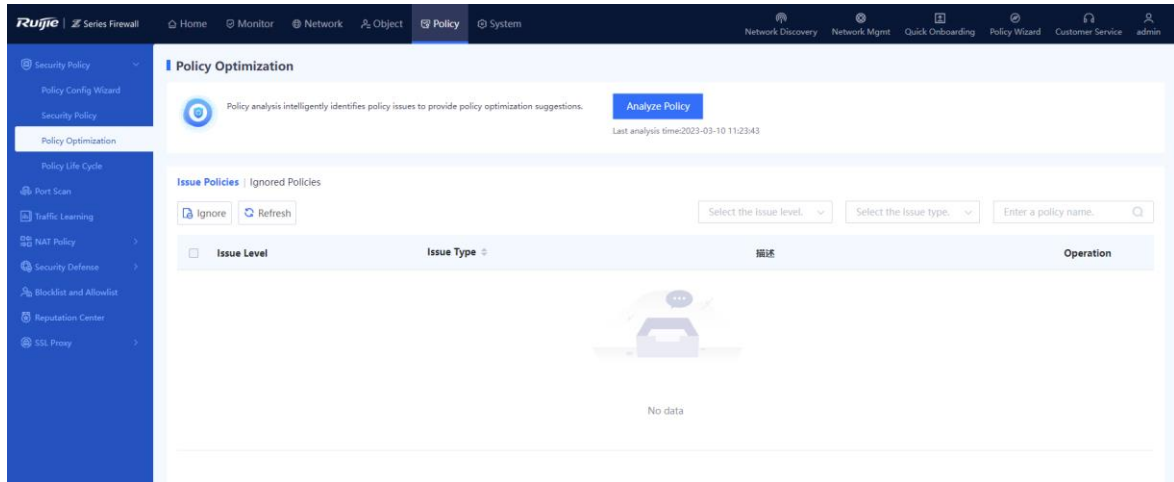
5.1.7 Optimizing Security Policies

Application Scenario

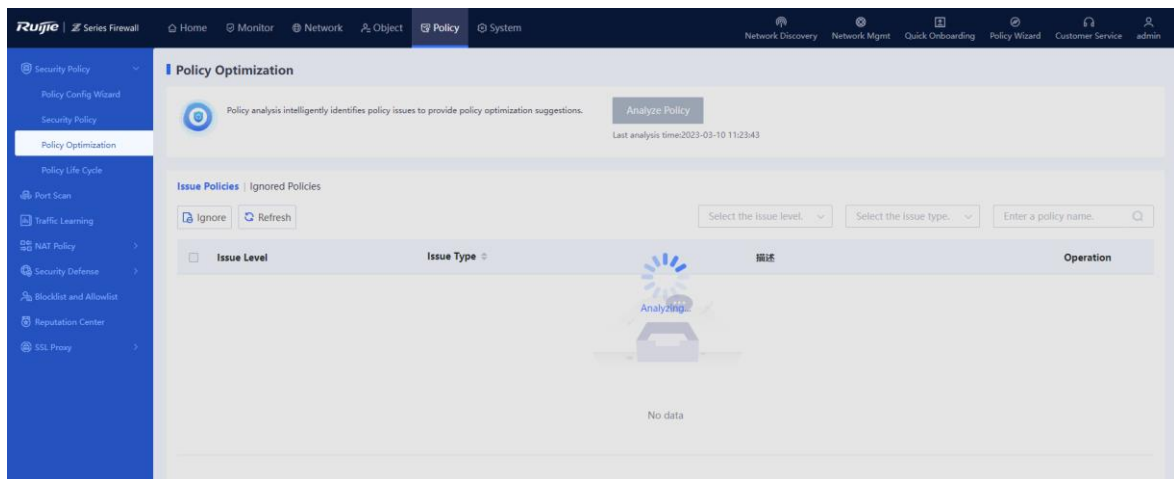
Affected by factors such as service accumulation and change of O&M personnel, the configuration complexity of security policies becomes increasingly high during the routine security policy O&M process. The policy optimization function of Z-S series firewalls can intelligently compare and analyze the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

- 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

Question Description

Description: 该策略允许任何源到任何目的数据包转发, 权限过大

Impact: 故通过大策略可能允许恶意用户或攻击者获得对网络服务的未授权访问

Solution: 仅限那些需要访问权限的主机限制对服务的访问

Issue No./Total: 1/1 [Previous] [Next]

Optimize Policy

Color description: To-be-optimized

Optimization suggestion: 仅限那些需要访问权限的主机限制对服务的访问

Priority	Name	Source	First Creation Time	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Operation
2	allow_all	manual	2023-03-13 10:55:06	any	any	any	any	any	any	<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.

5.1.8 Viewing Policy Life Cycle

Application Scenario

The policy life cycle page displays detailed information about the adding, modification, and deletion of security policies for O&M personnel to trace problems.

Procedure

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

Policy Life Cycle

Export Refresh Search Criteria Enter the policy name.

Change Time	Change Strategy	Change Type	Account	User IP	Operation
2023-03-13 11:43:54	allow_all	Create	admin	172.25.22.250	View Details
2023-03-13 11:36:32	test	Create	admin	172.20.36.39	View Details
2023-03-10 12:31:20	allow_all	Move	admin	172.26.36.232	View Details
2023-03-10 12:30:54	123	Move	admin	172.26.36.232	View Details
2023-03-10 12:28:27	111	Delete	admin	172.26.36.232	View Details
2023-03-10 12:25:27	111	Create	admin	172.26.36.232	View Details
2023-03-09 14:08:59	123	Edit	admin	172.20.36.27	View Details
2023-03-08 16:22:55	123	Edit	-	-	View Details
2023-03-08 16:22:23	123	Edit	-	-	View Details
2023-03-08 10:15:29	123	Move	-	-	View Details

10 / Page Total: 19 Go to 1 1 2

- (2) Click **View Details** to view policy change details.

[Back](#) **Change Details**

Operation Info
 Policy Name: 123 Change Time: 2023-03-09 14:08:59 Account/IP: admin/172.20.36.27

Change Details Check Changed Items Only

Policy	Before the Change	After the Change
Name	123	123
Policy Group	def-group	def-group
Priority	1	1
Description	any	any
Src. Security Zone	any	any
Src. Address	any	any
Dest. Security Zone	any	any
Dest. Address	any	any
Service	any	any
App	any	any
Time Range	any	any
Action	Permit	Permit
Intrusion Prevention	1234-block	1234-alert Change
Virus Protection	-	-

5.1.9 Enabling Basic Protocol Packet Control

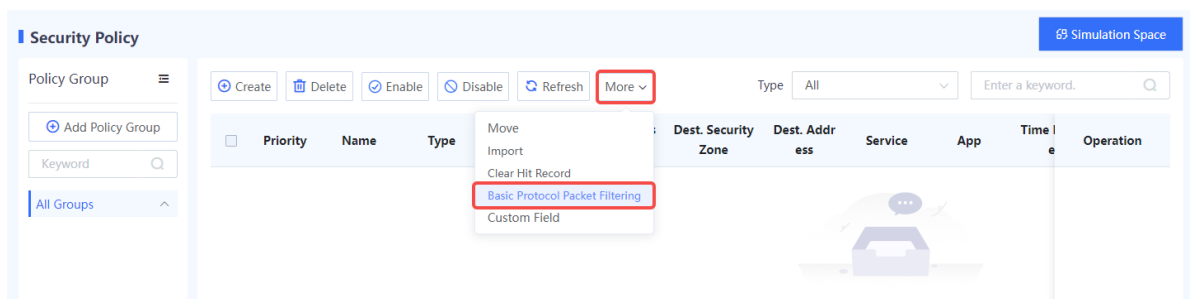
Application Scenario

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

By default, the firewall does not perform security control on the network basic protocol packets (such as DHCP packets and auto-discovery protocol packets). It directly forwards these packets if no additional configurations are performed so that the device can quickly access the network. If you want to control forwarding behavior of basic protocol packets by configuring a security policy, you can enable the basic protocol packet control function to control these packets.

Procedure

- (1) Choose **Policy > Security Policy > Security Policy**.
- (2) Click **More** and select **Basic Protocol Packet Filtering** from the drop-down list.



- (3) On the **Basic Protocol Packet Control** page, enable Basic Protocol Packet Control.

Basic Protocol Packet Control ⊗

i When this function is enabled, forwarding of packets using DHCP or an auto-discovery protocol is controlled by security policies.

Basic Protocol Packet

Control

OK

Cancel

(4) Click **OK**.

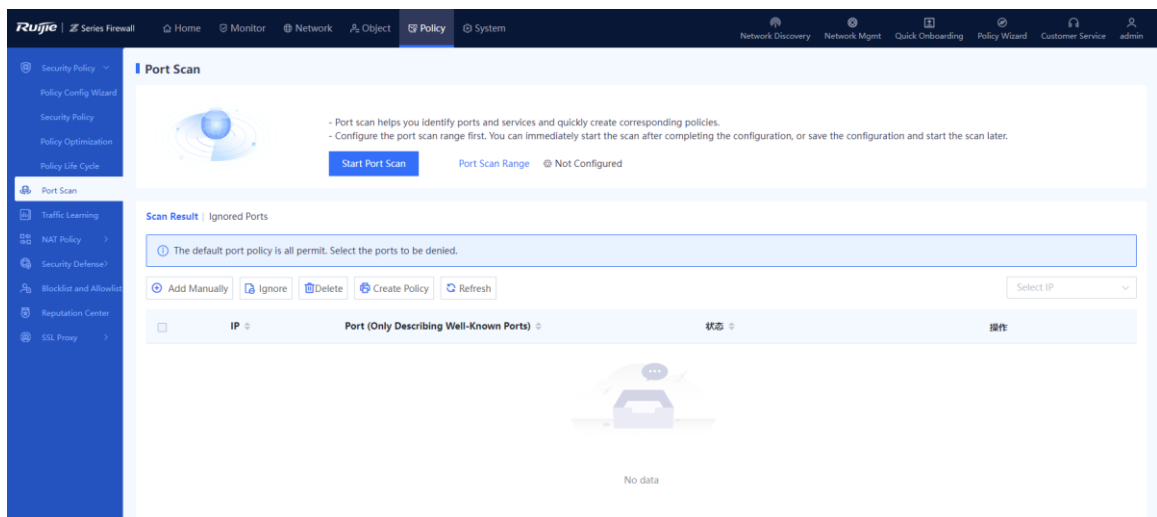
5.2 Enabling Port Scan

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

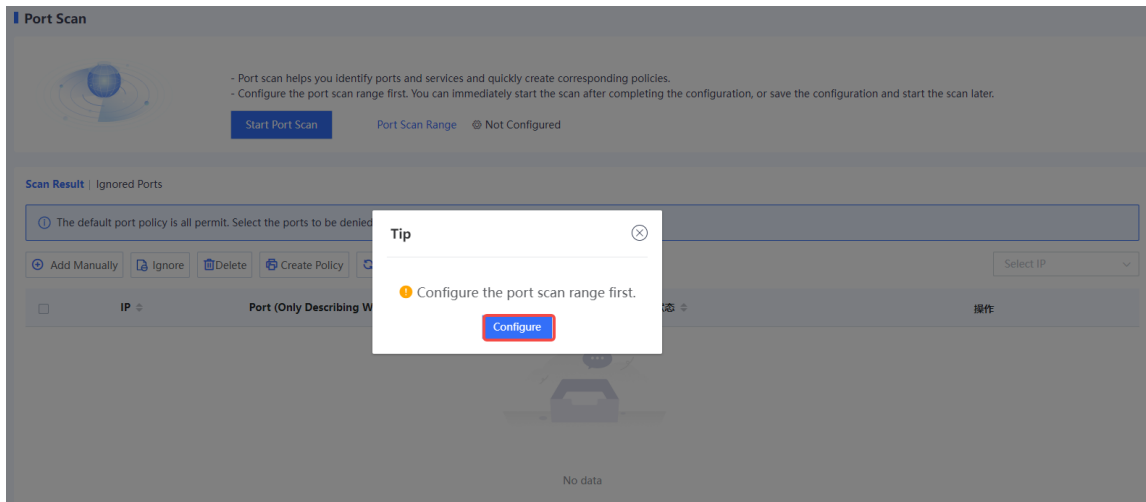
(1) Choose **Policy > Port Scan**.



(2) (Optional) If the port scan range is not configured, configure it first.

a Click **Start Port Range**.

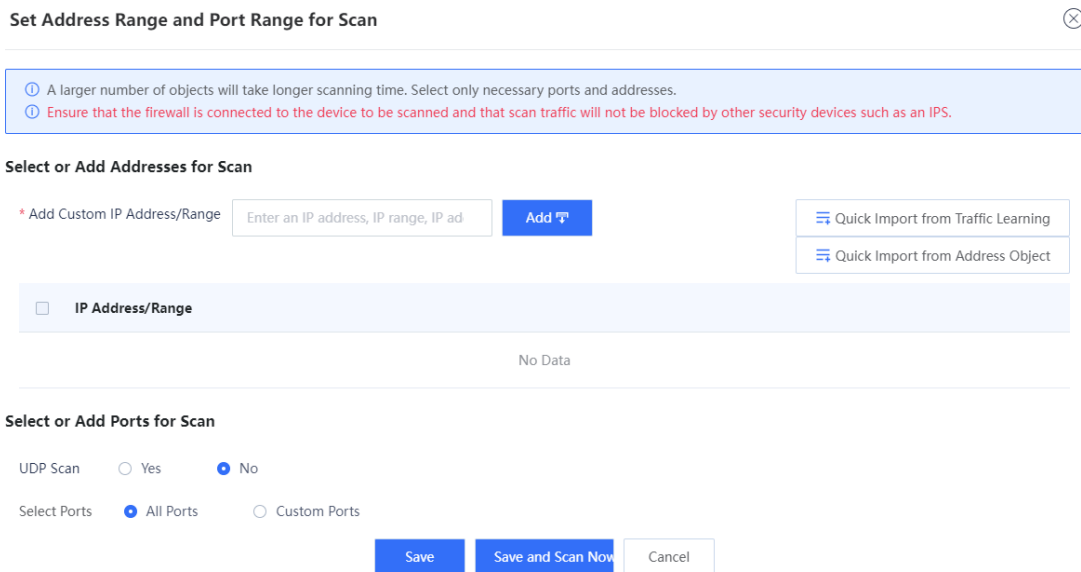
If the system displays "Configure the port scan range first", click **Configure**.



- b Select or add the IP address to be scanned.
- c 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**.



- d Select or add the port to be scanned.

Select or Add Ports for Scan

UDP Scan Yes No

Select Ports All Ports Custom Ports

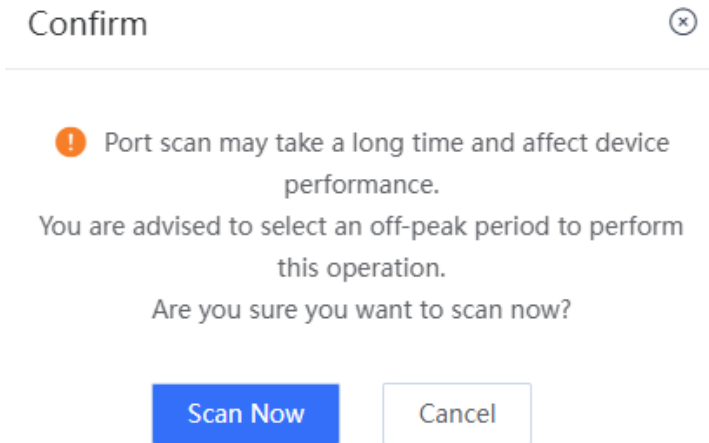
Common Ports [Select Common Ports](#)

Custom Ports

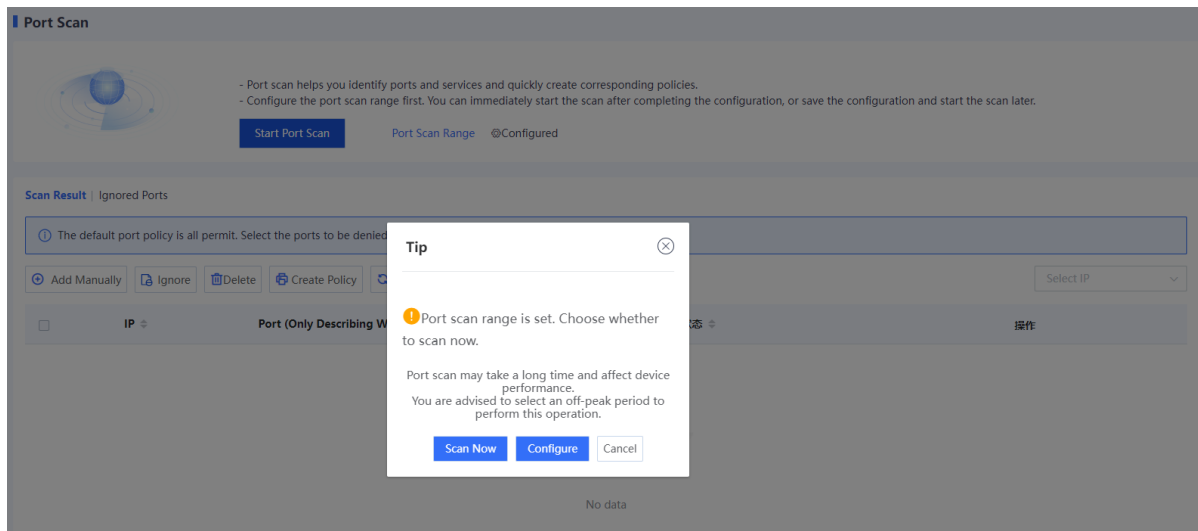
Add Custom Port Range

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

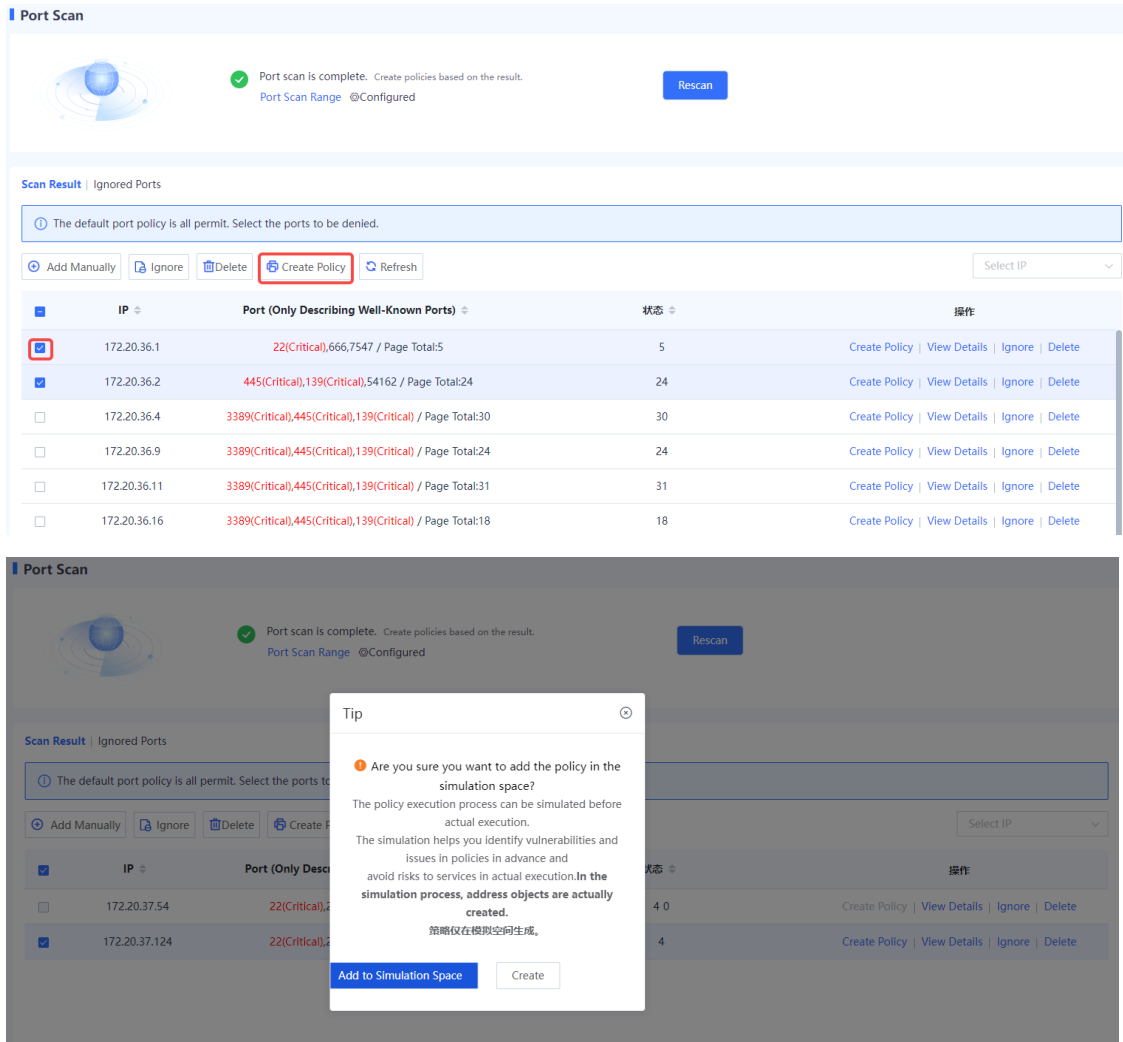
- e Choose whether to start port scan immediately according to service situation.
 - o When services are busy, click **Save** to save the port scan configuration. You can start port scan when services are idle.
 - o When services are idle, click **Save and Scan Now** to save the port scan configuration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

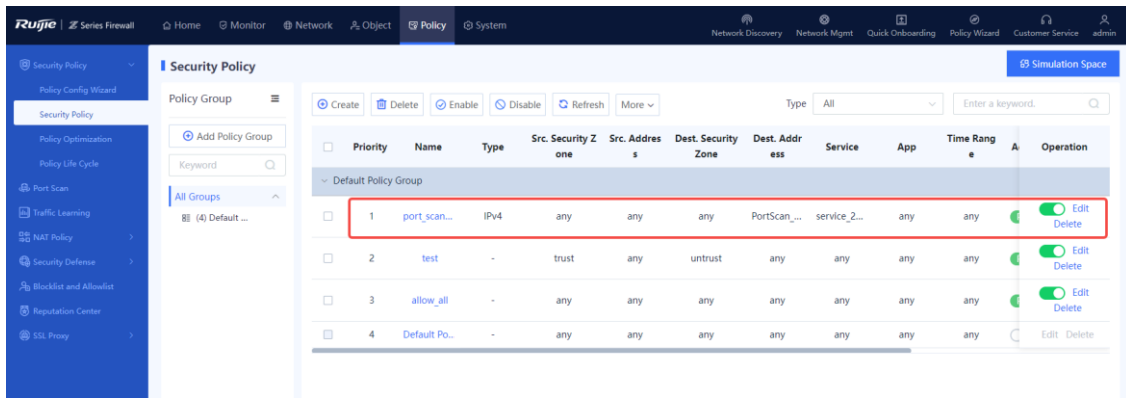
Insert it to the specified location. ⊗

* 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

Scan Result | Ignored Ports

The default port policy is all permit. Select the ports to be denied.

<input checked="" type="checkbox"/>	IP	Port (Only Describing Well-Known Ports)	状态	操作
<input type="checkbox"/>	172.20.37.54	22(Critical),20099,2048 / Page Total:4	4 0	Create Policy View Details Ignore Delete
<input checked="" type="checkbox"/>	172.20.37.124	22(Critical),20099,2048 / Page Total:4	4	Create Policy View Details Ignore Delete

- Move the cursor to the scanned port number, and the page displays the purpose of commonly used ports and the risk information of high-risk ports.
- Select an IP address and click **Create Policy** to generate a security policy for the IP address. On the port scan details page, you can set security policy actions, or edit policies on the security policy page.
- Select an IP address and click **View Details** to view the open port number of the IP address and generate a security policy for a single port number.
- Select an IP address and click **Ignore** to add all ports of the IP address to the ignored list and set the ignore duration. (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.

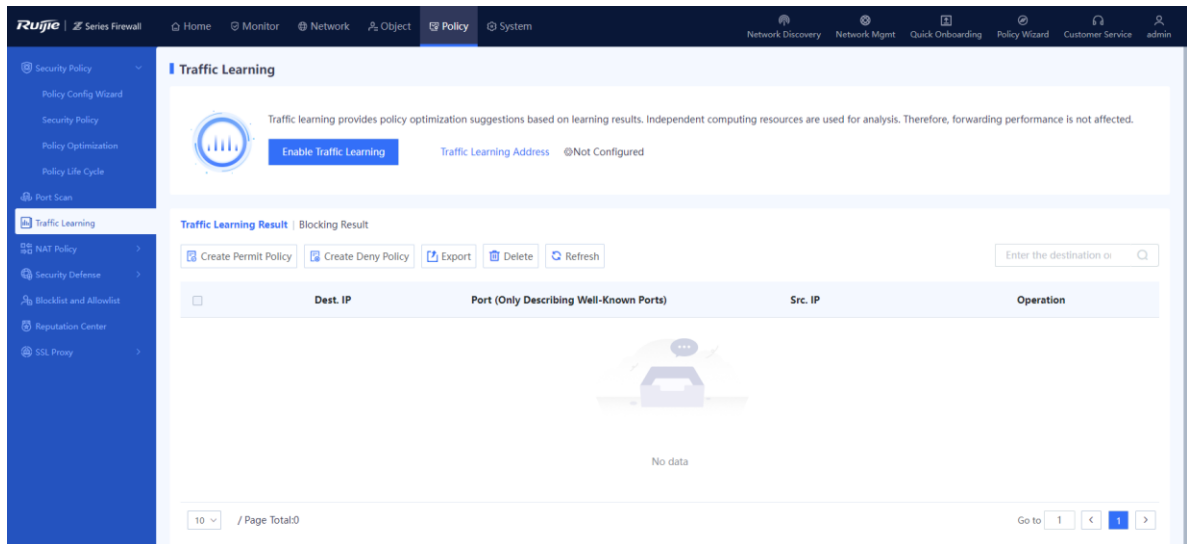
5.3 Enabling Traffic Learning

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 asset IP addresses, open ports, and access relationships between assets on the network based on the configured asset IP addresses or IP address ranges.

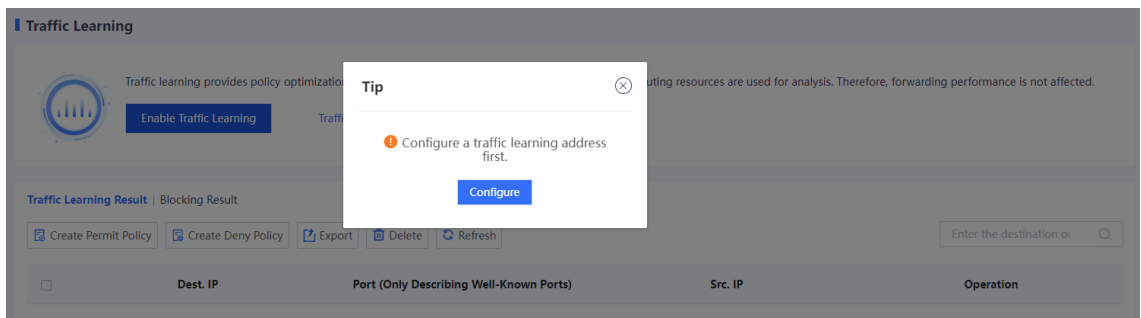
Procedure

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



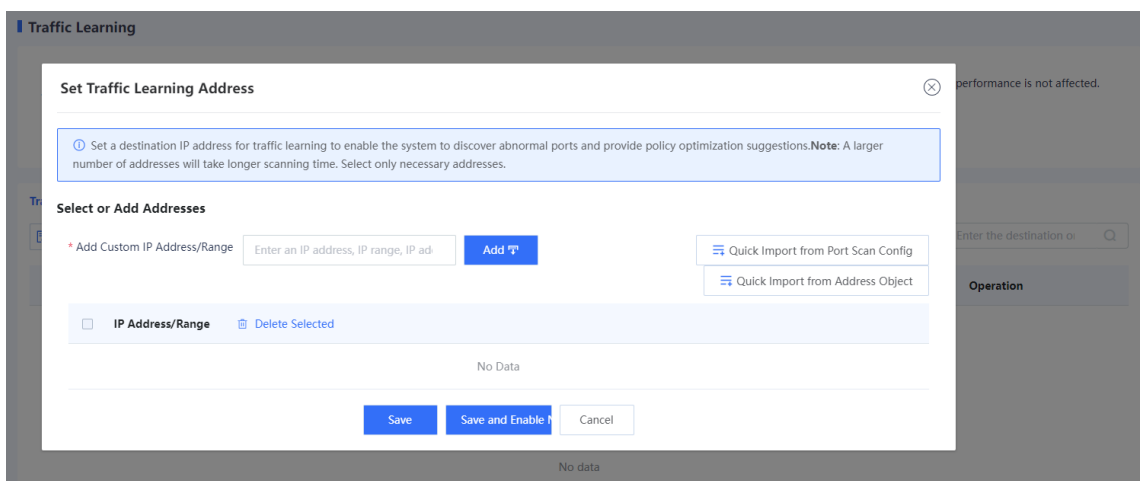
(2) (Optional) If the traffic learning address is not configured, configure it first.

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



- b Select or add the IP address to be learned.

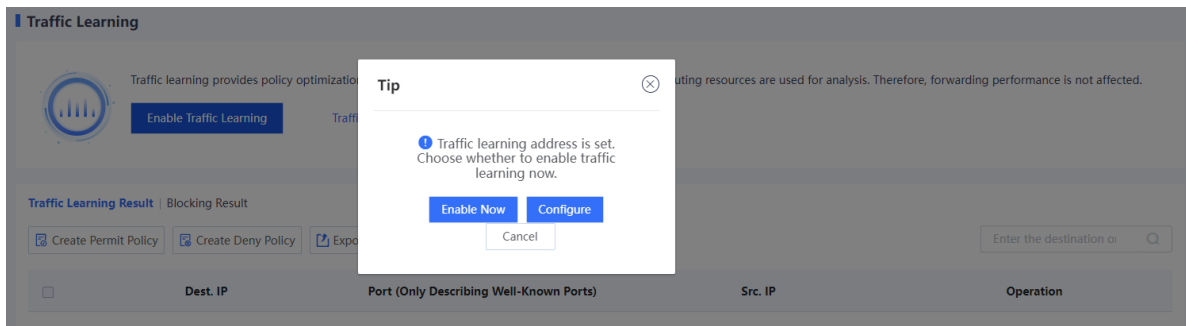
Enter the IP address or range to be learned in the **Add Custom IP Address/Range** input box, and click **Add** to add it to the **IP Address/Range** area.



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**.



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



- b Add this policy to the simulation space or directly to the security policy list according to service requirements.

Tip ⊗

! Are you sure you want to add the policy in the simulation space?

The policy execution process can be simulated before actual execution.

The simulation helps you identify vulnerabilities and issues in policies in advance and avoid risks to services in actual execution. **In the simulation process, address objects are actually created.**

The policies are created only in the simulation space.

Add to Simulation Space

Insert it to the specified location. ⊗

* Policy Name
Prefix

* Policy Group
Policy

Before/After
the Adjacent Policy

- 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	Perm		0	Clear	View Details.. Edit Delete
3	test	any	any	any	any	Perm		0	Clear	View Details.. Edit Delete
4	allow_all	any	any	any	any	Perm		0	Clear	View Details.. Edit Delete

d To view the learned blocked access relationships, click the **Blocking Result** tab. To view the number of blocking times, blocking policy, blocked service, and the time of the last block, click **View Details**.

Traffic Learning

Traffic learning provides policy optimization suggestions based on learning results. Independent computing resources are used for analysis. Therefore, forwarding performance is not affected.

[Enable Traffic Learning](#) Traffic Learning Address @Configured

Traffic Learning Result | **Blocking Result**

[Refresh](#) Enter the destination or

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

5.4 Traffic Control Policy

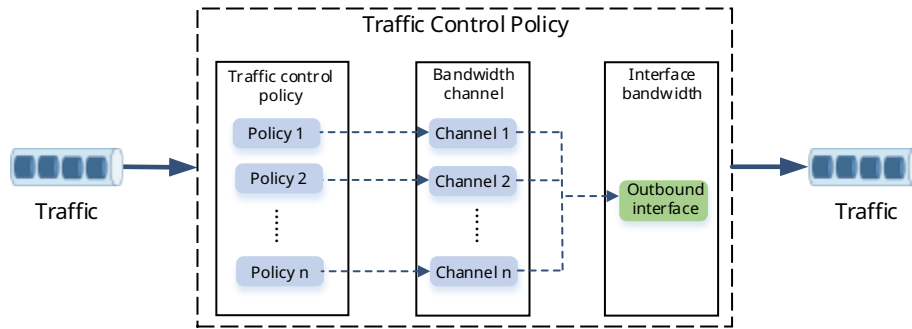
5.4.1 Overview

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:

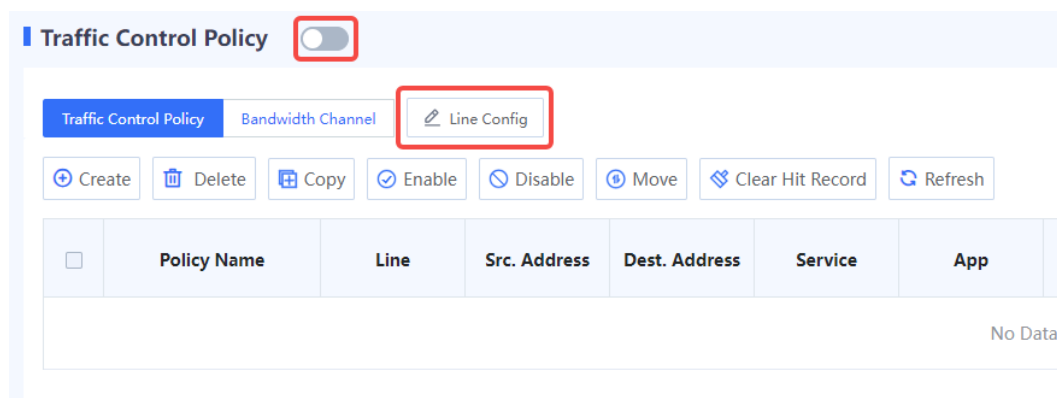


- (1) After a device receives traffic, the device matches the traffic against traffic control policies in the configured order until one policy is matched. If the traffic matches no policy, no traffic control action is performed.
- (2) The closer a policy is to the front, the higher its priority in matching. 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.

5.4.2 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.

Traffic Control Policy ☐

← Back
Line Config
Any unidentified WAN interfaces? [Configure WAN Interface](#)

Interface Ge0/7 Ge0/8

Ge0/7

Uplink Mbps ▼

Downlink Mbps ▼

Ge0/8

Uplink Mbps ▼

Downlink Mbps ▼

Save

i **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.

Traffic Control Policy ☑

Traffic Control Policy
Bandwidth Channel
✎ Line Config

+ Create
📄 Copy
🗑 Delete
🔄 Refresh

	Channel Name	Overall Rate Limit	Priority	Reference Count	Operation
<input type="checkbox"/>	1	Guaranteed Rate: ↑50 Mbps Max. Rate: ↑100 Mbps	1 (Highest)	0	Edit Copy Delete

(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 v

Guaranteed Uplink Rate Mbps v

Max. Downlink Rate Mbps v

Guaranteed Downlink Rate Mbps v

ⓘ Priority 4 (Medium) v

Save

Item	Description	Remarks
Basic Info		
Name	Bandwidth channel name.	[Example] Channel 1
Overall Rate Limit		
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

Item	Description	Remarks
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
Basic Info		
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.	-
Src. and Dest.		
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
Services and Apps		
Service	The traffic of specified services matches the policy.	[Example] Any
App	The traffic of specified applications matches the policy.	[Example] Any
User/User Group		

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

(4) Click **Save**.

5.5 NAT Policy

5.5.1 NAT Overview

Network Address Translation (NAT) is a process of translating the IP address in the header of an IP packet into another IP address. Both the source and destination IP addresses can be translated.

In actual implementation, NAT is mainly used on edge devices that connect two networks to allow intranet users to access public networks and allow public networks to access specific intranet resources (such as intranet servers).

5.5.2 NAT Types

NAT can be classified into the following types according to different classification principles.

- The following table describes classification based on IP address types before and after NAT.

NAT Type	NAT Content	Before NAT	After NAT
Traditional NAT (NAT44)	Source NAT (SNAT)	The source address is a private IPv4 address.	The source address is a public IPv4 address.
	Destination NAT (DNAT)	The destination address is a public IPv4 address.	The destination address is a private IPv4 address.
	Twice NAT	The source address is a private IPv4 address, and the destination address is a public IPv4 address.	The source address is a public IPv4 address, and the destination address is a private IPv4 address.

NAT Type	NAT Content	Before NAT	After NAT
NAT46	Source address and destination address	Both the source and destination addresses are IPv4 addresses.	Both the source and destination addresses are IPv6 addresses.
NAT64	Source address and destination address	Both the source and destination addresses are IPv6 addresses.	Both the source and destination addresses are IPv4 addresses.
NAT66	SNAT	The source address is a private IPv6 address.	The source address is a public IPv6 address.
	DNAT	The destination address is a public IPv6 address.	The destination address is a private IPv6 address.

- The following table describes classification based on whether the source port number is translated.

SNAT Type	NAT Content	Application Scenario
No-PAT	Only IP addresses are translated, and port numbers at the transport layer are not translated.	<ul style="list-style-type: none"> Intranet and public network connected by NAT device: 1:1 translation between private IP address and public IP address. This mode is used when there are only a small number of Internet access users, which is close to the number of available public IP addresses. IPv4 and IPv6 networks connected by NAT device: 1:1 translation of IPv4 address and IPv6 address. This mode is used when the number of IPv4 addresses is close to that of IPv6 addresses.
PAT (NAPT)	Both IP addresses and port numbers at the transport layer are translated.	<ul style="list-style-type: none"> Intranet and public network connected by NAT device: Multiple private IP addresses share one or multiple public IP addresses. This mode is used when only a few public IP addresses are available, and a large number of private network users require Internet access. IPv4 and IPv6 networks connected by NAT device: Multiple IPv6 addresses can be translated into one IPv4 address, and the mappings are distinguished by port. This mode is used when only a few IPv4 addresses are available.

- The following table describes classification based on address mapping modes of NAT.

NAT Type	Description
Static NAT	A permanent 1:1 mapping is manually established between addresses.
Dynamic NAT	Available addresses in the NAT address pool are dynamically selected as addresses after NAT, with no fixed mapping between the addresses before and after NAT.

5.5.3 Working Principle

1. NAT64 Prefix

The NAT64 prefix is an IPv6 address prefix with a length of 32, 40, 48, 56, 64 or 96 bits. It is used to construct an IPv6 address of an IPv4 node on an IPv6 network in NAT46/NAT64, thereby enabling communication between IPv4 and IPv6 networks. When an IPv4 host initiates an access request packet, the device can use the NAT64 prefix to translate the source IPv4 address of the packet into an IPv6 address. When an IPv6 host initiates an access request packet, the device can extract the translated IPv4 address from the destination IPv6 address of the packet based on the NAT64 prefix.

The position where the IPv4 address is embedded in the IPv6 address varies with the NAT64 prefix length. As shown in [Figure 5-1](#), when the NAT64 prefix length is 32, 64, or 96 bits, the entire IPv4 address is embedded in the IPv6 address. When the NAT64 prefix length is 40, 48, or 56 bits, the IPv4 address is split into two parts which are embedded before bit 64 and after bit 71.

Note

PL indicates the prefix length.

Figure 5-1 IPv6 Address Formats for Different NAT64 Prefix Lengths

PL	0	31	39	47	55	63	71	79	87	95	103	127
32	NAT64 prefix		IPv4 address				00	All zeros				
40	NAT64 prefix		v4 (24)		00	(8)	All zeros					
48	NAT64 prefix		v4 (16)		00	v4 (16)		All zeros				
56	NAT64 prefix		(8)	00	v4 (24)		All zeros					
64	NAT64 prefix				00	IPv4 address			All zeros			
96	NAT64 prefix									IPv4 address		

For example, when the IPv4 address is 192.168.1.10 and the NAT prefix is 3001::/64, the corresponding IPv6 address is 3001:0000:0000:0000:00C0:A801:0A00:0000, or 3001::C0:A801:A00:0.

2. NAT-PT

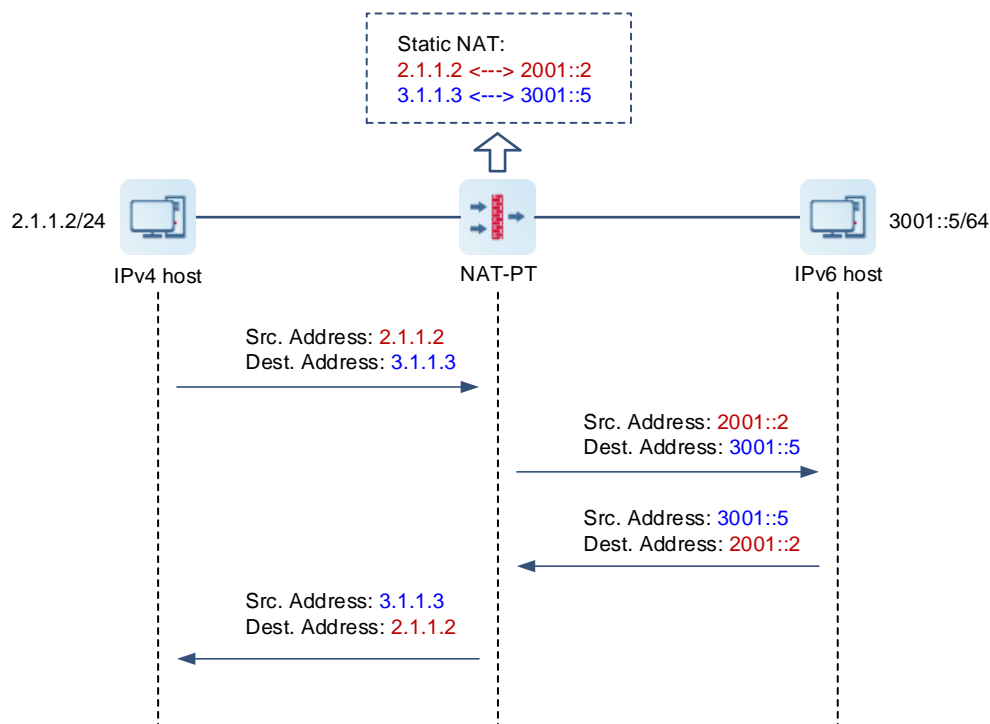
Network Address Translation-Protocol Translation (NAT-PT) enables communication between IPv6 and IPv4 networks. It integrates and evolves from Stateless IP/ICMP Translation (SIIT) and Network Address Translation (NAT). SIIT provides 1:1 mapping for translation between IPv4 and IPv6 addresses. Based on SIIT, NAT-PT also supports N:1 mapping and N:N mapping for address translation.

NAT-PT falls into static and dynamic modes.

- Static NAT-PT

1:1 static mapping rules are manually configured to enable translation between IPv4 and IPv6 addresses. In a scenario where an IPv4 network node needs to access an IPv6 network node, an address mapping rule needs to be pre-configured on the NAT-PT device.

Figure 5-2 Example of the Static NAT-PT Working Process



In this example, an IPv4 host initiates an access request. The working process of static NAT-PT is as follows:

- (1) The IPv4 host sends an IPv4 packet to the IPv6 host through the NAT-PT device.
- (2) After receiving the packet from the IPv4 host, the NAT-PT device translates the source and destination IPv4 addresses into the corresponding IPv6 addresses according to the configured mapping rule, and then sends the packet to the destination IPv6 host.
- (3) The IPv6 host responds based on the source IPv6 address, and sends an IPv6 packet to the NAT-PT device.
- (4) After receiving the IPv6 packet, the NAT-PT device translates the source and destination IPv6 addresses into the corresponding IPv4 addresses and returns it to the IPv4 host.

- Dynamic NAT-PT

The dynamic NAT-PT process is similar to that of static NAT-PT. The difference is that mappings between IPv6 and IPv4 addresses are dynamically generated and variable in dynamic NAT-PT. After receiving an IPv6 packet from an IPv6 host, the NAT-PT device modifies the header by replacing the destination IPv6 address with a specified destination IPv4 address and replacing the source IPv6 address with an available address in the defined IPv4 address pool.

Dynamic NAT-PT also supports Network Address Port Translation-Protocol Translation (NAPT-PT) for translating both network addresses and port numbers simultaneously. In this way, one IPv4 address can be mapped to different IPv6 addresses based on port numbers, thereby increasing the scope of address translation and reducing IPv4 address space.

3. NAT64

NAT-PT enables communication between IPv6 and IPv4 networks through network address and protocol translation. However, NAT-PT has many limitations. For example, it cannot translate the option in the IPv4

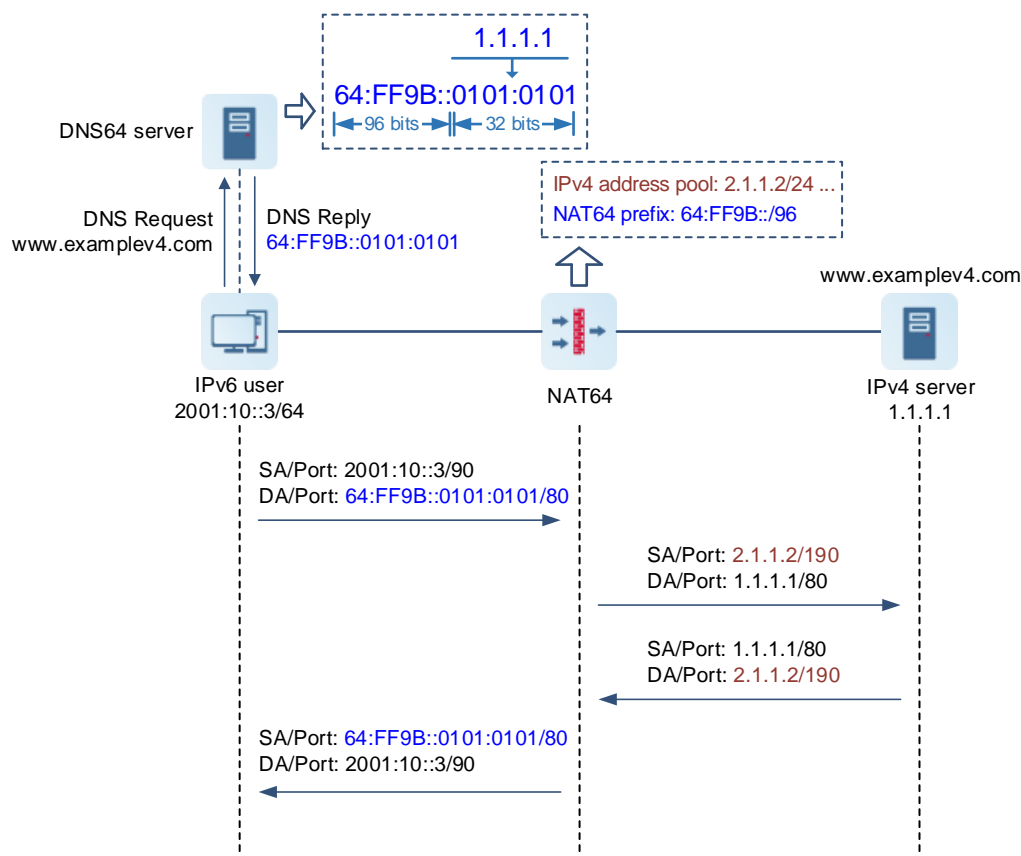
header or provide end-to-end security. To eliminate the limitations in NAT-PT, the Internet Engineering Task Force (IETF) designed a new solution: NAT64 and DNS64.

NAT64 falls into dynamic and static modes.

- Dynamic NAT64

Dynamic NAT64 only applies to scenarios where an IPv6 host initiates a request to access an IPv4 host (for example, an IPv6 user needs to access an IPv4 server). The NAT64 device creates a session table when receiving IPv6-to-IPv4 traffic and records the address mapping. When IPv4-to-IPv6 traffic matches the session table, a reply is sent according to the reverse address mapping.

Figure 5-3 Example of the Dynamic NAT64 Working Process



In this example, an IPv6 user initiates a request to access an IPv4 server. The working process of dynamic NAT64 is as follows:

- (1) The IPv6 user initiates an AAAA request (`www.examplev4.com`) to a DNS64 server to obtain an IPv6 address that corresponds to the IPv4 server domain name.
- (2) After receiving the AAAA request, the DNS64 server resolves the request packet and finds that the server address is an IPv4 address. Based on the configured NAT64 prefix `64:ff9b::/96`, it forms the NAT64 address `64:ff9b::0101:0101`, and sends it to the IPv6 user.
- (3) After receiving the reply packet from the DNS64 server, the IPv6 user initiates an access request to the IPv4 server with the resolved address as the destination address.
- (4) After receiving the IPv6 packet from the IPv6 user, the NAT64 device extracts the destination IPv4 address `1.1.1.1` based on the NAT64 prefix, and obtains a source IPv4 address `2.1.1.2` from the NAT address pool

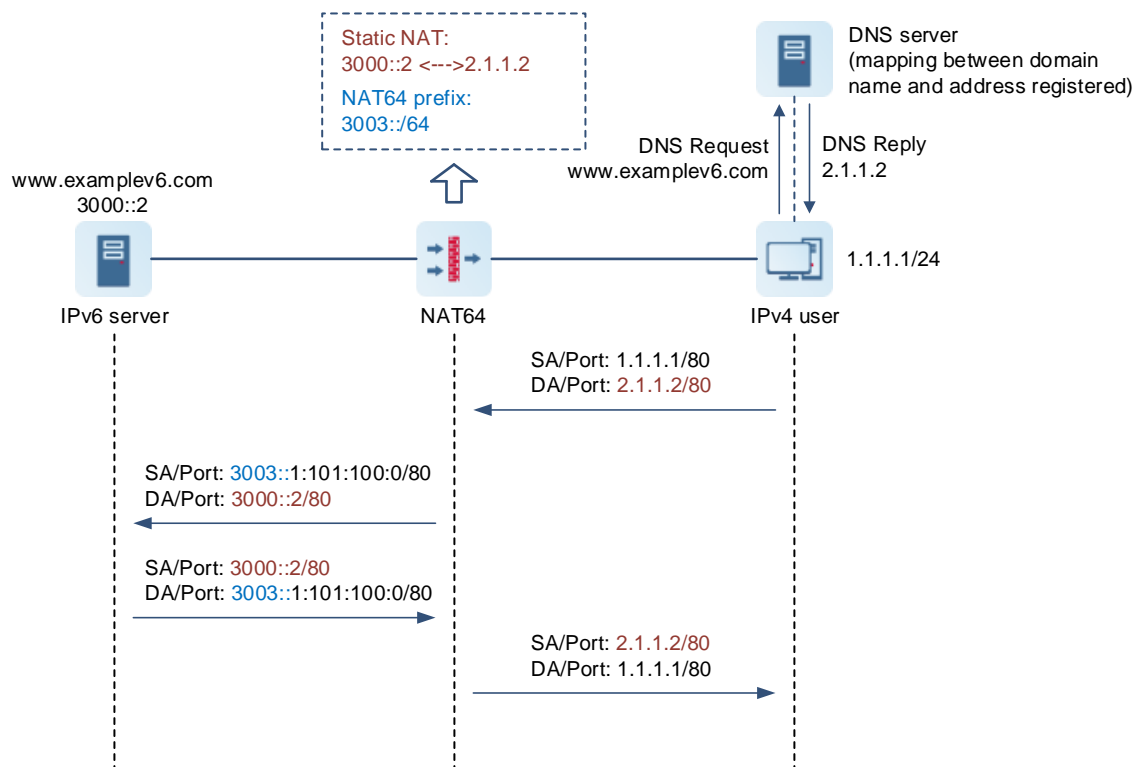
according to the mapping relationship configured in the NAT64 policy. In this way, the IPv6 packet is converted into an IPv4 packet.

- (5) The NAT64 device sends the IPv4 packet to the IPv4 server and creates a session table for storing the mappings between the IPv6 and IPv4 addresses.
- (6) After receiving the packet, the IPv4 server returns a reply packet. After receiving the reply packet from the IPv4 server, the NAT64 device converts the IPv4 packet into an IPv6 packet according to the mappings recorded in the session table, and then sends the IPv6 packet to the IPv6 user.

- Static NAT64

The mappings between IPv6 and IPv4 addresses are manually configured so that both IPv4-to-IPv6 traffic and IPv6-to-IPv4 traffic trigger the creation of a session table. Therefore, static NAT64 also applies to the scenario where an IPv4 host needs to access an IPv6 host, as well as the IPv6-to-IPv4 scenario.

Figure 5-4 Example of the Static NAT64 Working Process



In this example, an IPv4 user initiates a request to access an IPv6 server, and the working process of static NAT64 is as follows:

- (1) The IPv4 user initiates an A request (**www.examplev6.com**) to a DNS server to obtain the IPv4 address 2.1.1.2 that corresponds to the IPv6 server domain name. (Typically, the mapping between the domain name and address has been pre-configured on the DNS server.) Then, the IPv4 user initiates an access request to the IPv6 server with 2.1.1.2 as the destination address.
- (2) After receiving the IPv4 packet from the IPv4 user, the NAT64 device translates the destination IPv4 address to a destination IPv6 address according to the static mapping relationship configured in the NAT64 policy, and forms the source IPv6 address 3003:0000:0000:0000:0001:0101:0100:0000 based on the source IPv4 address and configured NAT64 prefix. In this way, the IPv4 packet is converted into an IPv6 packet.

- (3) The NAT64 device sends the IPv6 packet to the IPv6 server and creates a session table for storing the mappings between the IPv4 and IPv6 addresses.
- (4) After receiving the packet, the IPv6 server returns a reply packet. After receiving the reply packet from the IPv6 server, the NAT64 device converts the IPv6 packet into an IPv4 packet according to the mappings recorded in the session table, and then sends the IPv4 packet to the IPv4 user.

4. NPTv6

NAT66 refers to translation between IPv6 addresses, and IPv6-to-IPv6 Network Prefix Translation (NPTv6) is an implementation of NAT66. NPTv6 replaces the IPv6 address prefix in the packet header with another IPv6 address prefix with the same length to achieve IPv6 address translation.

NPTv6 provides two address translation modes:

- Source NPTv6: translates source IPv6 addresses for intranet hosts to access extranets.
- Destination NPTv6: translates destination IPv6 addresses for extranets to access services provided by intranet hosts.

5.5.4 Configuring NAT

NAT (NAT44) falls into the following three types.

NAT Type	NAT Content	Application Scenario
SNAT	Source IP address	Public IP addresses are sufficient and only a small number of private network users require Internet access. In this scenario, 1:1 translation of private IP addresses and public IP addresses is performed.
DNAT	Destination IP address	Public network users need to use public network addresses to access intranet servers.
Twice NAT	Source and destination IP addresses	Intranet PCs need to use public network addresses to access intranet servers.

1. Configuring an SNAT Policy

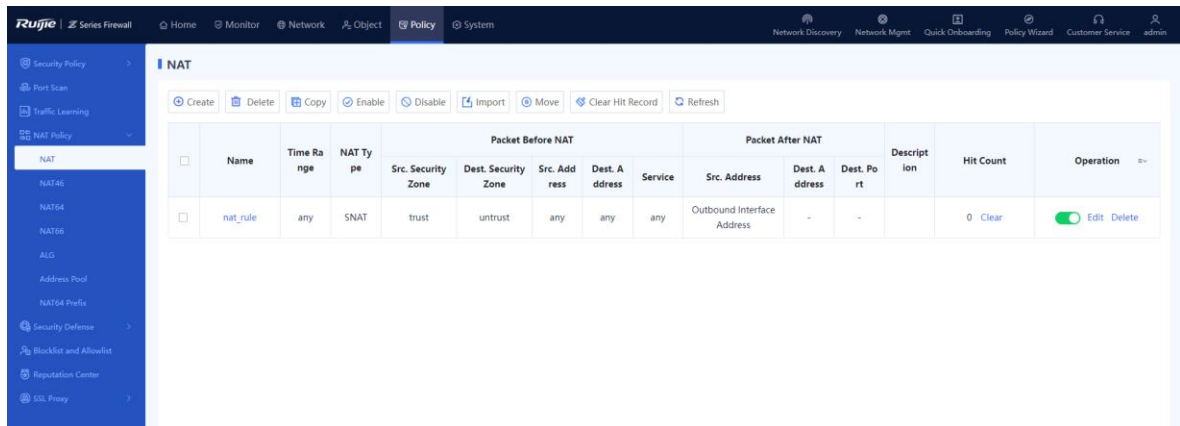
Application Scenario

SNAT refers to the translation of the source address in a packet, which is typically used for intranet hosts to access extranets.

SNAT translates private network IP addresses into public network IP addresses so that private network users can use public network addresses to access the Internet.

Procedure

- (1) Choose **Policy > NAT Policy > NAT**.



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

The **Add NAT** page is displayed.

< Back

Add NAT

NAT Mode

NAT Mode SNAT DNAT Twice Nat

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. Security Zone

* Dest. Address

* Service

Packet After NAT

Src. Address Translated to Address Pool Designated IP Outbound Interface Address

* Address Pool [⊕ Add Address Pool](#)

(3) Configure an SNAT policy.

The following table lists the configuration parameters for the SNAT policy.

Item	Description	Remarks
NAT Type		
NAT Type	NAT type. <ul style="list-style-type: none"> ● SNAT: source address translation ● DNAT: destination address translation ● Twice NAT: source and destination address translation 	[Example] SNAT

Item	Description	Remarks
Basic Info		
Name	Name of the NAT policy.	Characters such as `~!#%^&*+ \{ };:/'<>? and spaces are not allowed. [Example] NAT_policy_1
Enabled State	Whether to enable the NAT policy immediately after configuration is completed.	[Example] Enable
Description	Description of the NAT policy.	Characters such as `~!#%^&*+ \{ };:/'<>? are not allowed. [Example] NAT_policy_1
Time Range	Time range in which the NAT policy is effective.	<ul style="list-style-type: none"> ● Select a time range from the drop-down list. ● The default value is any. ● To add a time plan, click Add One-Off Time Plan or Add Cyclic Time Plan. [Example] any
Packet Before NAT		
Src. Security Zone	NAT is performed for packets from these security zones.	[Example] any
Src. Address	NAT is performed for packets from these addresses.	[Example] any
Dest. Security Zone	NAT is performed for packets sent to these security zones.	[Example] any
Dest. Address	NAT is performed for packets sent to these addresses.	[Example] any
Service	NAT is performed for packets of these services.	[Example] any
Packet After NAT		

Item	Description	Remarks
Src. Address Translated to	<p>Select the translated source address type based on the scenario. Valid values:</p> <ul style="list-style-type: none"> ● Address Pool Set an address pool. ● Designated IP Set an IP address. ● Outbound Interface Address 	[Example] Address Pool

(4) Click **Save**.

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**.
- To copy the content of a NAT policy, select the policy and click **Copy**. The NAT policy creation page is displayed, and the configuration parameters are automatically set.
- To move a NAT policy, select the policy and click **Move**. The closer a policy is to the front, the higher its priority is in matching.

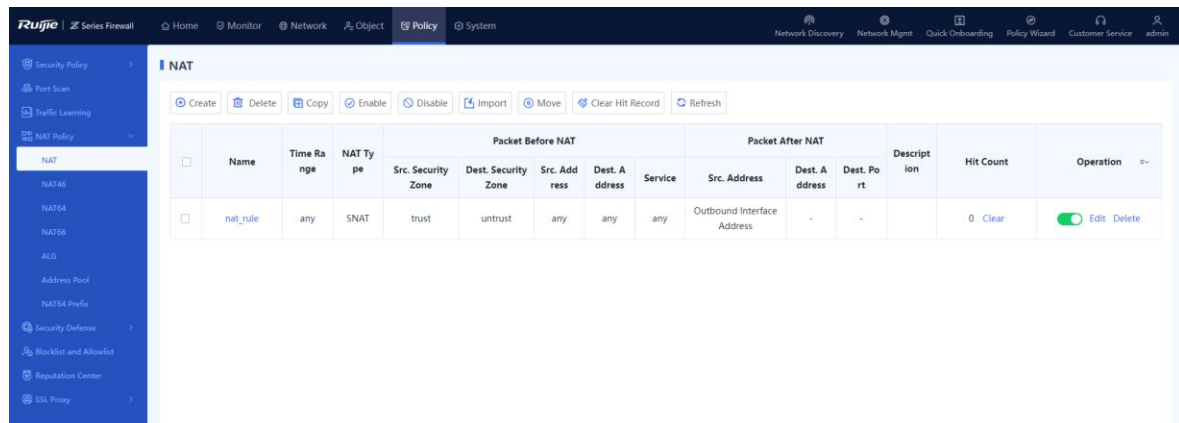
2. Configuring a DNAT Policy

Application Scenario

DNAT refers to the translation of the destination address and port number in a packet, which is typically used to map intranet servers for extranets. DNAT translates public network IP addresses into private network IP addresses so that public network users can use public network addresses to access intranet servers.

Procedure

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



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

The **Add NAT** page is displayed.

< Back

Add NAT

NAT Mode

NAT Mode SNAT DNAT Twice Nat

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

(3) Configure a DNAT policy.

The following table lists the configuration parameters for the DNAT policy.

Item	Description	Remarks
NAT Type		

Item	Description	Remarks
NAT Type	NAT type. <ul style="list-style-type: none"> ● SNAT: source address translation ● DNAT: destination address translation ● Twice NAT: source and destination address translation 	[Example] DNAT
Basic Info		
Name	Name of the NAT policy.	Characters such as `~!#%^&*+ \{ } ; : " ' / < > ?` and spaces are not allowed. [Example] NAT_policy_1
Enabled State	Whether to enable the NAT policy immediately after configuration is completed.	[Example] Enable
Description	Description of the NAT policy.	Characters such as `~!#%^&*+ \{ } ; : " ' / < > ?` are not allowed. [Example] NAT_policy_1
Time Range	Time range in which the NAT policy is effective.	<ul style="list-style-type: none"> ● The default value is any. You can also select a configured time plan from the drop-down list. ● To add a time plan, click Add One-Off Time Plan or Add Cyclic Time Plan. [Example] any
Packet Before NAT		
Src. Security Zone	NAT is performed for packets from these security zones.	[Example] any
Src. Address	NAT is performed for packets from these addresses.	[Example] any
Dest. Security Zone	NAT is performed for packets sent to these security zones.	[Example] any
Dest. Address	NAT is performed for packets sent to these addresses.	[Example] any
Service	NAT is performed for packets of these services.	[Example] any

Item	Description	Remarks
Packet After NAT		
IP	Translated destination IP address.	[Example] 192.168.10.30
Port	Translated destination port number.	[Example] 80

(4) Click **Save**.

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**.
- To copy the content of a NAT policy, select the policy and click **Copy**. The NAT policy creation page is displayed, and the configuration parameters are automatically set.
- To move a NAT policy, select the policy and click **Move**. The closer a policy is to the front, the higher its priority is in matching.

3. Configuring a Twice NAT Policy

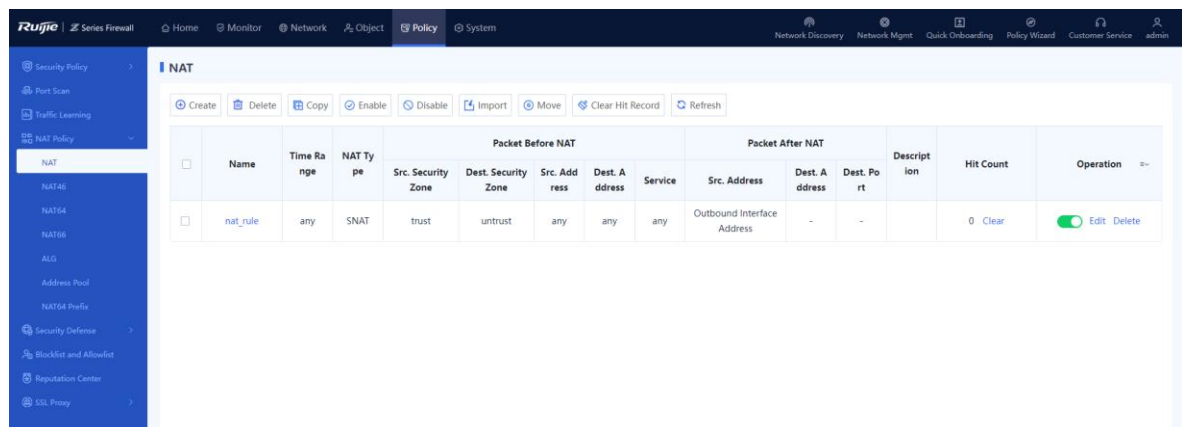
Application Scenario

Twice NAT translates both source and destination information of a packet. By combining SNAT and DNAT, Twice NAT translates the source and destination addresses in a packet simultaneously when the data flow passes through the firewall.

It applies to a scenario where intranet PCs need to use public network addresses to access intranet servers.

Procedure

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



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

The **Add NAT** page is displayed.

< Back

Add NAT

NAT Mode

NAT Mode SNAT DNAT Twice Nat

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 v

* Src. Address v

* Dest. Address v

* Service v

Packet After NAT

Src. Address Translated to Address Pool Designated IP Outbound Interface Address

* Address Pool [⊕ Add Address Pool](#)

* Dest. Address
Translated to

[ⓘ](#) Dest. Port Number
Translated to

(3) Configure a twice NAT policy.

Configure the NAT policy as required.

The following table lists the configuration parameters for the twice policy.

Item	Description	Remarks
NAT Type		
NAT Type	NAT type. <ul style="list-style-type: none"> ● SNAT: source address translation ● DNAT: destination address translation ● Twice NAT: source and destination address translation 	[Example] Twice NAT
Basic Info		
Name	Name of the NAT policy.	Characters such as `~!#%^&*+ \{};:~"/<>?` and spaces are not allowed. [Example] NAT_policy_1
Enabled State	Whether to enable the NAT policy immediately after configuration is completed.	[Example] Enable
Description	Description of the NAT policy.	Characters such as `~!#%^&*+ \{};:~"/<>?` are not allowed. [Example] NAT_policy_1
Time Range	Time range in which the NAT policy is effective.	<ul style="list-style-type: none"> ● The default value is any. You can also select a configured time plan from the drop-down list. ● To add a time plan, click Add One-Off Time Plan or Add Cyclic Time Plan. [Example] any
Packet Before NAT		
Src. Security Zone	NAT is performed for packets from these security zones.	[Example] any
Src. Address	NAT is performed for packets from these addresses.	[Example] any
Dest. Security Zone	NAT is performed for packets sent to these security zones.	[Example] any
Dest. Address	NAT is performed for packets sent to these addresses.	[Example] any

Item	Description	Remarks
Service	NAT is performed for packets of these services.	[Example] any
Packet After NAT		
Src. Address Translated to	Select the translated source address type based on the scenario. Valid values: <ul style="list-style-type: none"> ● Address Pool Set an address pool. ● Designated IP Set an IP address. ● Outbound Interface Address 	[Example] Address Pool
Dest. Address Translated to	Translated destination IP address.	[Example] 192.168.10.30
Dest. Port Number Translated to	Translated destination port number.	[Example] 80

(4) Click **Save**.

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**.
- To copy the content of a NAT policy, select the policy and click **Copy**. The NAT policy creation page is displayed, and the configuration parameters are automatically set.
- To move a NAT policy, select the policy and click **Move**. The closer a policy is to the front, the higher its priority is in matching.

4. Importing Configuration Files to Configure NAT

Application Scenario

Z-S series firewalls support fast generation of security policies based on imported configuration files.

Prerequisites

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.

Note

For the usage of the policy migration tool, contact technical support engineers.

Procedure

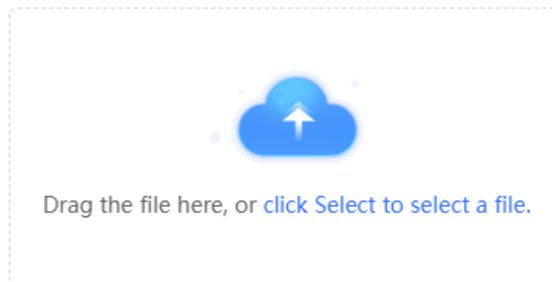
- (1) Choose **Policy > NAT Policy > NAT**.
- (2) In the operation area, click **Import**.

A tip dialog box is displayed.

Tip

Note 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.

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 **click Select to select a file** 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 following handling methods can be used:

- **Display Conflicting Data:** 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.

5.5.5 Configuring NAT46

Application Scenario

Configure a NAT46 policy to translate source and destination addresses in IPv4 packets to IPv6 addresses, thereby enabling IPv4 hosts to access IPv6 networks.

Procedure

(1) Choose **Policy > NAT Policy > NAT46**.

	Name	NAT Type	Packet Before NAT			Packet After NAT				Hit Count	Description	Operation	≡
			Src. Address	Dest. Address	Service	NAT64 Prefix	Src. Address Translated to	Dest. Address Translated to	Dest. Port Number Translated to				
No Data													

(2) Click **Create**. The **Add IPv4-to-IPv6 NAT** page is displayed.

< Back

Add IPv4-to-IPv6 NAT

Basic Info

* Name

Enabled State Enable Disable

Description

Packet Before NAT

* Src. Address

* Dest. Address

* Service

Packet After NAT

NAT Mode Stateless NAT64 Static NAT-PT Static NAT64

* NAT64 Prefix [⊕ Create NAT64 Prefix](#)

[IP Address NAT Tool](#)

(3) Configure a NAT46 policy. The following table lists the configuration parameters.

Item	Description	Remarks
Basic Info		
Name	Name of the NAT46 policy.	Characters such as `~!#%^&*+ \ {};:'"/<>?` and spaces are not allowed. [Example] NAT46_policy_1
Enabled State	Whether to enable the NAT46 policy immediately after configuration is completed.	[Example] Enable

Item	Description	Remarks
Description	Description of the NAT46 policy.	Characters such as `~!#%^&*+ {};:'"/<>? are not allowed. [Example] NAT46 policy_1
Packet Before NAT		
Src. Address	NAT is performed for packets from these addresses.	<ul style="list-style-type: none"> ● Click the drop-down list, and select an associated IPv4 address object in the To-be-selected area. The selected object is automatically added to the Selected area. ● Click Add Address to create an IPv4 address object for the source address. ● Click Add Address Group to create a source IPv4 address group object that contains multiple IPv4 address objects.
Dest. Address	NAT is performed for packets sent to these addresses.	<ul style="list-style-type: none"> ● Click the drop-down list, and select an associated IPv4 address object in the To-be-selected area. The selected object is automatically added to the Selected area. ● Click Add Address to create an IPv4 address object for the destination address. ● Click Add Address Group to create a destination IPv4 address group object that contains multiple IPv4 address objects.
Service	NAT is performed for packets of these services.	<ul style="list-style-type: none"> ● Click Add Service to create a custom service. ● Click Add Service Group to create a custom service group that contains multiple services. [Example] any
Packet After NAT		
NAT Mode	NAT46 implementation mode. Valid values: <ul style="list-style-type: none"> ● Stateless NAT64 ● Static NAT-PT ● Static NAT64 	For different implementation modes, you need to configure different parameters. [Example] Stateless NAT64
NAT Mode: Stateless NAT64.		

Item	Description	Remarks
NAT64 Prefix	NAT64 prefix for forming an IPv6 address. In stateless NAT64, the translated source and destination IPv6 addresses are formed by combining the NAT64 prefix and IPv4 address.	<ul style="list-style-type: none"> ● Click the drop-down list, and select a NAT64 prefix. ● Click Create NAT64 Prefix to create a NAT64 prefix. [Example] 3001:db8::/64
NAT Mode: Static NAT-PT		
NAT64 Prefix	In NAT-PT, after receiving an IPv6 packet, the NAT-PT device checks the prefix of the destination IPv6 address in the packet. IPv6-to-IPv4 translation is performed only for packets with a prefix same as the configured NAT64 prefix.	<ul style="list-style-type: none"> ● Click the drop-down list, and select a NAT64 prefix. ● Click Create NAT64 Prefix to create a NAT64 prefix. ● The prefix must be the same as that of the translated source address. [Example] 3001:db8::/64
Src. Address Translated to	Source IPv6 address translated from the source IPv4 address in an IPv4 packet.	The prefix in the translated source IPv6 address must be the same as the NAT64 prefix. [Example] 3001:db8::5
Dest. Address Translated to	Destination IPv6 address translated from the destination IPv4 address in an IPv4 packet.	Enter the destination IPv6 address to be translated to. [Example] 2001::2
NAT Mode: Static NAT64		
NAT64 Prefix	NAT64 prefix for forming an IPv6 address. In static NAT64, the translated source IPv6 address is formed by combining the NAT64 prefix and source IPv4 address.	<ul style="list-style-type: none"> ● Click the drop-down list, and select a NAT64 prefix. ● Click Create NAT64 Prefix to create a NAT64 prefix. [Example] 3001:db8::/64
Dest. Address Translated to	Destination IPv6 address translated from the destination IPv4 address in an IPv4 packet.	Enter the destination IPv6 address to be translated to. [Example] 2001::2

Item	Description	Remarks
Dest. Port Number Translated to	Destination port number translated from the destination port number in an IPv4 packet.	<ul style="list-style-type: none"> Optional. This parameters specifies the port number translation mode. The destination port number is not translated if it is left blank. [Example] 90

- (4) (Optional) Click **IP Address NAT Tool** to quickly calculate the translated IPv4 or IPv6 address. You can use this tool to translate the input IPv6 address to an IPv4 address based on the configured NAT64 prefix using the standard NAT64 translation algorithm and vice versa.

Packet After NAT

NAT Mode Stateless NAT64 Static NAT-PT Static NAT64

* NAT64 Prefix [Create NAT64 Prefix](#)

[IP Address NAT Tool](#)

IP Address NAT Tool ⊗

i Translate the input IPv6 address to an IPv4 address based on the configured NAT64 prefix using the standard NAT64 translation algorithm and vice versa.

* IPv6 Address

* IPv4 Address

- (5) Click **Save**.

Follow-up Procedure

- The NAT policy list displays the configuration information and hit count of the policy. You can click **Clear**, or select policies and click **Clear Hit Record** to clear the hit statistics for the specified policies.
- 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**.
- To copy the content of a NAT policy, select the policy and click **Copy**. The policy copy page is displayed, and the configuration parameters are automatically set.
- To move a NAT policy, select the policy and click **Move**. The closer a policy is to the front, the higher its priority is in matching.

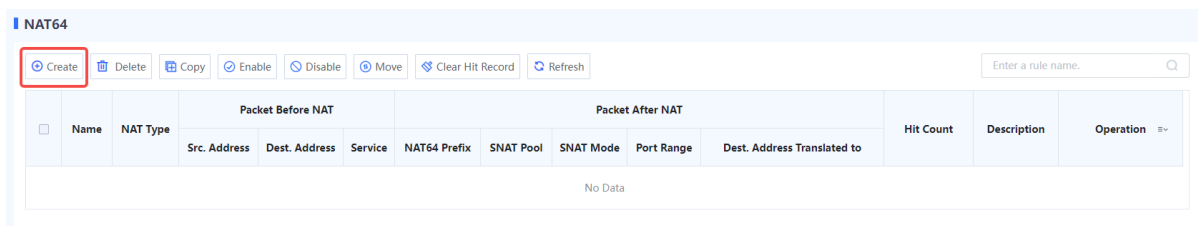
5.5.6 Configuring NAT64

Application Scenario

Configure a NAT64 policy to translate source and destination addresses in IPv6 packets to IPv4 addresses, thereby enabling IPv6 hosts to access IPv4 networks.

Procedure

- (1) Choose **Policy > NAT Policy > NAT64**.



- (2) Click **Create**. The **Add IPv6-to-IPv4 NAT** page is displayed.

< Back
Add IPv6-to-IPv4 NAT

Basic Info

* Name

Enabled State Enable Disable

Description

Packet Before NAT

* Src. Address

* Dest. Address

* Service

Packet After NAT

NAT Mode Dynamic NAT-PT Dynamic NAT64

* NAT64 Prefix [⊕ Create NAT64 Prefix](#)

* Translate Src. [⊕ Add Address Pool](#)

Address to Address
in Address Pool

SNAT Mode NO-PAT PAT

* Dest. Address

Translated to

Save

(3) Configure a NAT64 policy. The following table lists the configuration parameters.

Item	Description	Remarks
Basic Info		
Name	Name of the NAT64 policy.	Characters such as `~!#%^&*+\\{ };:'''/<>?` and spaces are not allowed. [Example] NAT64_policy_1
Enabled State	Whether to enable the NAT64 policy immediately after configuration is completed.	[Example] Enable
Description	Description of the NAT64 policy.	Characters such as `~!#%^&*+\\{ };:'''/<>?` are not allowed. [Example] NAT64_policy_1

Item	Description	Remarks
Packet Before NAT		
Src. Address	NAT is performed for packets from these addresses.	<ul style="list-style-type: none"> ● Click the drop-down list, and select an associated IPv6 address object in the To-be-selected area. The selected object is automatically added to the Selected area. ● Click Add Address to create an IPv6 address object for the source address. ● Click Add Address Group to create a source IPv6 address group object that contains multiple IPv6 address objects.
Dest. Address	<p>NAT is performed for packets sent to these addresses.</p> <p>Enter the destination IPv6 address in the NAT64 prefix and IPv4 address format, which is calculated from the destination IPv4 address using the standard NAT64 translation algorithm.</p> <p>Example: If the NAT64 prefix is 3001:db8::/64 and the destination IPv4 server address is 2.1.1.2, the destination IPv6 address should be set to 3001:db8::2:101:200:0.</p>	<ul style="list-style-type: none"> ● Click the drop-down list, and select an associated IPv6 address object in the To-be-selected area. The selected object is automatically added to the Selected area. ● Click Add Address to create an IPv6 address object for the destination address. ● Click Add Address Group to create a destination IPv6 address group object that contains multiple IPv6 address objects.
Service	NAT is performed for packets of these services.	<ul style="list-style-type: none"> ● Click Add Service to create a custom service. ● Click Add Service Group to create a custom service group that contains multiple services. <p>[Example]</p> <p>any</p>
Packet After NAT		
NAT Mode	<p>NAT64 implementation mode. Valid values:</p> <ul style="list-style-type: none"> ● Dynamic NAT-PT ● Dynamic NAT64 	<p>For different implementation modes, you need to configure different parameters.</p> <p>[Example]</p> <p>Dynamic NAT64</p>
NAT Mode: Dynamic NAT-PT		

Item	Description	Remarks
NAT64 Prefix	In NAT-PT, after receiving an IPv6 packet, the NAT-PT device checks the prefix of the destination IPv6 address in the packet. IPv6-to-IPv4 translation is performed only for packets with a prefix same as the configured NAT64 prefix.	<ul style="list-style-type: none"> Click the drop-down list, and select a NAT64 prefix. Click Create NAT64 Prefix to create a NAT64 prefix. [Example] 3001:db8::/64
Translate Src. Address to Address in Address Pool	IPv4 address pool for translating source IPv6 addresses. The device obtains an available IPv4 address from the pool as the IPv4 address translated from the source IPv6 address.	<ul style="list-style-type: none"> Click the drop-down list, and select an address pool. Click Add Address Pool to create a custom address pool. [Example] nat_pool_1
SNAT Mode	Whether to translate the transport-layer source port numbers in packets: <ul style="list-style-type: none"> NO-PAT: The source port number is not translated and remains the same in the packets before and after the translation. PAT: Both the source address and source port number are translated so that one IPv4 address can be shared by multiple IPv6 addresses. 	If SNAT Mode is set to PAT , you need to specify a range for translated source port numbers. [Example] PAT
Port Number Range	Range of translated source port numbers in PAT mode.	[Example] 60000-65000
Dest. Address Translated to	Destination IPv4 address translated from the destination IPv6 address in an IPv6 packet.	Enter the destination IPv4 address to be translated to. [Example] 2.1.1.3
NAT Mode: Dynamic NAT64		
NAT64 Prefix	NAT64 prefix for forming an IPv6 address. In dynamic NAT64, the IPv4 address is extracted from the destination IPv6 address of the IPv6 packet based on the NAT64 prefix.	<ul style="list-style-type: none"> Click the drop-down list, and select a NAT64 prefix. Click Create NAT64 Prefix to create a NAT64 prefix. [Example] 3001:db8::/64

Item	Description	Remarks
Translate Src. Address to Address in Address Pool	IPv4 address pool for translating source IPv6 addresses. The device obtains an available IPv4 address from the pool as the IPv4 address translated from the source IPv6 address.	<ul style="list-style-type: none"> Click the drop-down list, and select an address pool. Click Add Address Pool to create a custom address pool. [Example] nat_pool_1
SNAT Mode	Whether to translate the transport-layer source port numbers in packets: <ul style="list-style-type: none"> NO-PAT: The source port number is not translated and remains the same in the packets before and after the translation. PAT: Both the source address and source port number are translated so that one IPv4 address can be shared by multiple IPv6 addresses. 	If SNAT Mode is set to PAT , you need to specify a range for translated source port numbers. [Example] PAT
Port Number Range	Range of translated source port numbers in PAT mode.	[Example] 60000-65000

(4) Click **Save**.

Follow-up Procedure

- The NAT policy list displays the configuration information and hit count of the policy. You can click **Clear**, or select policies and click **Clear Hit Record** to clear the hit statistics for the specified policies.
- 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**.
- To copy the content of a NAT policy, select the policy and click **Copy**. The policy copy page is displayed, and the configuration parameters are automatically set.
- To move a NAT policy, select the policy and click **Move**. The closer a policy is to the front, the higher its priority is in matching.

5.5.7 Configuring NAT66

1. Configuring Source NPTv6

Application Scenario

Source NPTv6 translates source IPv6 addresses in IPv6 packets for intranet hosts to access extranets.

Procedure

(1) Choose **Policy > NAT Policy > NAT66**.

NAT66

□	Name	NAT Type	Packet Before NAT			Packet After NAT	Hit Count	Status	Description	Operation
			Src. Address	Dest. Address	Service	NPT Info				
No Data										

(2) Click **Create**. The **Add NAT66** page is displayed.

[Back](#) **Add NAT66**

NAT Mode

NAT Mode Source NPTv6 Destination NPTv6

Basic Info

* Name

Enabled State Enable Disable

Description

Packet Before NAT

* Src. Address

* Dest. Address

* Service

Packet After NAT

* NPT Info

(3) Set **NAT Type** to **Source NPTv6** to configure a source NPTv6 policy. The following table lists the configuration parameters.

Item	Description	Remarks
NAT Type		
NAT Type	NAT66 translation mode.	[Example] Source NPTv6
Basic Info		
Name	Name of the NAT66 policy.	Characters such as `~!#%^&*+ {};:'"/<>? and spaces are not allowed. [Example] NPTv6_policy_1
Enabled State	Whether to enable the policy immediately after configuration is completed.	[Example] Enable
Description	Policy description.	Characters such as `~!#%^&*+ {};:'"/<>? are not allowed. [Example] NPTv6_policy1
Packet Before NAT		
Src. Address	NAT is performed for packets from these addresses.	<ul style="list-style-type: none"> Click the drop-down list, and select an associated IPv6 address object in the To-be-selected area. The selected object is automatically added to the Selected area. Click Add Address to create an IPv6 address object for the source address. Click Add Address Group to create a source IPv6 address group object that contains multiple IPv6 address objects.
Dest. Address	NAT is performed for packets sent to these addresses.	<ul style="list-style-type: none"> Click the drop-down list, and select an associated IPv6 address object in the To-be-selected area. The selected object is automatically added to the Selected area. Click Add Address to create an IPv6 address object for the destination address. Click Add Address Group to create a destination IPv6 address group object that contains multiple IPv6 address objects.
Service	NAT is performed for packets of these services.	<ul style="list-style-type: none"> Click Add Service to create a custom service. Click Add Service Group to create a custom service group that contains multiple services. [Example] any
Packet After NAT		

Item	Description	Remarks
NPT Info	Translated source IPv6 address prefix. After this policy is delivered, the source IPv6 address prefix in the original IPv6 packet is replaced with this IPv6 address prefix.	<ul style="list-style-type: none"> Enter a valid IPv6 address prefix and prefix length. The following values are not allowed: <ul style="list-style-type: none"> Loopback address: 0:0:0:0:0:0:1 or ::1 Link-local address: addresses with a prefix of FE80:: Multicast address: IPv6 addresses in the range of FF00::/8–FFFF::/8, that is, addresses starting with FF Invalid address The translated prefix length must be the same as the length of the IPv6 address prefix of the source address object in the original packet. <p>[Example] 3003::/64</p>

(4) Click **Save**.

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**.
- To copy the content of a NAT policy, select the policy and click **Copy**. The policy copy page is displayed, and the configuration parameters are automatically set.
- To move a NAT policy, select the policy and click **Move**. The closer a policy is to the front, the higher its priority is in matching.

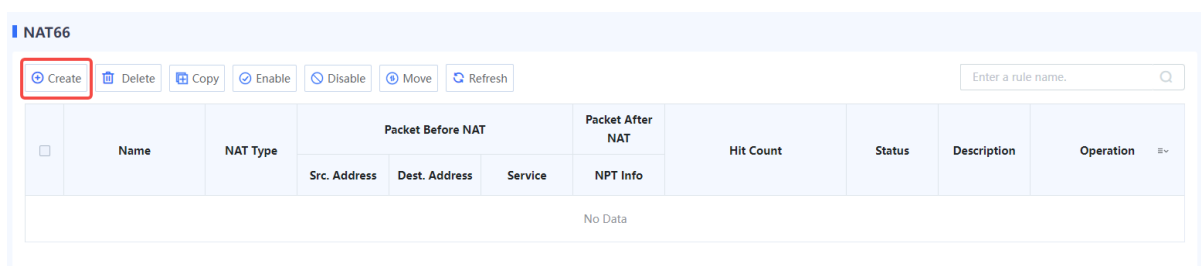
2. Configuring Destination NPTv6

Application Scenario

Destination NPTv6 translates destination IPv6 addresses in IPv6 packets for extranets to access services provided by intranet hosts.

Procedure

(1) Choose **Policy > NAT Policy > NAT66**.



(2) Click **Create**. The **Add NAT66** page is displayed.

< Back Add NAT66

NAT Mode

NAT Mode Source NPTv6 Destination NPTv6

Basic Info

* Name

Enabled State Enable Disable

Description

Packet Before NAT

* Src. Address

* Dest. Address

* Service

Packet After NAT

* ⓘ NPT Info

(3) Set **NAT Type** to **Destination NPTv6** to configure a destination NPTv6 policy. The following table lists the configuration parameters.

Item	Description	Remarks
NAT Type		
NAT Type	NAT66 translation mode.	[Example] Destination NPTv6
Basic Info		

Item	Description	Remarks
Name	Name of the NAT66 policy.	Characters such as `~!#%^&*+\\ {};:"'/<>?` and spaces are not allowed. [Example] NPTv6_policy_1
Enabled State	Whether to enable the policy immediately after configuration is completed.	[Example] Enable
Description	Policy description.	Characters such as `~!#%^&*+\\ {};:"'/<>?` are not allowed. [Example] NPTv6 policy1
Packet Before NAT		
Src. Address	NAT is performed for packets from these addresses.	<ul style="list-style-type: none"> ● Click the drop-down list, and select an associated IPv6 address object in the To-be-selected area. The selected object is automatically added to the Selected area. ● Click Add Address to create an IPv6 address object for the source address. ● Click Add Address Group to create a source IPv6 address group object that contains multiple IPv6 address objects.
Dest. Address	NAT is performed for packets sent to these addresses.	<ul style="list-style-type: none"> ● Click the drop-down list, and select an associated IPv6 address object in the To-be-selected area. The selected object is automatically added to the Selected area. ● Click Add Address to create an IPv6 address object for the destination address. ● Click Add Address Group to create a destination IPv6 address group object that contains multiple IPv6 address objects.
Service	NAT is performed for packets of these services.	<ul style="list-style-type: none"> ● Click Add Service to create a custom service. ● Click Add Service Group to create a custom service group that contains multiple services. [Example] any
Packet After NAT		

Item	Description	Remarks
NPT Info	Translated destination IPv6 address prefix. After this policy is delivered, the destination IPv6 address prefix in the original IPv6 packet is replaced with this IPv6 address prefix.	<ul style="list-style-type: none"> ● Enter a valid IPv6 address prefix and prefix length. The following values are not allowed: <ul style="list-style-type: none"> ○ Loopback address: 0:0:0:0:0:0:1 or ::1 ○ Link-local address: addresses with a prefix of FE80:: ○ Multicast address: IPv6 addresses in the range of FF00::/8–FFFF::/8, that is, addresses starting with FF ○ Invalid address ● The translated prefix length must be the same as the length of the IPv6 address prefix of the destination address object in the original packet. <p>[Example]</p> <p>3003::/64</p>

(4) Click **Save**.

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**.
- To copy the content of a NAT policy, select the policy and click **Copy**. The policy copy page is displayed, and the configuration parameters are automatically set.
- To move a NAT policy, select the policy and click **Move**. The closer a policy is to the front, the higher its priority is in matching.

5.5.8 Enabling the ALG Function

Application Scenario

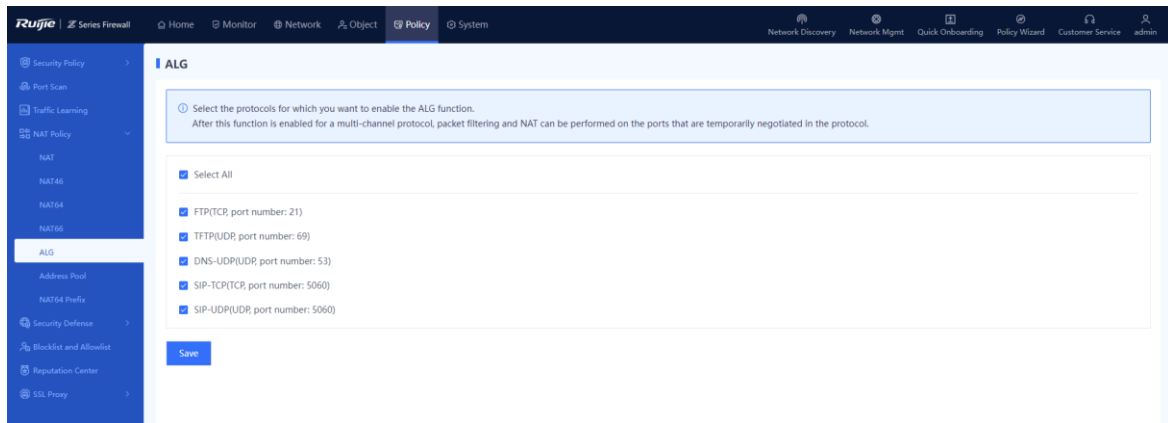
The application-level gateway (ALG) function is used to automatically detect application layer information for certain packets in a NAT scenario. Corresponding access rules are enabled (a server-map table is generated) based on the application layer information, and IP address and port information in the packet payload are automatically translated.

In regular NAT, only IP addresses and port numbers in packet headers are translated, and application layer data cannot be translated. However, packet payload that use application layer protocols may also contain address or port information. If this information is not translated, communication exceptions may occur.

After the ALG function is enabled, corresponding access rules can be enabled based on the application layer information, and NAT can be performed on application layer data.

Procedure

- (1) Choose **Policy > NAT Policy > ALG**.



(2) Select the protocol names for which ALG needs to be enabled and click **Save**.

(3) After the ALG function is enabled, information in the packets of these protocols can be translated by NAT.

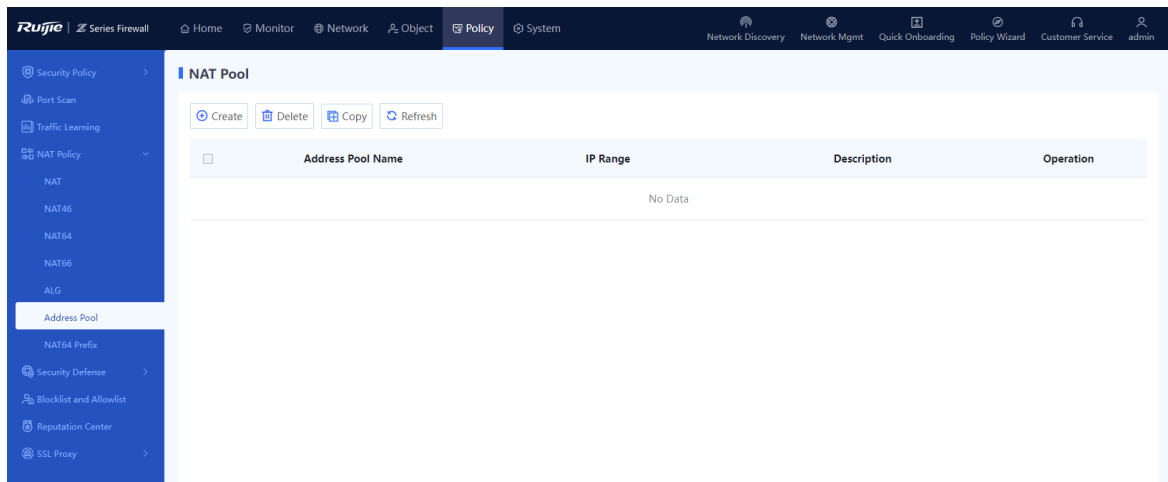
5.5.9 Configuring an Address Pool

Application Scenario

After an address pool is configured, the addresses in the pool can be selected when you set parameters of **Packet After NAT** for a NAT policy.

Procedure

(1) Choose **Policy > NAT Policy > Address Pool**.



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

The **Add NAT Pool** page is displayed.

(3) Enter the address pool name, and configure IP addresses or an IP address range.

(4) Click **Save**.

Follow-up Procedure

- After an address pool is configured for NAT, the configuration information is synchronized to proxy ARP. Proxy ARP is enabled for all the interfaces that correspond to the IP addresses in the pool.
- To copy the content of an existing address pool, select the pool and click **Copy**. The **Copy NAT Pool** page is displayed, and the configuration parameters are automatically set.
- To delete multiple address pools in a batch, select the address pools that you want to delete and click **Delete**.

5.5.10 Configuring NAT64 Prefixes

Application Scenario

The NAT64 prefix is an IPv6 address prefix with a length of 32, 40, 48, 56, 64 or 96 bits. It is used to construct an address of an IPv4 node on an IPv6 network in NAT46/NAT64, thereby enabling communication between IPv4 and IPv6 networks.

When configuring a NAT64 or NAT46 policy, you can reference the configured NAT64 prefix as the NAT64 prefix for NAT.

Procedure

(1) Choose **Policy > NAT Policy > NAT64 Prefix**.

(2) Click **Create**. The **Create NAT64 Prefix** page is displayed.

< Back
Create NAT64 Prefix

* Name

* 🔔 NAT64 Prefix

Prefix Length ▼

Save

(3) Configure a NAT64 prefix. The following table lists the configuration parameters.

Item	Description	Remarks
Name	NAT64 prefix name.	[Example] nat64prefix_1
NAT64 Prefix	Address of the NAT64 prefix.	Enter a valid IPv6 address. [Example] 3001:db8::
Prefix Length	NAT64 prefix length.	Click the drop-down list, and select a NAT64 prefix length. [Example] 64

(4) Click **Save**.

Follow-up Procedure

- To modify an existing NAT64 prefix, click **Edit**.
- To delete a NAT64 prefix, select the prefix and click **Delete**. To delete multiple NAT64 prefixes in a batch, select the prefixes and click **Delete**.

5.6 Security Defense

5.6.1 Overview

There may be many forms of attacks in customers' network environments, such as traffic-targeted DDoS attacks and packet- or protocol-targeted attacks (such as teardrop, smurf, and redirect attacks). The target may be a user on the intranet or the device itself. On the Z-S series firewall, you can configure security defense policies to help intranet users and devices defend against attacks:

DoS/DDoS attack defense: prevents various common scan attacks, protocol attacks, and flood attacks on the network.

Local defense: provides default policies to ensure the normal operation of the device.

ARP attack defense: provides static ARP configuration, proxy ARP, and anti-ARP spoofing functions on the intranet.

5.6.2 Attack Types

The following describes basic principles and characteristics of common network attacks. After understanding the basic principles of these attacks, you can enable security defense based on the actual network environment.

- 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.

- 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 attacks.

- Scan

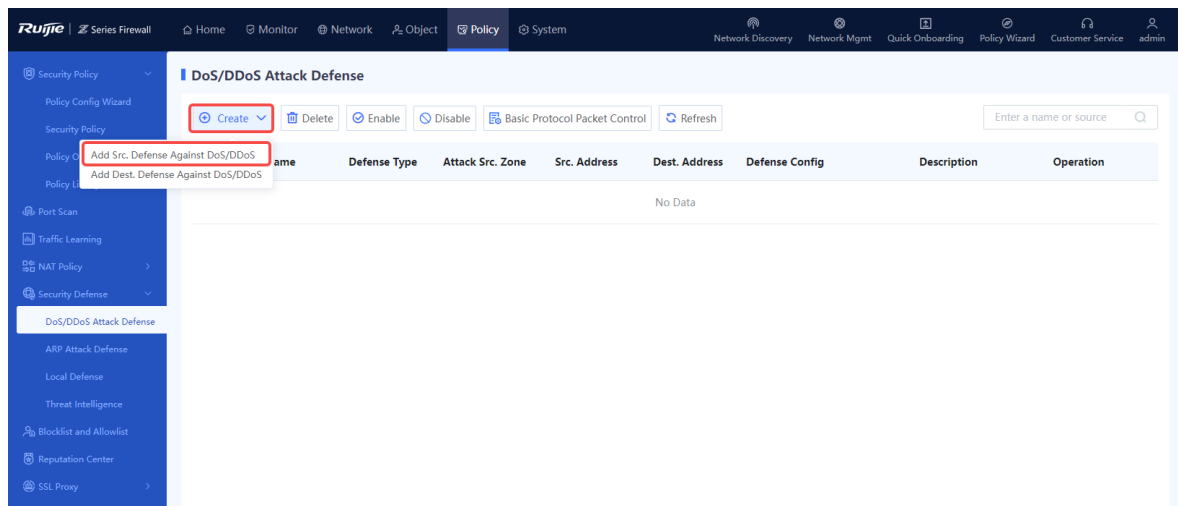
Scan attack is usually the first step in the attacker's attempt to the target host/network. By scanning ports/IP addresses, the attacker discovers the ports, services, and OS types in the target host/network, which is the basic information for further penetration or attack. By traffic analysis, you will 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.

5.6.3 Configuring DoS/DDoS Attack Defense

1. Configuring Source Defense Against DoS/DDoS

Procedure

(1) Choose **Policy > Security Defense > DoS/DDoS Attack Defense**.



(2) In the operation area, click **Create** and select **Add Src. Defense Against DoS/DDoS**.

The **Add Src. Defense Against DoS/DDoS** page is displayed.

< 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

Smurf Attack Defense

LAND Attack Defense

Large ICMP Packet Attack Defense

Control IP Packets with Source Routes

ICMP Redirect Attack Defense

WinNuke Attack Defense

Control IP Packets with Record Routes

ICMP Unreachable Attack Defense

Fraggle Attack Defense

Filtering out IPv6 Packets with Specific EHs

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

Item	Description	Remarks
Basic Info		
Name	Name of the DoS/DDoS attack defense policy.	Characters such as `~!#%^&*+ \{};:~/"<>? and spaces are not allowed. [Example] DoS_policy_1
Enabled State	Whether to enable the policy immediately after configuration is completed.	[Example] Enable
Description	Description of the DoS/DDoS attack defense policy.	Characters such as `~!#%^&*+ \{};:~/"<>? are not allowed. [Example] New policy

Item	Description	Remarks
Protected Host Range		
Range of the attack source associated with the policy. The policy takes effect when matching.		
Attack Src. Zone	After this policy is delivered, the device checks the traffic from this security zone.	[Example] any
Src. Address	After this policy is delivered, the device checks the traffic from this address set.	any indicates all addresses. [Example] any
Dest. Address	After this policy is delivered, the device checks the traffic to this address set.	any indicates all addresses. [Example] any
Defense Config		
Scan Attack Types		
IP Scan Defense	Whether IP scan defense is enabled.	[Example] Enabled
Limit (pps)	Threshold for detecting an IP scan attack and triggering defense.	[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 defense.	[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 attacks.	Click an attack defense type to enable defense against the specific attacks. [Example] SYN Flood Attack Defense: Enabled
Src. IP Blocking Limit (pps)	Global trigger threshold of flood attack defense.	[Example] 2000

Item	Description	Remarks
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: <ul style="list-style-type: none"> ● Log: Only record a security log, but not block traffic. ● Block: Only block traffic, but not record a security log. 	[Example] Log + Block
Advanced Defense		
Packet-based Attack	Whether defense against packet-based attacks is enabled.	[Example] All
Filtering out IPv6 Packets with Specific EHs	Filter out the IPv6 packets with the extended headers of the specified type.	[Example] Empty EHs

(4) Click **Save** to complete the configuration of DoS/DDoS attack defense policy.

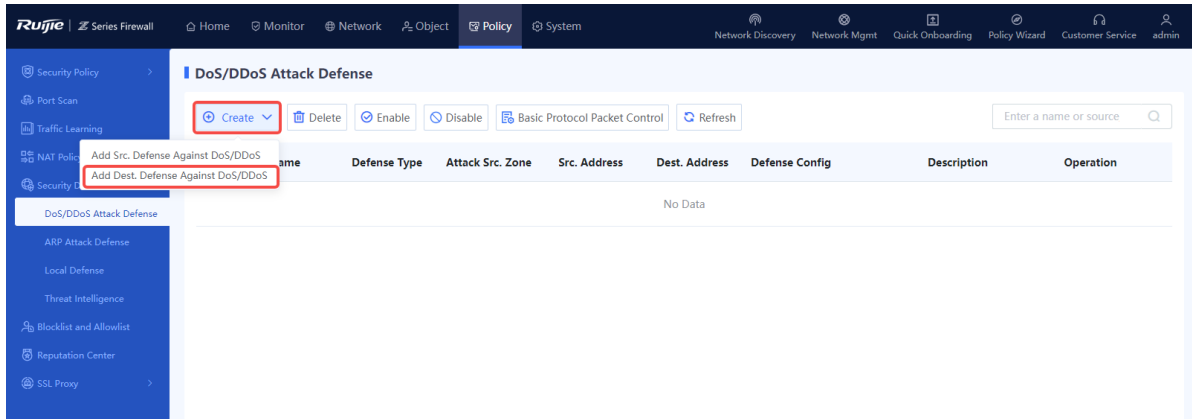
Follow-up Procedure

- To modify an existing policy, click **Edit**. To delete a policy, click **Delete**. To enable or disable the policy, click the switch.
- To delete multiple policies in a batch, select the policies that you want to delete and click **Delete**.
- To enable multiple policies in a batch, select the policies that you want to enable and click **Enable**.
- To disable multiple policies in a batch, select the policies that you want to disable and click **Disable**.
- Enter the policy names, policy associated objects, full or part of the policy description in the search box to search for the policies. Fuzzy search is supported.

2. Configuring Destination Defense Against DoS/DDoS

Procedure

- (1) Choose **Policy > Security Defense > DoS/DDoS Attack Defense**.



(2) In the operation area, click **Create** and select **Add Dest. Defense Against DoS/DDoS**.

The **Add Dest. Defense Against DoS/DDoS** page is displayed.

< Back
Add Dest. 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

Dest. Defense Against Selected Defense Types: SYN Flood Attack Defense,UDP Flood Attack Defense,ICMP Flood Attack Defense,ICMPv6 Flood Attack Defense

DoS/DDoS

Action After Detecting Attacks Log Limit

Advanced Defense

Packet-based Attack All

Teardrop Attack Defense

Smurf Attack Defense

LAND Attack Defense

Large ICMP Packet Attack Defense

Control IP Packets with Source Routes

ICMP Redirect Attack Defense

WinNuke Attack Defense

Control IP Packets with Record Routes

ICMP Unreachable Attack Defense

Fraggle Attack Defense

Filtering out IPv6 Packets with Specific EHS

(3) Set the parameters related to the 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	After this policy is delivered, the device checks the traffic from this security zone.	[Example] any
Src. Address	After this policy is delivered, the device checks the traffic from this address set.	any indicates all addresses. [Example] any
Dest. Address	After this policy is delivered, the device checks the traffic to this address set.	any indicates all addresses. [Example] any
Defense Config		
Dest. Defense Against DoS/DDoS		
Attack Defense Type	SYN Flood Attack Defense, UDP Flood Attack Defense, ICMP Flood Attack Defense, and ICMPv6 Flood Attack Defense are supported.	Click an attack defense type to enable defense against the specific attacks. [Example] SYN Flood Attack Defense: Enabled
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

Item	Description	Remarks
Action After Detecting Attacks	Action taken after the system detects an attack, including: Log: Only record a security log, but not limit the traffic rate. Limit: Only limit the traffic rate, but not record a security log.	[Example] Log + Limit
Advanced Defense		
Packet-based Attack	Whether defense against packet-based attacks is enabled.	[Example] All
Filtering out IPv6 Packets with Specific EHs	Filter out the IPv6 packets with the extended headers of the specified type.	[Example] Empty EHs

(4) Click **Save** to complete the configuration of DoS/DDoS attack defense policy.

Follow-up Procedure

- To modify an existing policy, click **Edit**. To delete a policy, click **Delete**. To enable or disable the policy, click the switch.
- To delete multiple policies in a batch, select the policies that you want to delete and click **Delete**.
- To enable multiple policies in a batch, select the policies that you want to enable and click **Enable**.
- To disable multiple policies in a batch, select the policies that you want to disable and click **Disable**.
- Enter the policy names, policy associated objects, full or part of the policy description in the search box to search for the policies. Fuzzy search is supported.

5.6.4 Configuring ARP Attack Defense

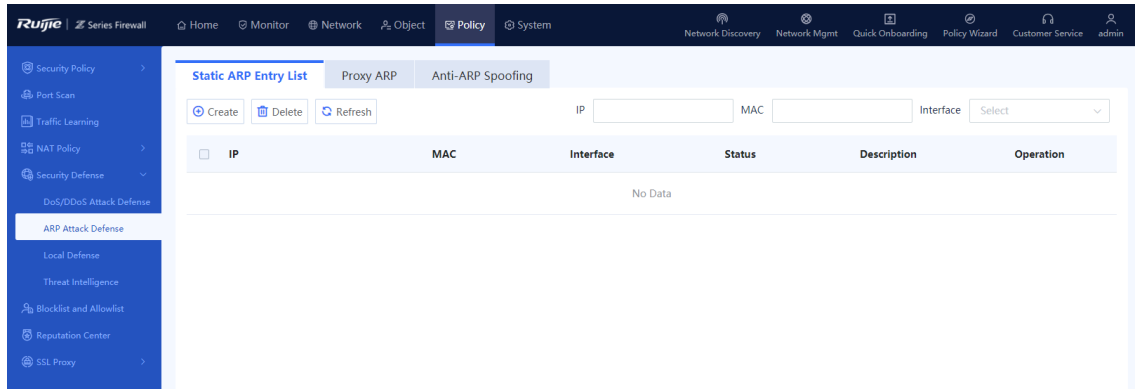
1. Configuring Static ARP

Application Scenario

Configuring static ARP entries can protect ARP entries from being modified by received forged gratuitous ARP packets or ARP response packets.

Procedure

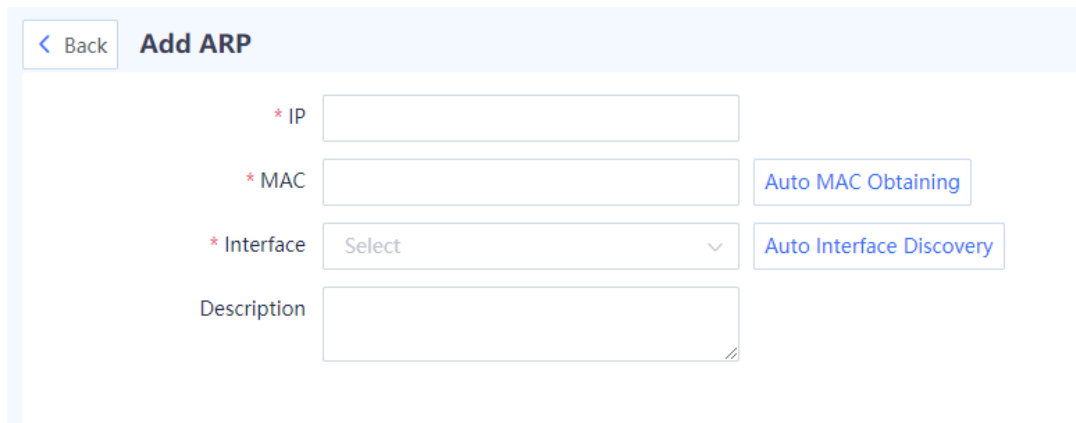
(1) Choose **Policy > Security Defense > ARP Attack Defense > Static ARP Entry List**.



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

The **Add ARP** page is displayed.



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

Item	Description	Remarks
IP	IP address to be bound to the static ARP entry.	[Example] 192.168.10.3
MAC	MAC address to be bound to the static ARP entry.	Two configuration methods are supported: <ul style="list-style-type: none"> ● Fill in the information manually. ● Click Auto MAC Obtaining. The device will search for the MAC address matching the IP address according to the available ARP entry information. If no address is found, the system displays "No address is matched." [Example] 11:22:33:44:55:66

Item	Description	Remarks
Interface	Physical interface to be bound.	<p>Two configuration methods are supported:</p> <ul style="list-style-type: none"> ● Fill in the information manually. ● Click Auto Interface Discovery. The device will configure the interface that may match the IP address according to the related information. If no interface is found, the system displays "No interface is matched." <p>[Example]</p> <p>Ge0/1</p>

(4) Click **Save**.

Follow-up Procedure

- To modify an existing entry, click **Edit**.
- To delete multiple entries in a batch, select the entries that you want to delete and click **Delete**.
- Enter the related parameters in the search box to filter the query result.

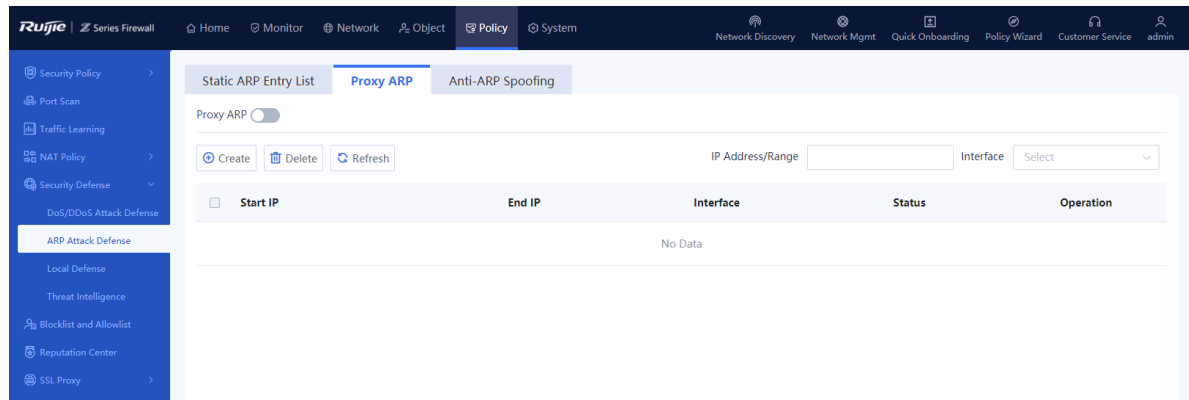
2. Configuring Proxy ARP

Application Scenario

When receiving an ARP request from the interface proxy network segment, the firewall returns the MAC address of the interface.

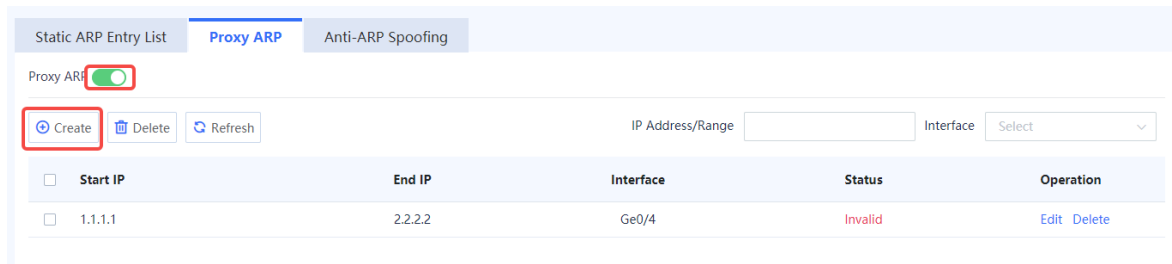
Procedure

(1) Choose **Policy > Security Defense > ARP Attack Defense > Proxy ARP**.



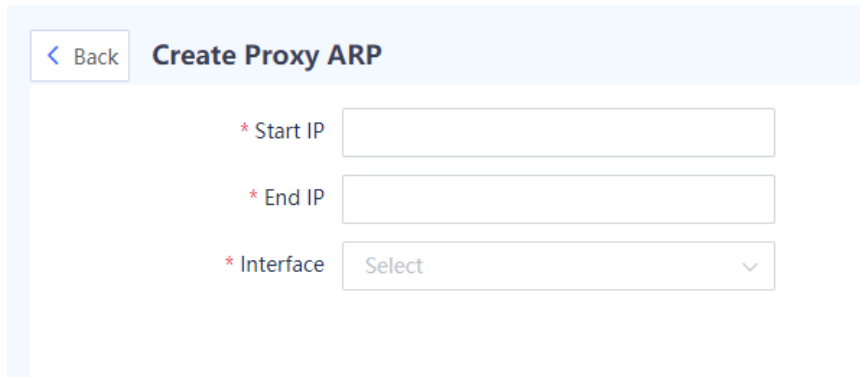
The proxy ARP network segments configured on the device are displayed. The **Status** column shows whether the interfaces bound to the entries are valid or invalid.

(2) Toggle on **Proxy ARP**.



(3) Click **Create**.

The **Create Proxy ARP** page is displayed.



(4) Fill in the start IP address and end IP address of proxy and select the proxy interface.

(5) Click **Save**.

Follow-up Procedure

- To modify an existing proxy ARP configuration, click **Edit**.
- To delete multiple configurations in a batch, select the configurations that you want to delete and click **Delete**.

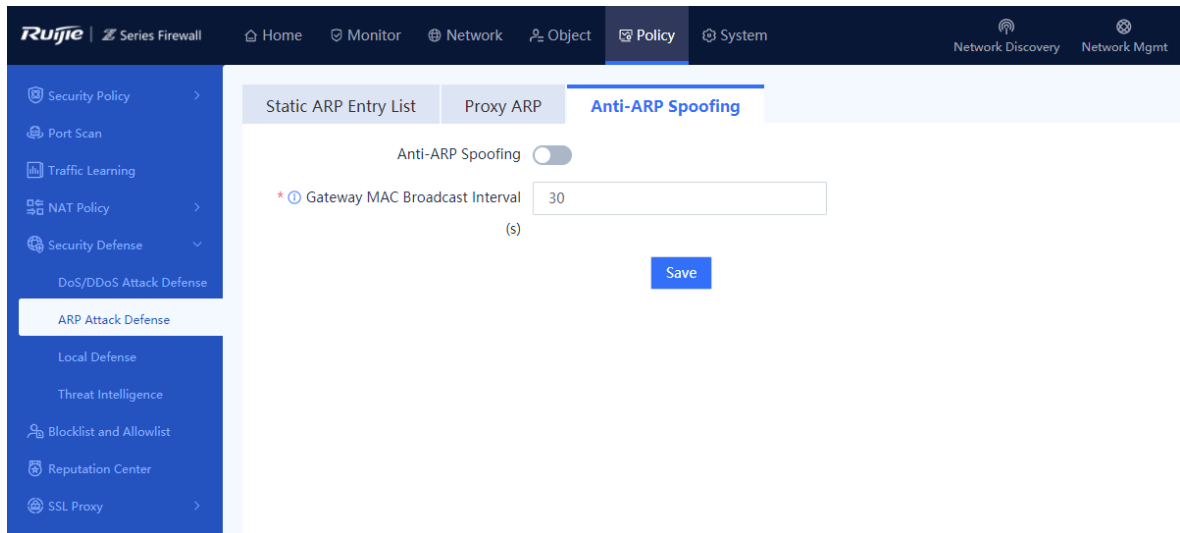
3. Configuring Anti-ARP Spoofing

Application Scenario

The firewall sends gratuitous ARP broadcast packets to allow terminals on the same network segment to obtain the correct MAC address of the firewall.

Procedure

(1) Choose **Policy > Security Defense > ARP Attack Defense > Anti-ARP Spoofing**.



(2) Toggle on **Anti-ARP Spoofing**.

(3) Modify **Gateway MAC Broadcast Interval**. The unit is second.

(4) Click **Save**.

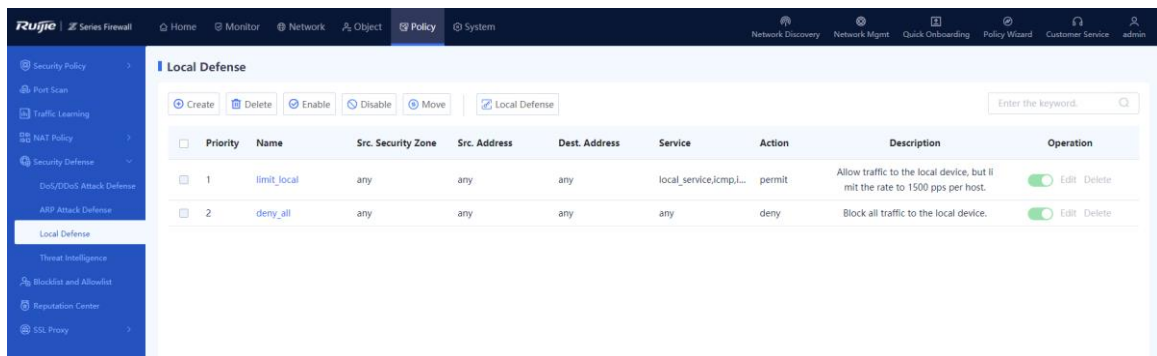
5.6.5 Configuring Local Defense

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.

Procedure

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



Note

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

(2) Enable Local Defense.

a In the operation area, click **Local Defense**.

Local Defense

<input type="checkbox"/>	Priority	Name	Src. Security Zone	Src. Address	Dest. Address	Service	Action
<input type="checkbox"/>	1	limit_local	any	any	any	local_service,icmp,I...	permit
<input type="checkbox"/>	2	deny_all	any	any	any	any	deny

b Toggle on **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

(3) Create a local defense policy.

a Click Create to access the Create Local Defense Policy page.

< Back **Create Local Defense Policy**

Basic Info

* Name

Enabled State Enable Disable

Adjacent Policy Select a policy. Before

Description

Src. and Dest.

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

Src. Address

To-be-selected (0)

Select Enter the keyword.

any

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

Selected (1) Clear

Enter the keyword.

any ✕

Dest. Address

To-be-selected (0)

Select Enter the keyword.

any

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

Service

Service

To-be-selected (78)

Select Enter the keyword.

Service/Group	Protocol	Dest.
Name	/Service	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

Enter the keyword.

any ✕

Service

Service

To-be-selected (78)

Select Enter the keyword.

Service/Group	Protocol	Dest.
Name	/Service	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

Enter the keyword.

any ✕

Action Settings

Action Option Permit Deny

IP-based Rate Limit

IP-based Rate Limit Disable Enable

b Set the parameters for the local defense policy.

Item	Description	Remarks
Basic Info		

Item	Description	Remarks
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.	N/A
Description	Security policy description.	Characters such as `~!#%^&*+\\ {};:"'/<>? are not allowed.
<p>Src. and Dest.</p> <p>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.</p>		
Src. Security Zone	After this policy is delivered, the device checks the traffic from this zone.	any indicates traffic of all zones. [Example] any
Src. Address	After this policy is delivered, the device checks the traffic from this address set.	any indicates all addresses. [Example] any
Dest. Address	After this policy is delivered, the device checks the traffic to this address set.	any indicates all addresses. [Example] any
Service	After this policy is delivered, the device checks the traffic of this service.	any indicates all services. [Example] any
Action Settings		
Action Option	Action taken on the traffic that hits the policy.	[Example] Permit
IP-based Rate Limit		

Item	Description	Remarks
IP-based Rate Limit	<p>Whether to restrict the number of packets that can pass per second in the traffic matching the policy.</p> <ul style="list-style-type: none"> ● Disable: not restricted ● Enable: restricted. The Packets Allowed to Pass Through Each Host (pps) field needs to be set. 	<p>[Example]</p> <p>Disable</p>

c Click **Save**.

Follow-up Procedure

- 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**.
- To move a policy, select the policy and 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.

5.7 Threat Intelligence

5.7.1 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 TI 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 TI, to block malicious IP addresses and domain names.

5.7.2 Enabling Threat Intelligence

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

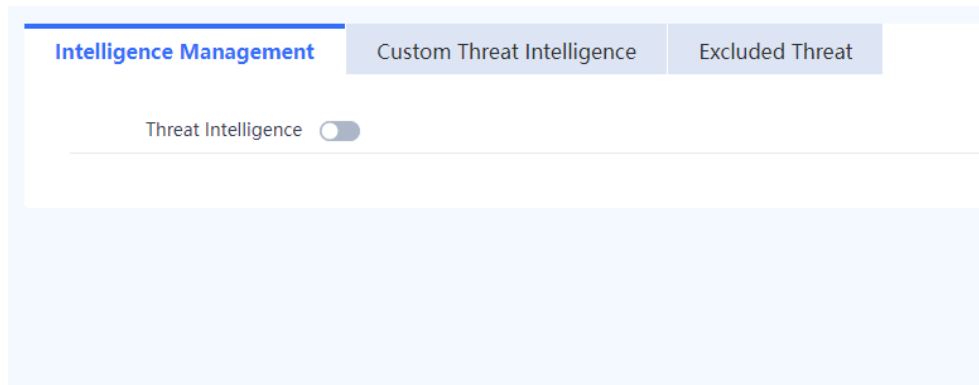
You have obtained and activated the TI capability license. For details about license activation, see [8.3 Activating the License](#).

i Note

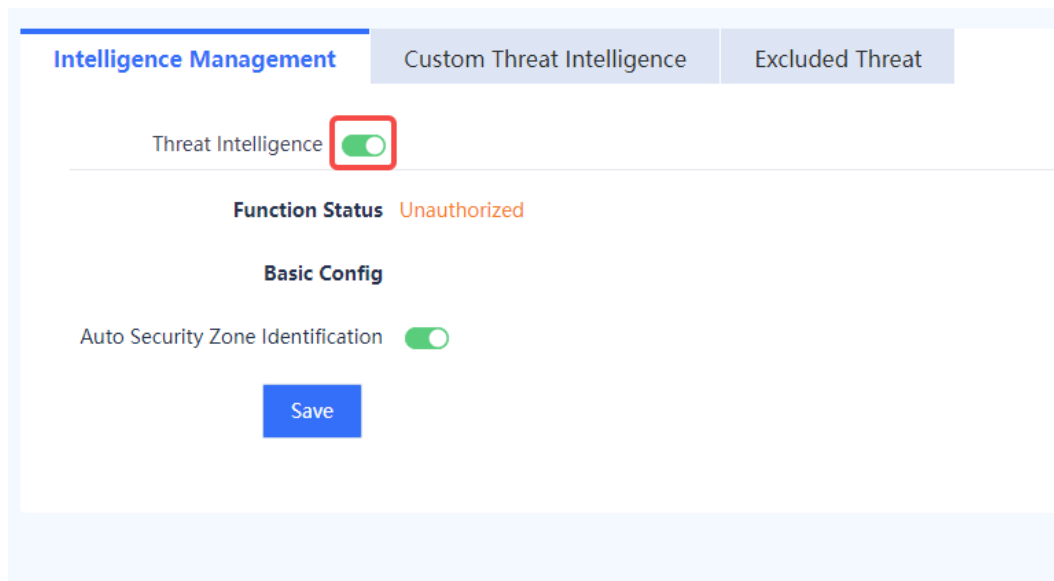
If the TI function is not authorized or authorization expires, the detection based on TI signature library is unavailable, and only the custom TI configured manually can be used. In this case, the TI signature library cannot be upgraded.

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"> ● Unauthorized: The TI function license is not activated, or online authorization fails. ● Normal: The TI function license is activated. The function is available and the library can be updated. ● Server Error: The TI function license is activated, but Ruijie Secure Cloud Platform cannot connect to the TI signature library update server. The TI signature library cannot be updated. 	<p>The status is displayed automatically according to the current TI function status.</p> <p>[Example] Normal</p>
Basic Config		
Auto Security Zone Identification	<p>Whether to identify the traffic inbound and outbound security zones automatically.</p> <ul style="list-style-type: none"> ● After this function is enabled, the device automatically identifies the inbound and outbound security 	<p>[Example] Enable</p>

Item	Description	Remarks
	<p>zones (ingress and egress) of traffic, and determines whether to perform threat signature matching for the traffic.</p> <ul style="list-style-type: none"> If this function is disabled, you can manually specify the effective security zones for TI. 	
Effective Security Zone	After the effective security zone is specified, the system performs TI matching and processing (block or alarm) for the traffic only when the outbound security zone of the traffic is the same as the specified zone.	When Auto Security Zone Identification is disabled, this parameter needs to be configured. [Example] untrust
Threat Intelligence Defense		
Type	Select the TI type to defend against.	Select to enable defense. [Example] APT
Action	<p>Action to be taken on the traffic matching the TI:</p> <ul style="list-style-type: none"> Deny: Block traffic and record a security log. Alarm: Not block traffic, but record a security log. 	[Example] Deny

(4) Click **Save**.

5.7.3 Customizing Threat Intelligence

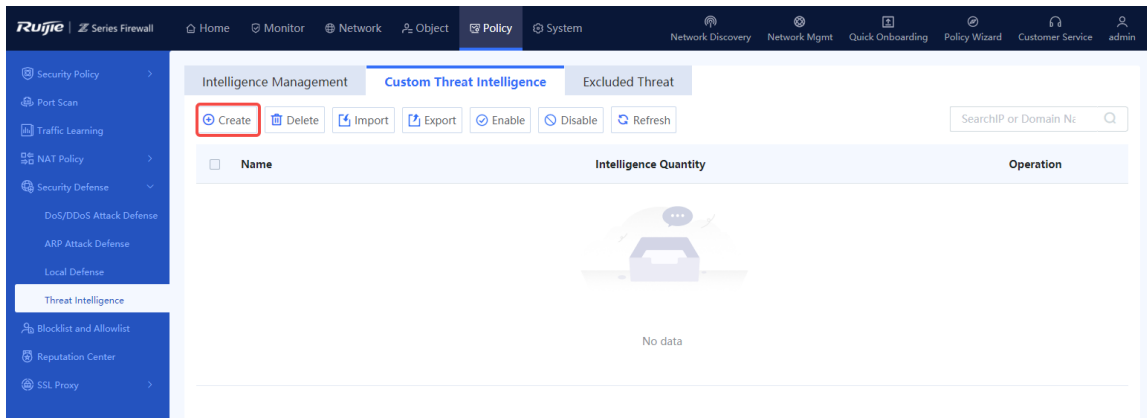
Application Scenario

In addition to the TI contained in the TI signature library, the system allows you to import malicious intelligence that you have collected. When a threat is detected, the system matches the threat against the custom TI first. The data matching custom TI is blocked and a security log is recorded.

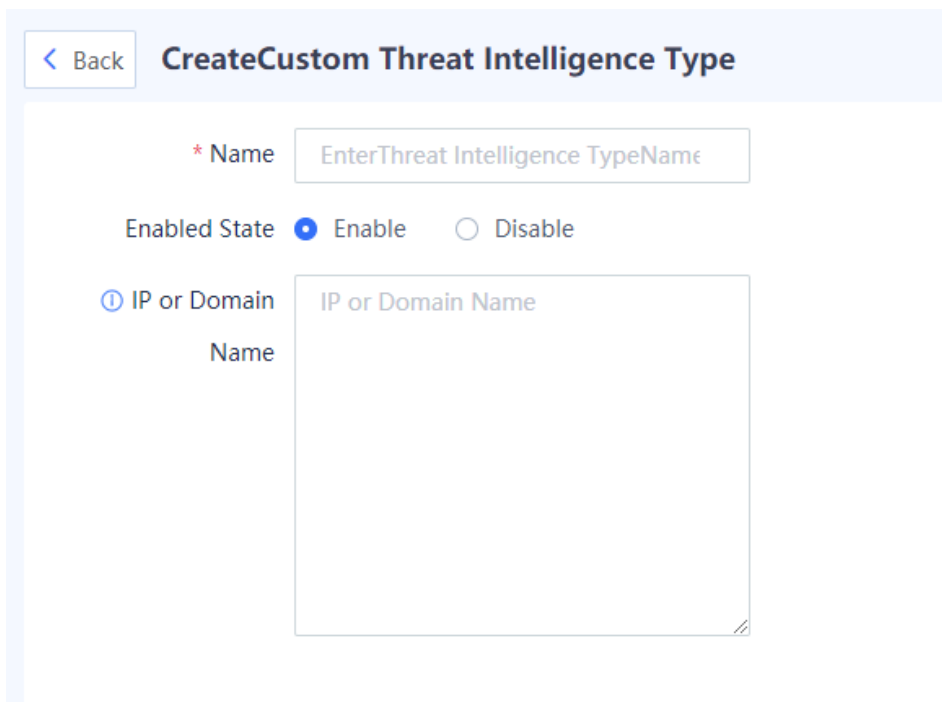
In the unauthorized state, custom TI can still be used for matching.

1. Manually Configuring Custom TI

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



(2) Click Create to access 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"> If multiple IP addresses or domain names need to be configured, enter one IP address or domain name per line, and press Enter to separate lines.

Item	Description	Remarks
		<ul style="list-style-type: none"> The domain name matching rule is full match. [Example] www.xxx.com

(4) Click **Save**.

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.

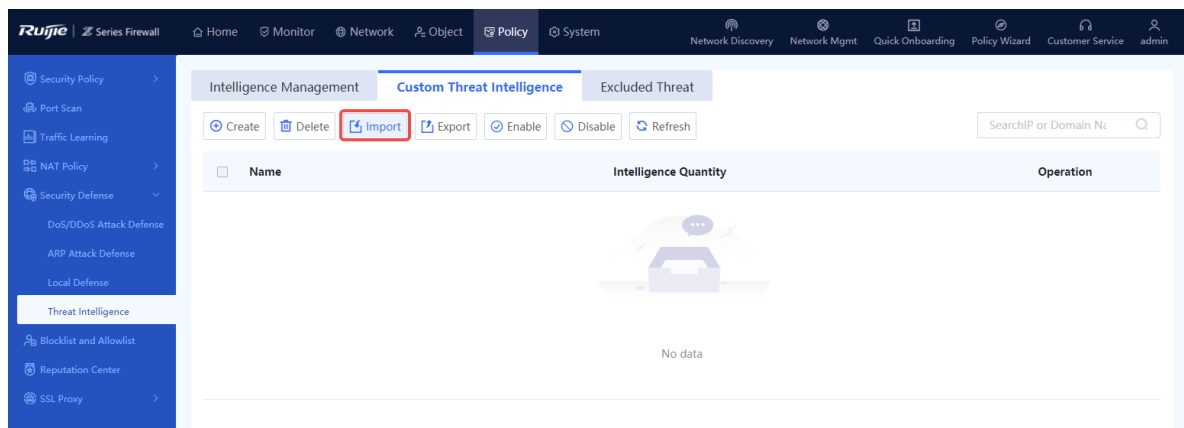
2. Importing Custom TI

Application Scenario

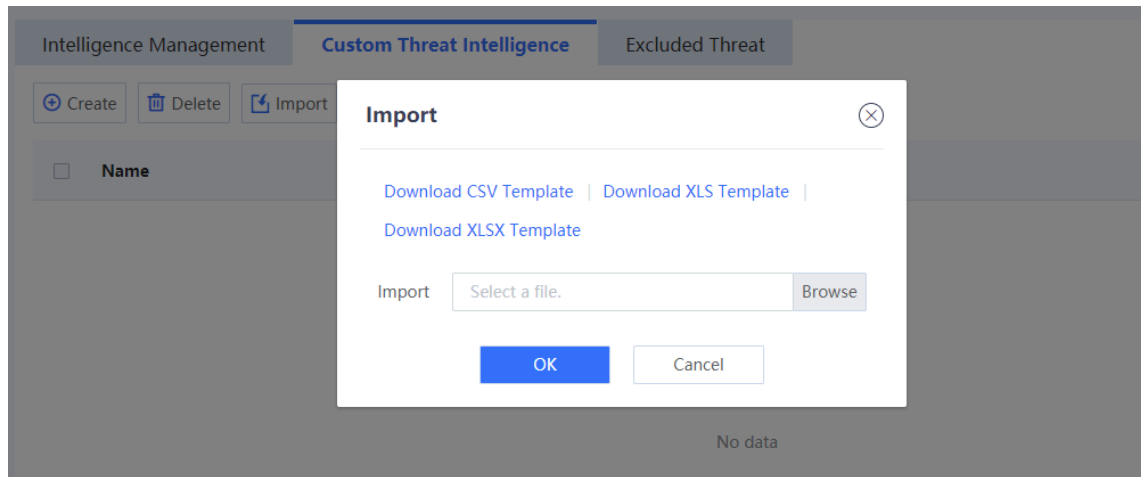
When you need to add a large number of TI types, you can fill in TI information in a template, and import them in a batch with one click.

Procedure

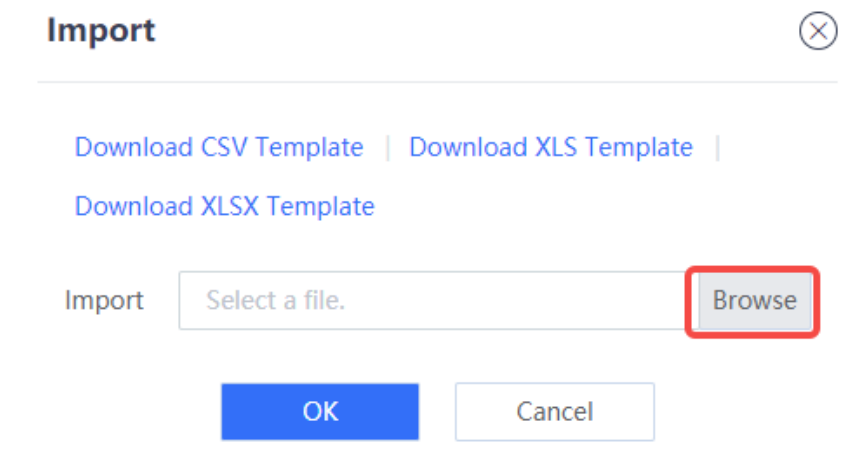
(1) Choose **Policy > Security Defense > Threat Intelligence > Custom Threat Intelligence**.



(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 **OK** 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.

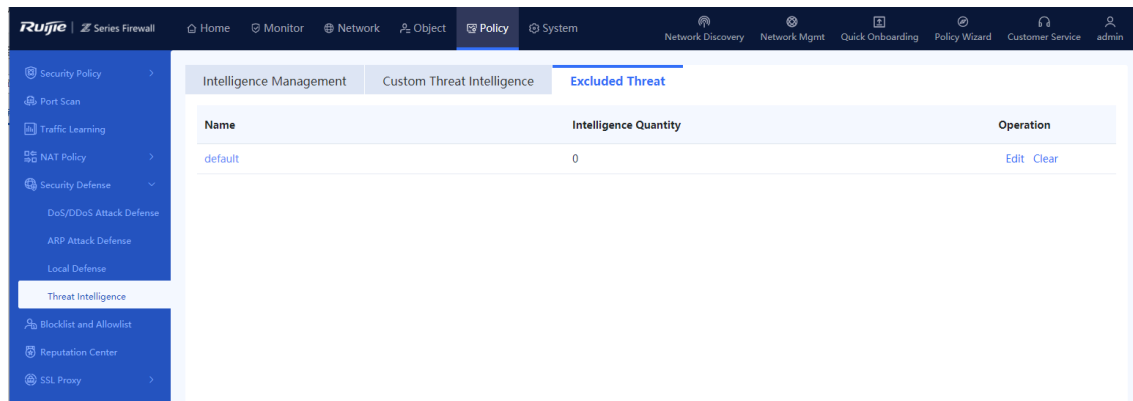
5.7.4 Configuring an Excluded Threat

Application Scenario

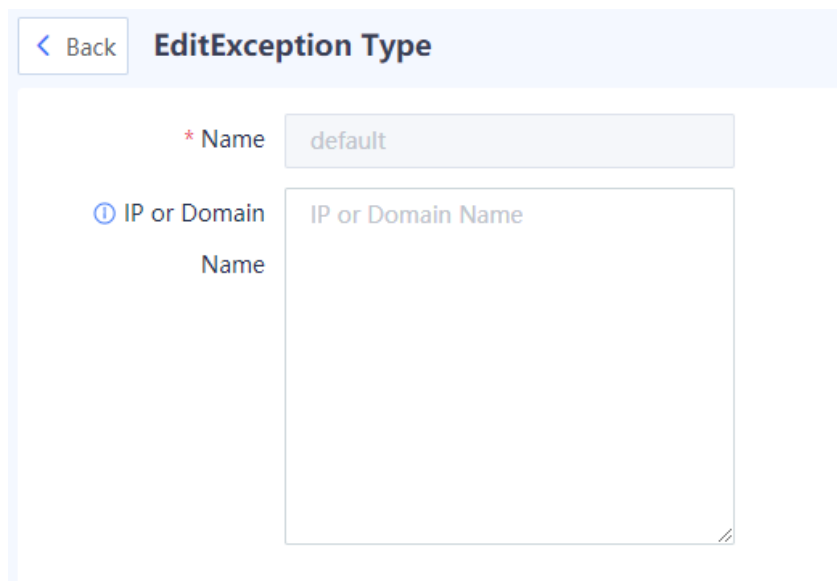
If the user's normal data is intercepted by mistake due to the not-updated TI content or other reasons, or if an IP address or domain name is not malicious, you can add the IP address or domain name to the excluded threat list. The traffic matching the excluded threat list will be permitted by the TI module.

Procedure

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



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



- (3) Set the parameters of the excluded threat.

Item	Description	Remarks
Name	Excluded threat name.	[Example] default

Item	Description	Remarks
IP or Domain Name	IP address or domain name of the excluded threat.	If multiple IP addresses or domain names need to be configured, enter one IP address or domain name per line, and press Enter to separate lines. [Example] 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 threat, click **Clear**.

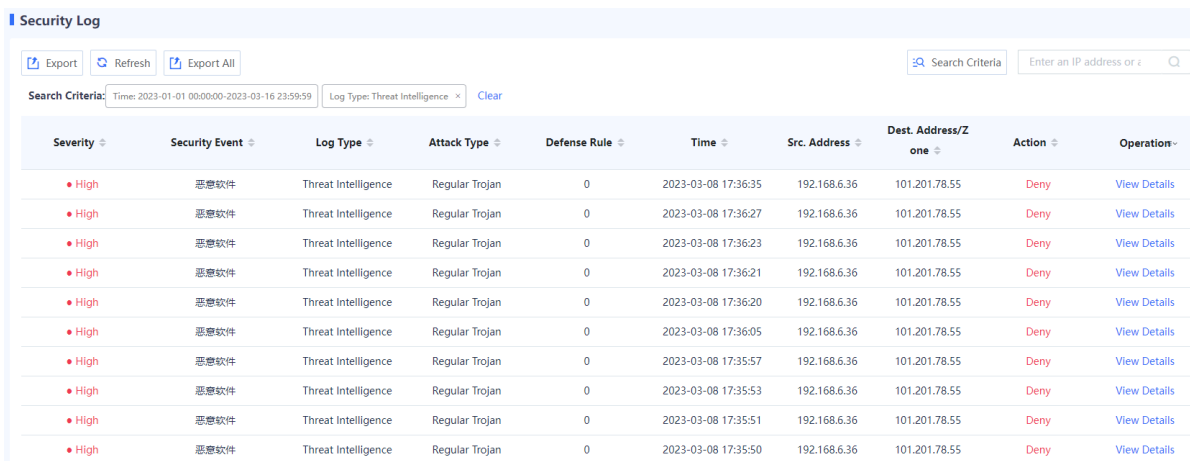
5.7.5 Viewing Threat Intelligence Logs

Application Scenario

When a malicious connection matches the TI, 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 TI type, helping you take further actions.

Procedure

- (1) Choose **Monitor > Log Monitoring > Security Log**.
- (2) The TI log information is displayed on the web UI.



The screenshot shows the 'Security Log' interface with a table of logs. The table has columns for Severity, Security Event, Log Type, Attack Type, Defense Rule, Time, Src. Address, Dest. Address/Zone, Action, and Operation. The logs show multiple entries with a severity of 'High', security event of '恶意软件' (Malware), log type of 'Threat Intelligence', attack type of 'Regular Trojan', defense rule of '0', and action of 'Deny'.

Severity	Security Event	Log Type	Attack Type	Defense Rule	Time	Src. Address	Dest. Address/Zone	Action	Operation
High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:36:35	192.168.6.36	101.201.78.55	Deny	View Details
High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:36:27	192.168.6.36	101.201.78.55	Deny	View Details
High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:36:23	192.168.6.36	101.201.78.55	Deny	View Details
High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:36:21	192.168.6.36	101.201.78.55	Deny	View Details
High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:36:20	192.168.6.36	101.201.78.55	Deny	View Details
High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:36:05	192.168.6.36	101.201.78.55	Deny	View Details
High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:35:57	192.168.6.36	101.201.78.55	Deny	View Details
High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:35:53	192.168.6.36	101.201.78.55	Deny	View Details
High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:35:51	192.168.6.36	101.201.78.55	Deny	View Details
High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:35:50	192.168.6.36	101.201.78.55	Deny	View Details

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

Security Log Details



[Exclude](#)

Regular Trojan

Src. → **Dest.**

Src. Security Zone: trust	Dest. Security Zone: untrust
Src. IP: 192.168.6.36	Dest. IP: 101.201.78.55
Src. Port: 17972	Dest. Port: 58468
MAC: f8:e4:3b:04:bd:5f	App:

Basic Info

Time: 2023-03-08 17:36:35	Type: Regular Trojan
Security Event: 恶意软件	Direction: LAN-to-WAN
Severity: High	Action: Deny
Blocking Duration: 0s	Defense Rule: 0
Security Policy Name: Threat Intelligence	
Domain Name/IP: 101.201.78.55	

Exclude: If you confirm that a threat is a false positive, click **Exclude** to add the TI information in this security log to the excluded threat list and permit subsequent traffic.

Note

For more information and configurations about the fields in security logs, see [9.2.2 2. Querying Security Logs](#).

5.7.6 Upgrading a Threat Intelligence Signature Library

Upgrade the TI signature library timely to improve the threat identification capability of the firewall. For details about signature library upgrade, see [8.5 Signature Library Upgrade](#).

5.8 Blocklist and Allowlist

5.8.1 Overview

Z-S series firewalls support blocklists and allowlists 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 validity period is the blocking duration of the brute-force security rule. You can also manually configure a temporary blocklist.

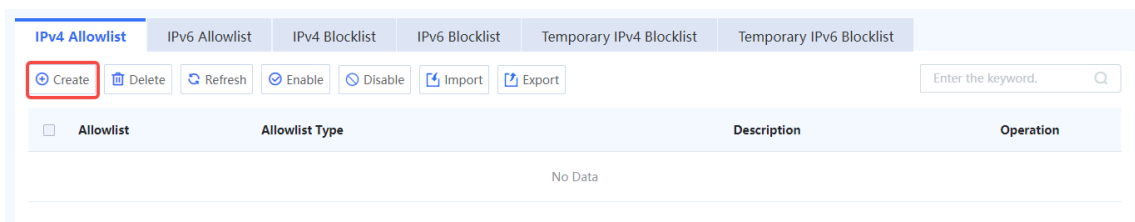
5.8.2 Creating an IPv4 Allowlist

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 In the operation area, click **Create**.



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

< Back

Add Allowlist

IP Type IPv4

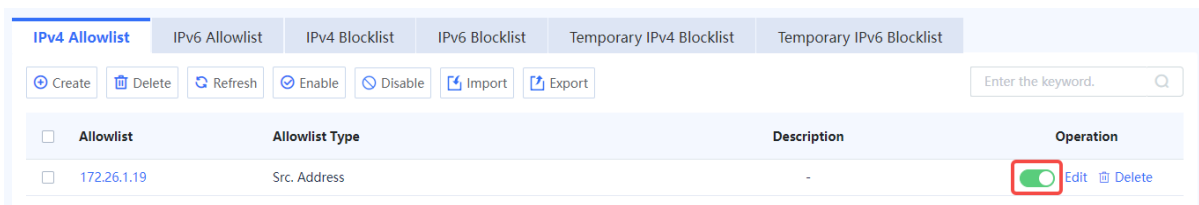
Allowlist Type Src. Address Dest. Address

* ⓘ IP Address/Range

Description

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

(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.

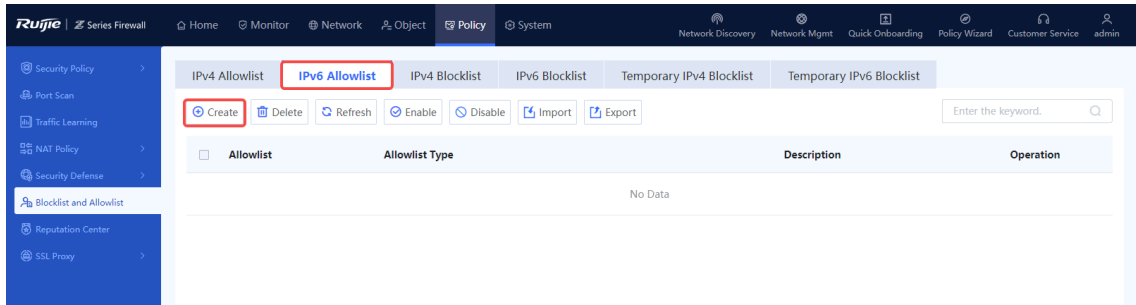
5.8.3 Creating an IPv6 Allowlist

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 In the operation area, click **Create**.



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

Add Allowlist

IP Type IPv6

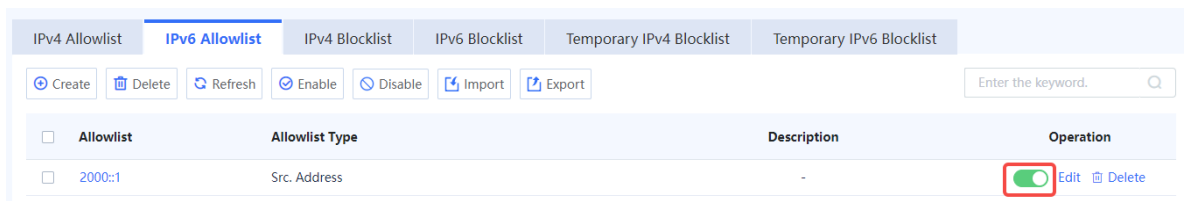
Allowlist Type Src. Address Dest. Address

*

Description

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

(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.

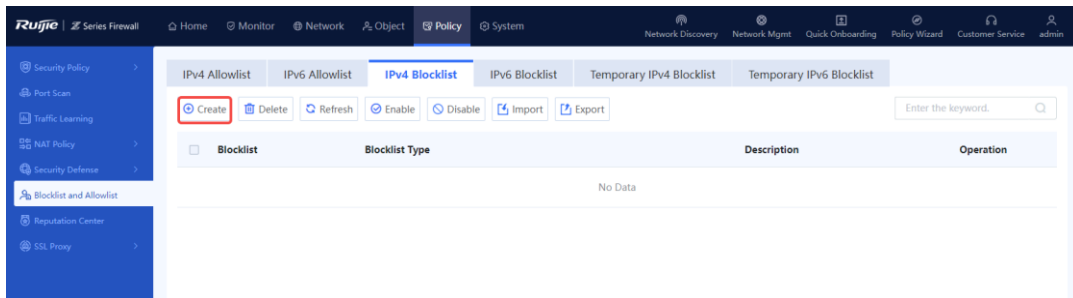
5.8.4 Creating an IPv4 Blocklist

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

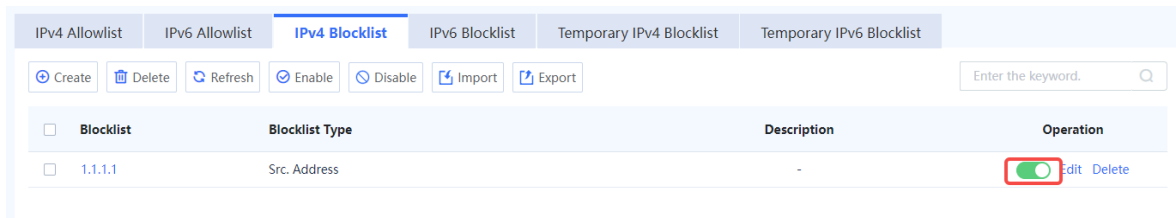
Blocklist Type Src. Address Dest. Address

*

Description

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

(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.

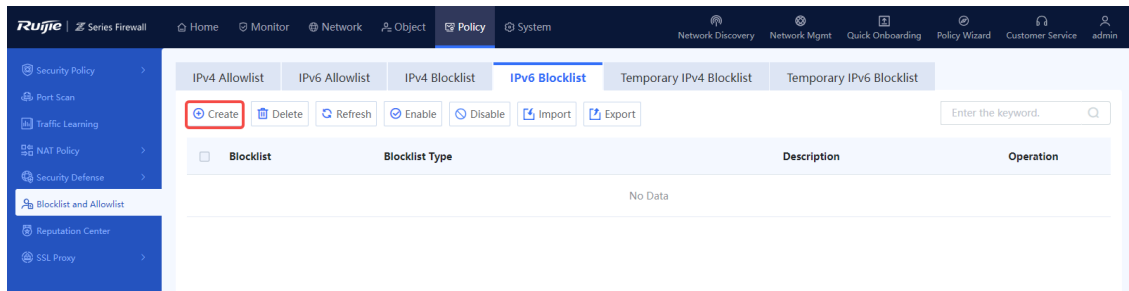
5.8.5 Creating an IPv6 Blocklist

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 In the operation area, click **Create**.



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

< Back

Add Blocklist

IP Type IPv6

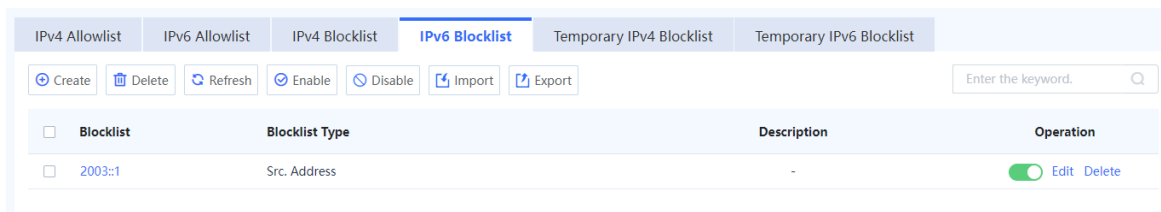
Blocklist Type Src. Address Dest. Address

* ① IP Address/Range

Description

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

(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.

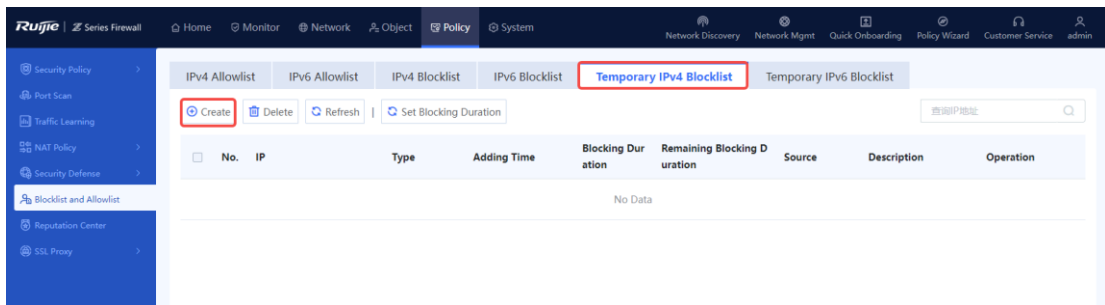
5.8.6 Creating a Temporary IPv4 Blocklist

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 In 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

* ⓘ 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"> ● Src. Address: Block packets sent from this address. ● Dest. Address: Block packets sent to this address. 	[Example] Src. Address
IP Address/Range	Temporary blocklist IP address/range.	The following two formats are supported: Single IP address: 192.168.1.1 IP range: 192.168.1.1-192.168.1.10
Blocking Duration	Validity period of the temporary blocklist. When the validity period expires, the blocklist becomes invalid and is automatically deleted.	[Example] 5 minutes
Description	Description of the temporary 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**.

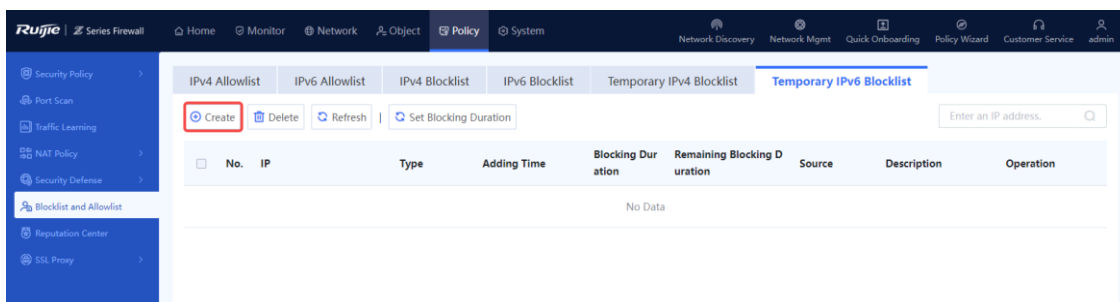
5.8.7 Creating a Temporary IPv6 Blocklist

Application Scenario

Configure a temporary IPv6 blocklist on the web UI.

Procedure

- (1) Access the **Add Temporary Blocklist** page.
 - Choose Policy > Blocklist and Allowlist > Temporary IPv6 Blocklist.
 - In 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

*

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"> ● Src. Address: Block packets sent from this address. ● Dest. Address: Block packets sent to this address. 	[Example] Src. Address
IP Address/Range	Temporary blocklist IP address/range.	The following two formats are supported: <ul style="list-style-type: none"> ● Single IP address: 1234::100 ● IP range: 1234::100-2345::100
Blocking Duration	Validity period of the temporary blocklist. When the validity period expires, the blocklist becomes invalid and is automatically deleted.	[Example] 5 minutes
Description	Description of the temporary blocklist.	Characters such as `~!#%^&*+\\{ };:'''/<>? are not allowed.

(3) After the configuration is completed, click **Save**.

Follow-up Procedure

- To delete multiple temporary blocklist policies in a batch, select the policies that you want to delete and click **Delete**.
- To configure the validity period of multiple temporary blocklist policies, select the policies and click **Set Blocking Duration**.

5.9 SSL Proxy

5.9.1 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 an SSL connection with the client.
Server protection		The firewall uses the imported server certificate to set up an SSL connection with the client.

5.9.2 Configuring an SSL Proxy Template

Application Scenario

Configure this function if you need to perform security detection including virus protection and IPS detection for HTTPS encrypted traffic. The system predefines a default template, which can be directly referenced or customized as required. This template applies to traffic proxy in common Internet access scenarios.

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

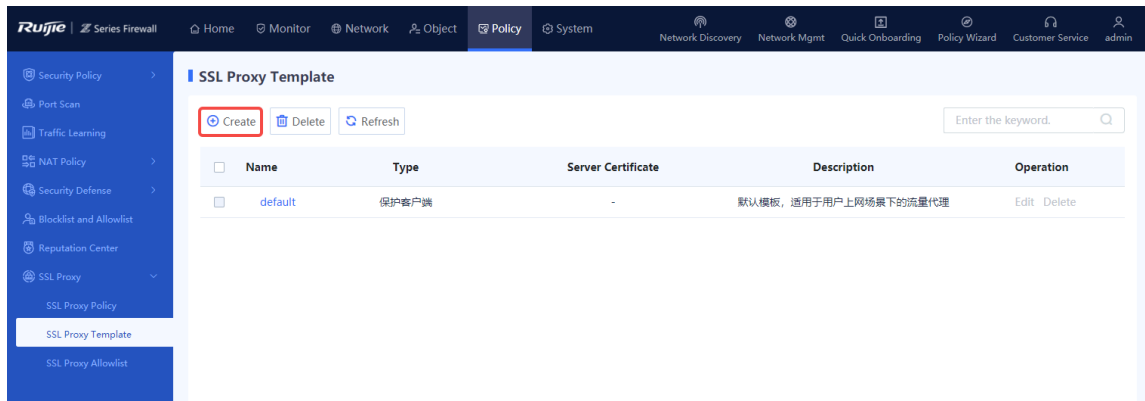
SSL proxy templates are classified into client protection and server protection based on the scenarios in which the SSL proxy function is used.

- 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 [6.8.3 SSL Certificate](#).
- If you select **Protect Server** as the SSL proxy template type, import the server certificate first. For details about server certificate import, see [6.8.3 4. Importing a Server Certificate](#).

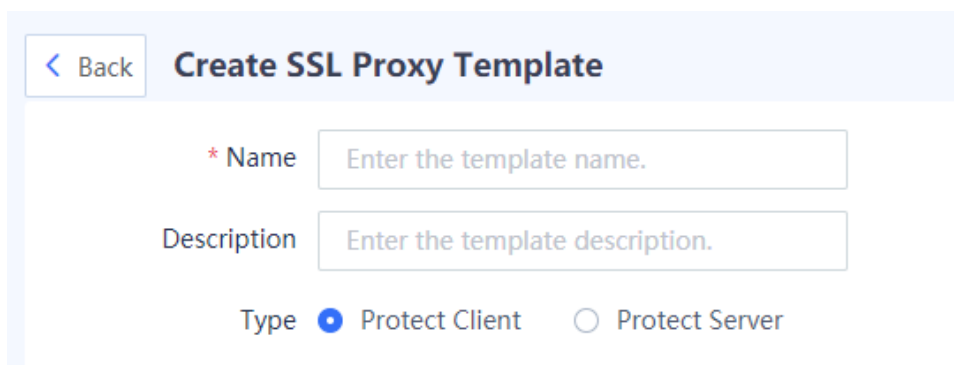
Procedure

(1) Access the **SSL Proxy Template** page.

Choose **Policy > SSL Proxy > SSL Proxy Template**.



(2) Click Create. The Create SSL Proxy Template page is displayed.



(3) Configure parameters for the SSL proxy template and click **Save**.

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 Protect Client or Protect Server .	Select the type according to the actual networking scenario. [Example] Protect Client
Server Certificate	Used to establish the trusted 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. For details about server certificate import, see 6.8.3.4. Importing a Server Certificate .

Follow-up Procedure

- Create an SSL proxy policy and reference an SSL proxy template. An SSL proxy template takes effect only when it is referenced by an SSL proxy policy.
- To delete an SSL proxy template that is not referenced, click **Delete**.
- Predefined SSL proxy templates on the device cannot be deleted.

5.9.3 Configuring an SSL Proxy Policy

Application Scenario

The SSL proxy policy is used to set the matching conditions of encrypted packets and whether to decrypt them after they are hit.

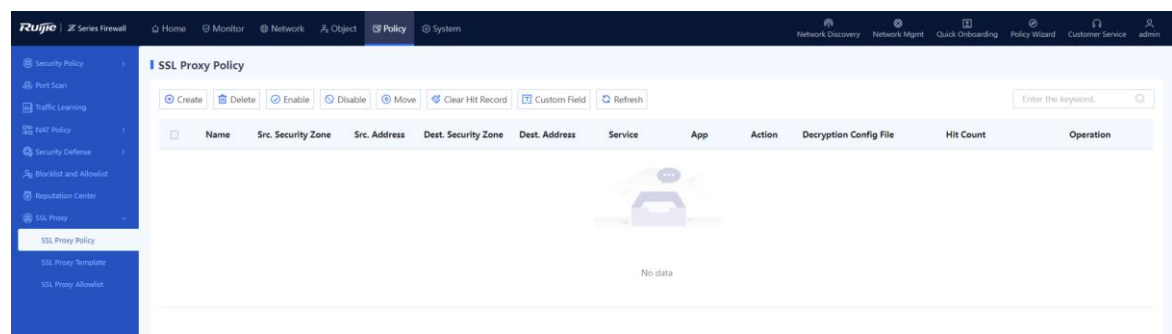
Configure this function if you need to perform security detection including virus protection and IPS detection for HTTPS encrypted traffic.

Prerequisites

An SSL proxy template has been created. For details about SSL proxy template creation, see [5.9.2 Configuring an SSL Proxy Template](#).

Procedure

- (1) Choose **Policy > SSL Proxy > SSL Proxy Policy**.



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

The **Create SSL Proxy Policy** page is displayed.

< 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

(3) Configure parameters for the SSL proxy policy.

Item	Description	Remarks
Basic Info		
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] Enable

Item	Description	Remarks
Description	Description of SSL proxy policy.	<p>Characters such as `~!#%^&*+\\{ };:!"/<>? are not allowed.</p> <p>[Example]</p> <p>Decrypt the HTTPS encrypted traffic from security zone 1 to security zone 2.</p>
Src. and Dest.		
Src. Security Zone	Source security zone that initiates the target data connection.	<ul style="list-style-type: none"> Click the drop-down list, and select a source security zone in the To-be-selected area. The selected zone is automatically added to the Selected area. Click Add Security Zone to add a custom security zone. <p>[Example]</p> <p>trust</p>
Src. Address	Source address that initiates the target data connection.	<p>Click the drop-down list, and select a source address in the To-be-selected area. The selected address is automatically added to the Selected area.</p> <p>[Example]</p> <p>any</p>
Dest. Security Zone	Destination security zone of the target data connection.	<ul style="list-style-type: none"> Click the drop-down list, and select a destination security zone in the To-be-selected area. The selected zone is automatically added to the Selected area. Click Add Security Zone to add a custom security zone. <p>[Example]</p> <p>trust</p>
Dest. Address	Destination address of the target data connection.	<p>Click the drop-down list, and select a destination address in the To-be-selected area. The selected address is automatically added to the Selected area.</p> <p>[Example]</p> <p>any</p>
Service	Service type of the target data connection request.	<p>[Example]</p> <p>any</p>

Item	Description	Remarks
App	Application type of the target data connection request.	You can set an application type to enable the device to decrypt traffic of the specified applications. [Example] any
Action Option	Action taken by the SSL proxy policy: decrypting or not decrypting the content of target data connection. If Decrypt is selected, an SSL proxy template must be specified.	[Example] Decrypt
SSL Proxy Template	SSL decryption configuration file that specifies how the device decrypts the packets that hit the policy and the required certificate file.	You need to select an SSL decryption configuration file when Action Option of the policy is set to Decrypt . Click Create SSL Proxy Template to create an SSL proxy template. [Example] default

(4) Click **Save**.

Follow-up Procedure


Name	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Action	Decryption Config File	Hit Count	Operation
test	trust	any	untrust	any	any	any	Decrypt	default	0	Clear Edit Delete

- The **SSL Proxy Policy** page displays the configuration information and hit count of the policy. You can click **Clear**, or select policies and click **Clear Hit Record** to clear the hit statistics for the specified policies.
- To move an SSL policy, select the policy and click **Move** to adjust its priority in matching.

SSL proxy 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 an SSL proxy policy, the next policy will not be matched. When you configure multiple SSL proxy policies, the list of the policies is arranged in the order of configuration by default. The policies that are configured later have higher priorities.

You can move the SSL proxy policies to adjust their priorities and achieve more precise traffic matching and processing.

- To modify a created SSL proxy policy, click **Edit**.
- To delete a created SSL proxy policy, click **Delete**.

- To enable or disable a policy, click  in the **Operation** column, or select the policy and click **Enable** or **Disable**. A disabled policy does not take effect.
- Click **Custom Field** to set the fields to be displayed on the page.

5.9.4 Configuring an SSL Proxy Allowlist

1. Overview

After an SSL proxy allowlist is enabled, the device transparently transmits the packets from the SSL connections that match the SSL proxy allowlist without performing the proxy function.

Application scenarios of the SSL proxy allowlist:

- The server needs to authenticate clients.
- The client needs to perform deep verification on the server certificate.

An SSL connection is established between the client and server and the client's applications have fixed predefined certificates. In this scenario, if the certificates used by the device that functions as proxy cannot pass the verification of the client, SSL disconnection occurs. In this case, you need to set an SSL proxy allowlist to enable the device to transparently transmit the packets from the SSL connection between the client and server, without performing the proxy function.

SSL proxy allowlist types:

- Domain name allowlist: Allowlists that contain domain names of websites that do need to or cannot be accessed by proxy.
- Application allowlist: Allowlists that contain application types that do need to or cannot be accessed by proxy.

The SSL proxy allowlists can be further classified into predefined and custom allowlists:

- Predefined allowlist: SSL proxy allowlists predefined on the device. The **Type** of these allowlists is **Predefined**.
- Custom allowlist: SSL proxy allowlists manually configured by users. The **Type** of these allowlists is **Custom**.

2. Configuring a 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 domain name allowlist for SSL proxy predefined on the device contains commonly used domain names and the domain names for which deep certificate verification is performed by clients. The domain names in the predefined allowlist cannot be deleted, but the allowlist function can be disabled for them as required.

Procedure

- (1) Choose **Policy > SSL Proxy > SSL Proxy Allowlist > Domain Name Allowlist**.

On the page that is displayed, you can view domain names in the predefined allowlist. Click  to enable or disable the allowlist function for a domain name.

Domain Name Allowlist		App Allowlist			
<input type="button" value="Create"/>	<input type="button" value="Delete"/>	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>	<input type="button" value="Refresh"/>	<input type="text" value="Enter the keyword."/>
Name	Type	Operation			
<input type="checkbox"/> login.live.com	public.predefined	<input checked="" type="checkbox"/>	Delete		
<input type="checkbox"/> *.googleapis.com	public.predefined	<input checked="" type="checkbox"/>	Delete		
<input type="checkbox"/> *.windows.com	public.predefined	<input checked="" type="checkbox"/>	Delete		
<input type="checkbox"/> *.microsoft.com	public.predefined	<input checked="" type="checkbox"/>	Delete		
<input type="checkbox"/> *.weixin.qq.com	public.predefined	<input checked="" type="checkbox"/>	Delete		
<input type="checkbox"/> ssl.ptlogin2.qq.com	public.predefined	<input checked="" type="checkbox"/>	Delete		
<input type="checkbox"/> xui.ptlogin2.qq.com	public.predefined	<input checked="" type="checkbox"/>	Delete		
<input type="checkbox"/> passport.baidu.com	public.predefined	<input checked="" type="checkbox"/>	Delete		
<input type="checkbox"/> wappass.baidu.com	public.predefined	<input checked="" type="checkbox"/>	Delete		
<input type="checkbox"/> nsclick.baidu.com	public.predefined	<input checked="" type="checkbox"/>	Delete		

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

The **Create Domain Name Allowlist** page is displayed.

< Back

Create Domain Name Allowlist

*

- (3) Enter the domain name to be added to the allowlist and click **Save**.

The wildcard character (*) can only be added at the beginning or end of a domain name to indicate any string. For example, *.ruijie.com.

Follow-up Procedure

- Click to enable or disable the allowlist function for a domain name. To enable or disable this function for domain names in a batch, select the domain names and click **Enable** or **Disable**.
- To delete a custom domain name from the allowlist, click **Delete**. Domain names in the predefined allowlist cannot be deleted.

3. Configuring an Application Allowlist

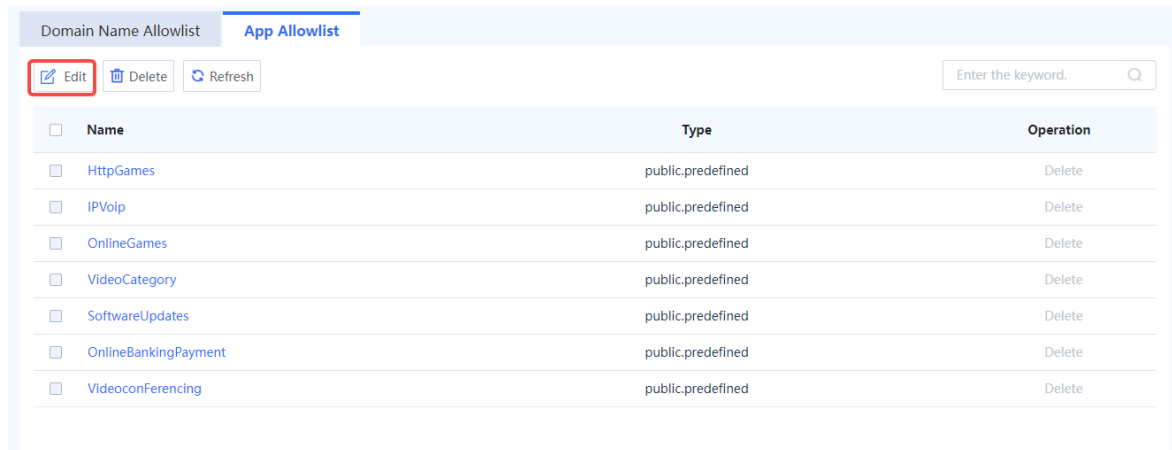
Application Scenario

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 application allowlist for SSL proxy predefined on the device contains the commonly used applications, applications that require client authentication, and applications for which deep certificate verification is performed by clients. You can add applications to the predefined application allowlist.

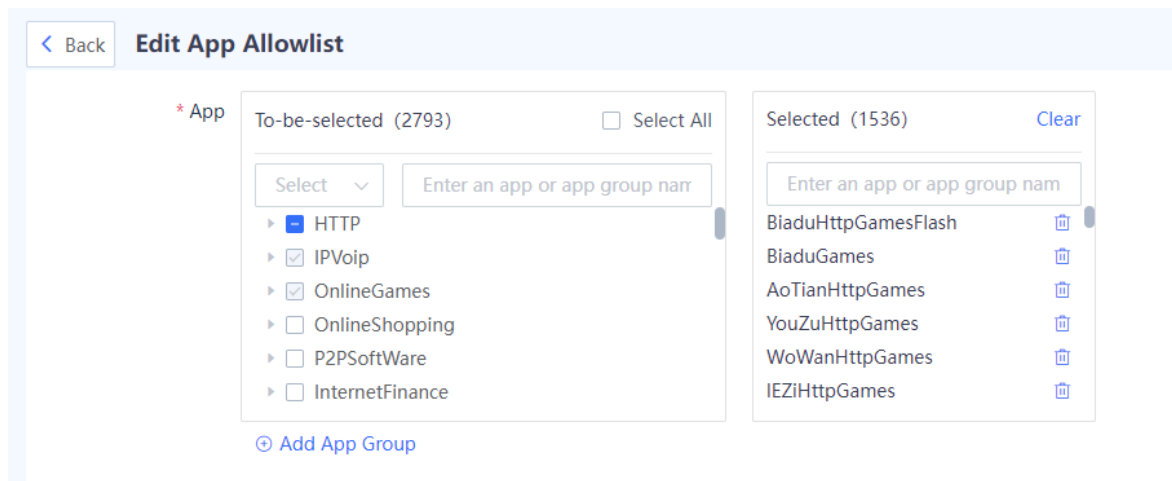
Procedure

- (1) Choose **Policy > SSL Proxy > SSL Proxy Allowlist > App Allowlist**.



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

The **Edit App Allowlist** page is displayed.



(3) Select an application in the **To-be-selected** area. The selected application is automatically added to the **Selected** area.

(4) After the configuration is completed, click **Save**.

Follow-up Procedure

To delete a custom application from the allowlist, click **Delete**. Applications in the predefined allowlist cannot be deleted.

6 Object Configuration and Management

6.1 Address Object

6.1.1 Overview

An address object is a collection of IP addresses, and an address group is a collection of address objects.

Address Group

An address object contains one or more IP addresses. It is a basic element, which needs to be defined only once and can be referenced by various policies, such as security policies and NAT policies.

For example, the subnet address of an office network is 192.168.1.0/24. To enable NAT for IP packets from this network, you can create an address object named **Office Area**, and add 192.168.1.0/24 to the address object. When configuring a NAT policy for the office network, you can reference the address object **Office Area**.

On the firewall, you can add the following types of addresses to an address object:

- Single IPv4 or IPv6 address
- IPv4 or IPv6 address range

Address Group Object

The members of an address group object are configured address objects. Address group objects makes address management more flexible.

For example, a company has finance, R&D, and marketing departments. Network resources that can be accessed by the departments are different, but all the three departments require NAT to access the Internet.

- Configure three address objects for these departments, and reference corresponding address object in the access control policy configured for each department.
- Create address group object **Company 1**, add the three address objects to the address group object, and reference **Company 1** in the NAT policy.

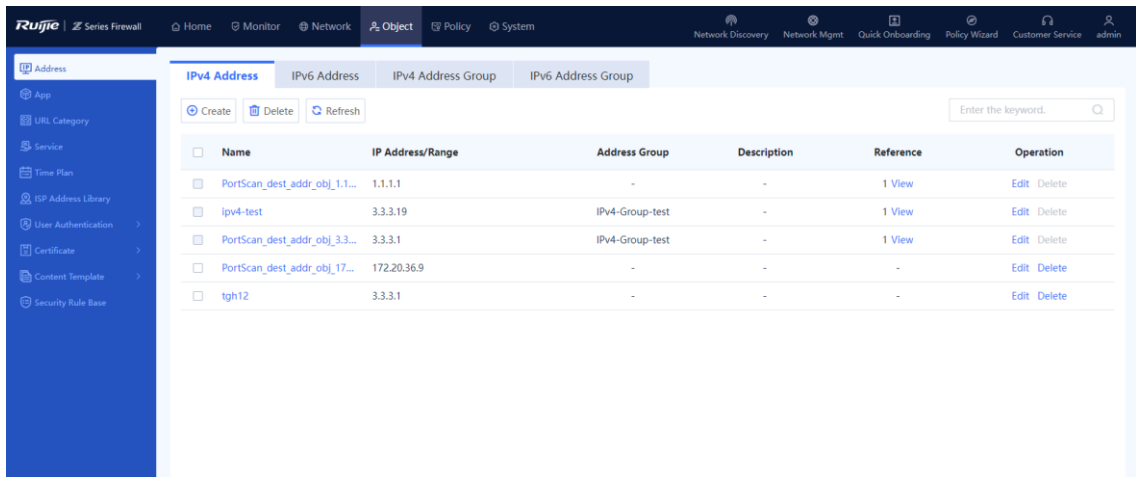
6.1.2 Creating an IPv4 Address Object

Application Scenario

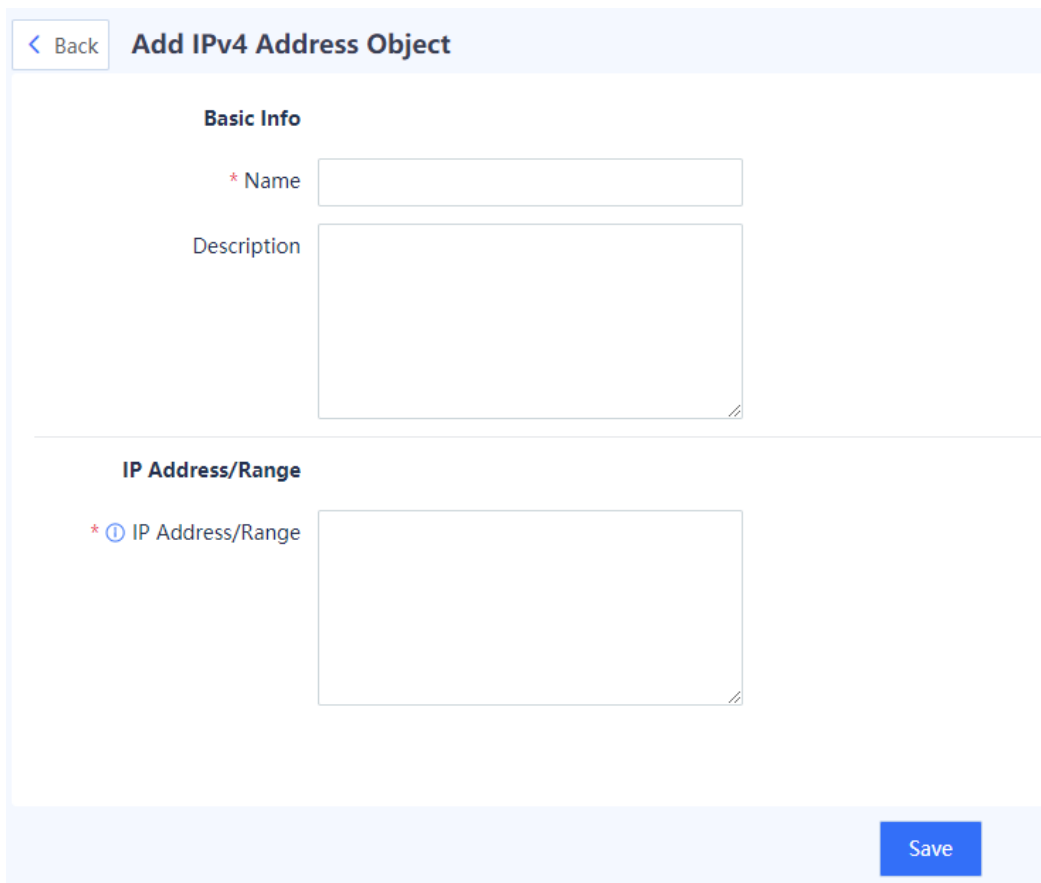
Create an address object on the web UI.

Procedure

- (1) Access the **Add IPv4 Address Object** page.
 - a Choose **Object > Address > IPv4 Address**.



b Click **Create**.



(2) Set parameters for the address object.

Item	Description	Remarks
Name	Name of the IP address object.	Characters such as `~!#%^&*+\\ {};:"'<>?` and spaces are not allowed. [Example] Addr1
Description	Description of the IP address object.	Characters such as `~!#%^&*+\\ {};:"'<>?` are not allowed. [Example] For office area 1
IP Address/Range	IP address or range.	Three configuration methods are supported: <ul style="list-style-type: none"> ● IP address: One or multiple IP addresses. Enter one IP address per line. Press Enter to separate lines. Example: 192.168.20.3 ● IP range: Range of IP addresses on the same subnet. Connect the start IP address and end IP address with a hyphen (-). Example: 192.168.20.1-192.168.20.3. ● Subnet: IP network segment. Example: 192.168.1.0/24 or 192.168.1.0/255.255.255.0

(3) Click **Save**.

Follow-up Procedure

- Click **Edit** to modify the description and IP range of an address object.
- Click **Delete** to delete an address object that is not referenced.

6.1.3 Creating an IPv4 Address Group Object

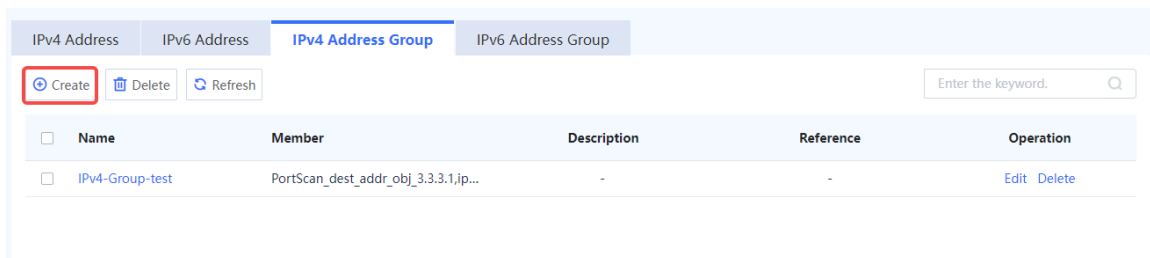
Application Scenario

Create an address group object on the web UI.

Procedure

(1) Access the **Add IPv4 Address Group** page.

a Choose Object > Address > IPv4 Address Group.



b Click **Create**.

< Back

Add IPv4 Address Group

Basic Info

* Name

Description

*** Included IP**

To-be-selected (13) Select All

Address Name	IP
<input type="checkbox"/> ipv4-test	3.3.3.19
<input type="checkbox"/> PortScan_des...	3.3.3.1
<input type="checkbox"/> PortScan_des...	172.20.36.9
<input type="checkbox"/> tgh12	3.3.3.1
<input type="checkbox"/> 85ggs	1.1.1.1

Selected (0) Clear

(2) Set parameters for the address group object.

Item	Description	Remarks
Name	Name of the address group object.	Characters such as `~!#%^&*+ \ {};:'"/<>? and spaces are not allowed. [Example] Addr_total
Description	Description of the address group object.	Characters such as `~!#%^&*+ \ {};:'"/<>? are not allowed. [Example] Address information of the entire company
Included IP	Address objects in the address group object.	Select address objects to be added in the To-be-selected area. The selected address objects are automatically added to the Selected area. [Example] Address Object 1

(3) Click **Save**.

Follow-up Procedure

- Click **Edit** to modify the description and members of an address group object.
- Click **Delete** to delete an address group object that is not referenced.

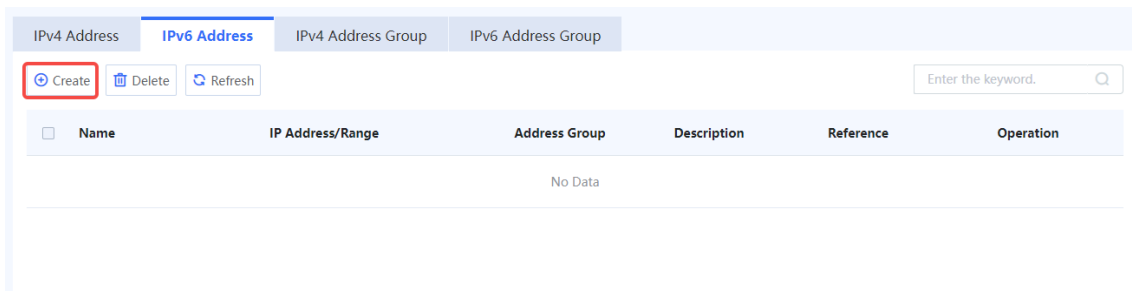
6.1.4 Creating an IPv6 Address Object

Application Scenario

Create an address object on the web UI.

Procedure

- (1) Access the **Add IPv6 Address Object** page.
 - a Choose Object > Address > IPv6 Address.



- b Click **Create**.

The screenshot shows the 'Add IPv6 Address Object' form. At the top left, there is a '< Back' button. The main title is 'Add IPv6 Address Object'. The form is divided into two sections: 'Basic Info' and 'IP Address/Range'. Under 'Basic Info', there is a required field for 'Name' (marked with a red asterisk) and a text area for 'Description'. Under 'IP Address/Range', there is a required field for 'IP Address/Range' (marked with a red asterisk and a help icon) and a text area for the IP address range.

- (2) Set parameters for the address object.

Item	Description	Remarks
Name	Name of the IP address object.	Characters such as `~!#%^&*+\\ {};:"' /<>?` and spaces are not allowed. [Example] Addr1
Description	Description of the IP address object.	Characters such as `~!#%^&*+\\ {};:"' /<>?` are not allowed. [Example] For office area 1
IP Address/Range	IP address or range.	Three configuration methods are supported: <ul style="list-style-type: none"> ● IP address: One or multiple IP addresses. Enter one IP address per line. Press Enter to separate lines. Example: 1234::100 ● IP range: Range of IP addresses on the same subnet. Connect the start IP address and end IP address with a hyphen (-). Example: 1234::100-2345::100 ● Subnet: IP network segment. Example: 1234::100/100

(3) Click **Save**.

Follow-up Procedure

- Click **Edit** to modify the description and IP range of an address object.
- Click **Delete** to delete an address object that is not referenced.

6.1.5 Creating an IPv6 Address Group Object

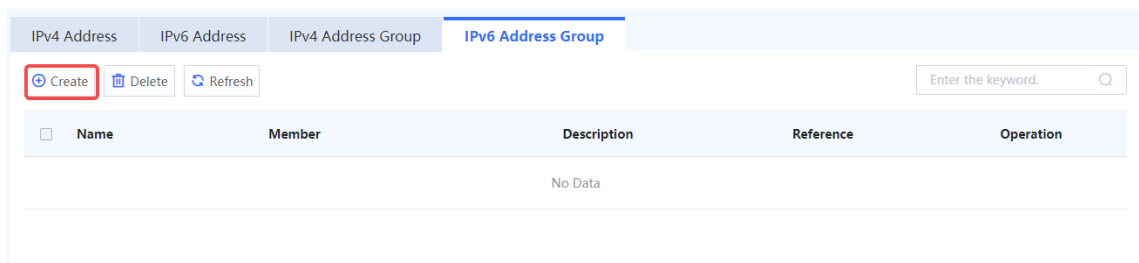
Application Scenario

Create an address group object on the web UI.

Procedure

(1) Access the **Add IPv6 Address Group** page.

a Choose **Object > Address > IPv6 Address Group**.



b Click **Create**.

< Back

Add IPv6 Address Group

Basic Info

* Name

Description

*** Included IP**

To-be-selected (0) Select All

Enter the keyword.

Address Name

IP

Selected (0) Clear

Enter the keyword.

(2) Set parameters for the address group object.

Item	Description	Remarks
Name	Name of the address group object.	Characters such as `~!#%^&*+ \ {};:"'/<>?` and spaces are not allowed. [Example] Addr_total
Description	Description of the address group object.	Characters such as `~!#%^&*+ \ {};:"'/<>?` are not allowed. [Example] Address information of the entire company
Included IP	Address objects in the address group object.	Select address objects to be added in the To-be-selected area. The selected address objects are automatically added to the Selected area. [Example] Address Object 1

(3) Click **Save**.

Follow-up Procedure

- Click **Edit** to modify the description and members of an address group object.
- Click **Delete** to delete an address group object that is not referenced.

6.2 Application

6.2.1 Overview

To identify different applications that use the same protocol and port number, the concept of applications is introduced on the Z-S series firewall. The firewall can accurately identify a variety of common applications based on application features. For example, both gaming and videos on web pages use the HTTP protocol and port 8080 for data transmission. The two types of applications can be distinguished based on application features.

By analyzing common applications, Ruijie Networks has built an application identification signature library. The library has predefined features of common applications, which can be used for identifying various applications. After loading the application identification signature library, the firewall can identify applications that have been defined in the signature library. These applications are displayed as predefined applications on the firewall.

 Note

Predefined applications cannot be modified or deleted. You can obtain the latest predefined applications by regularly upgrading the application identification signature library.

6.2.2 Viewing Application Information in a Signature Library

Application Scenario

View application information defined by the system.

Procedure

- (1) Choose **Object > App > App**.
- (2) View application details.

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
MeituxiuxiurMeiyan	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

The following table describes application details.

Item	Description
App Group	Application group that the application belongs to.
Reputation Level	The default reputation level of the application, which cannot be modified. For details about reputation levels, see 9.2.2 2. Querying Security Logs . To ensure that the reputation levels are correct, update the application identification signature library timely. For details about signature library upgrade, see 8.5 Signature Library Upgrade .
Reference	Application reference information. For example, an application is referenced by a custom application group or associated with a security policy.

Note

The application types are displayed in the left pane, and the corresponding applications are displayed on the right.

Follow-up Procedure

- Enter keywords in the search box to perform a fuzzy search on applications.
- When **Reference** is not 0, you can click **View** to check application reference details. A lower-level application inherits the application group and policy association information from its upper-level application.

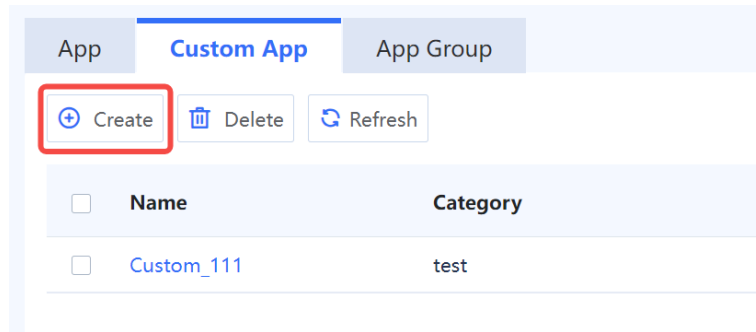
6.2.3 Creating a Custom Application

Application Scenario

The device provides common application information. You can customize application information as needed to enhance the application identification capability of the device.

Procedure

- (1) Choose **Object > App > Custom App**.
- (2) Click **Create**.



- (3) Configure the parameters for the custom application.

Add Custom App ⊗

* Name Enter the value.

Category Custom Type Select from existing categories.

* Category Name

* App Rule

Protocol Type	Src. IP	Dest. IP	Dest. Port	Operation
No Data				

Item	Description	Remarks
Name	Name of the custom application. The naming format is Custom_Name .	<ul style="list-style-type: none"> The name cannot contain characters such as `~!#%^&*+ {};:~"/<>?` and spaces. The name must be different from existing application names. Once the application is created, you cannot modify its name. <p>[Example] Custom_app_1</p>

Item	Description	Remarks
Category	Customize the application category. You can customize a category or select an existing category.	-
App Rule	Configure the matching rules of the custom application. The traffic matching the rules is classified as the traffic of the application.	Click Create next to App Rule to add traffic matching rules for the application.

(4) Click **Confirm**. To add more custom applications, click **Confirm** and **Continue Adding**.

Follow-up Procedure

After a custom application is added, you can create an application group to categorize it. You can also create a security policy to perform access control on the traffic to access the custom application.

6.2.4 Creating a Custom Application Group

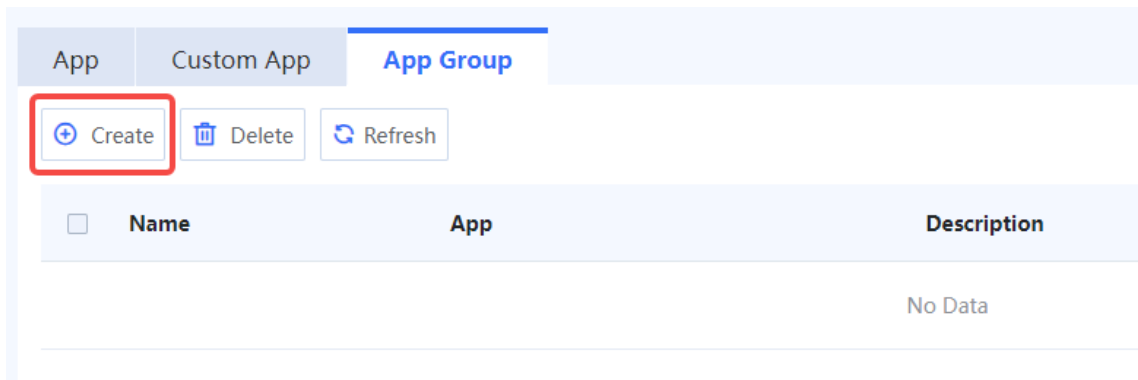
Application Scenario

To simplify management, you can combine applications with the same management requirements into an application group.

Procedure

(1) Access the **Add App Group** page.

a Choose **Object > App > App Group**.



b Click **Create**.

(2) Set parameters for the application group.

Item	Description	Remarks
Name	Name of the custom application group.	<ul style="list-style-type: none"> ● Characters such as `~!#%^&*+ \{\};:~'"</>?` and spaces are not allowed. ● The name of an existing application cannot be used. ● After the application group is created, the name cannot be modified. [Example] Zone1
Description	Description of the custom application group.	Characters such as `~!#%^&*+ \{\};:~'"</>?` are not allowed. [Example] New app group
Included App	Applications in the custom application group.	Select applications in the To-be-selected area. The selected applications are automatically added to the Selected area.

(3) Click **Save**.

Follow-up Procedure

- After creating an application group, you can view the detailed information about the group.

Item	Description
App	Applications in the application group.

Item	Description
Reference	The reference times of the application group and the reference details.

- Enter keywords in the search box to perform a fuzzy search on custom application groups.
- When **Reference** is not 0, you can click **View** to check the security policies associated with the application group.
- You can delete an application group when it is no longer in use. When the application group is associated with a policy, the application group cannot be deleted directly. You need to disassociate the application group from the policy first.

6.2.5 Upgrading an Application Identification Signature Library

Upgrade the application identification library timely to improve the application identification capability of the firewall. For details about signature library upgrade, see [8.5 Signature Library Upgrade](#).

6.3 URL Category

6.3.1 Overview

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. For details about URL filtering templates, see [6.9.3 URL Filtering](#).

6.3.2 Viewing Predefined URL Categories

Application Scenario

View URL categories predefined on the system.

Prerequisites

You have installed and activated the URL category license. For details about license activation, see [8.3 Activating the License](#).

Procedure

- (1) Choose **Object > URL Category > Predefined URL Category**.
- (2) View details about predefined URL categories.

Name	Description	Reference
Portal-Navigation	Web portals and websites that provide content navigation, including governme...	1 View
Search Engine	Web search engines, such as Google, and industry search engines	1 View
Online Shopping	C2C, B2B, and B2C online shopping websites, online stores, online transaction ...	1 View
Sports	Websites with contents related to sports (including sporting goods, sports com...	1 View

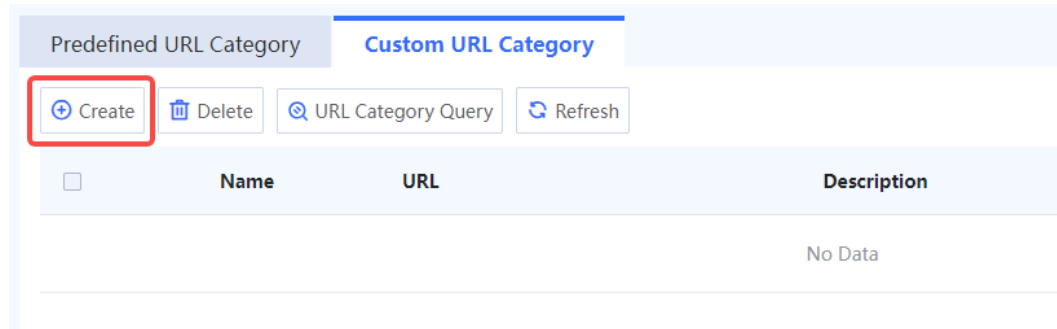
6.3.3 Configuring a Custom URL Category

Application Scenario

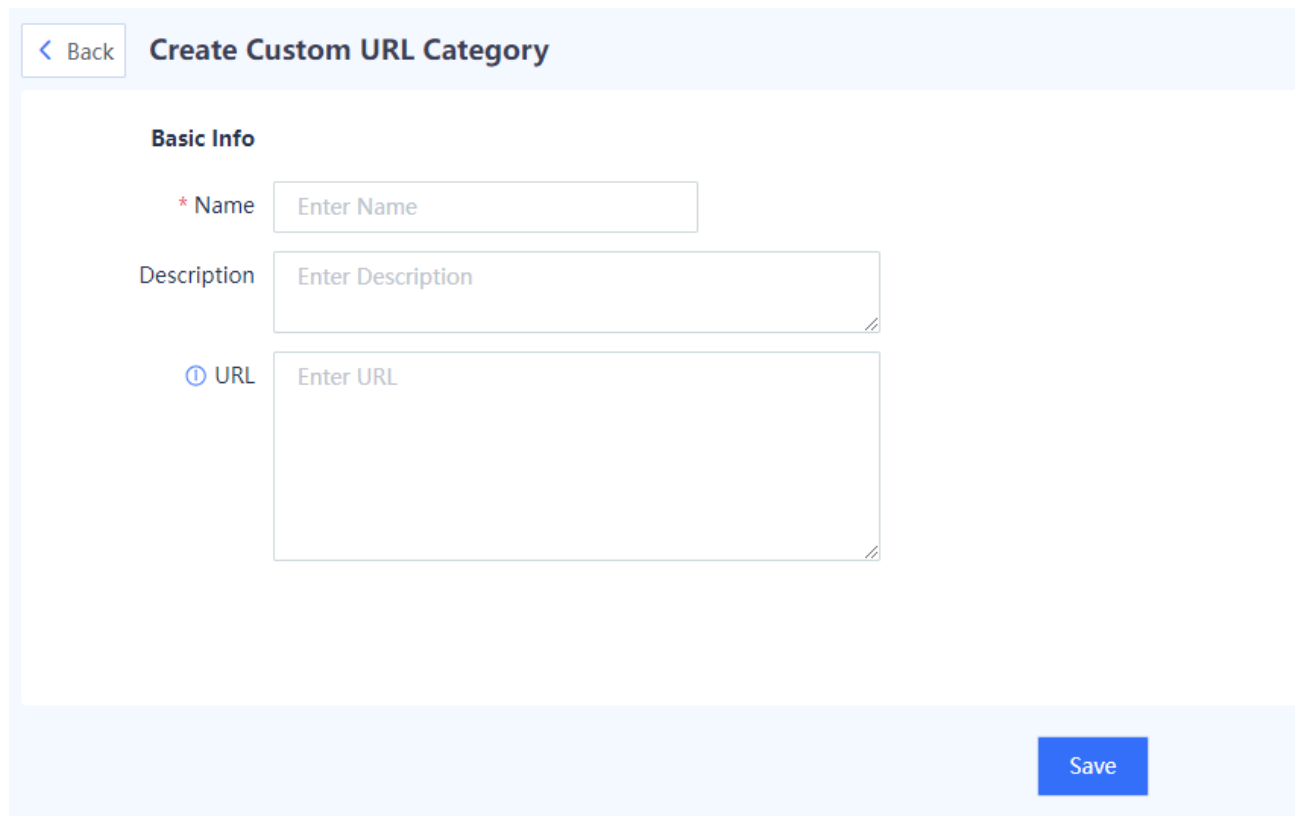
The device provides common URL categories. You can create custom URL categories as needed to monitor and manage the types of web pages that intranet users can access.

Procedure

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



- (3) Enter URL category information.



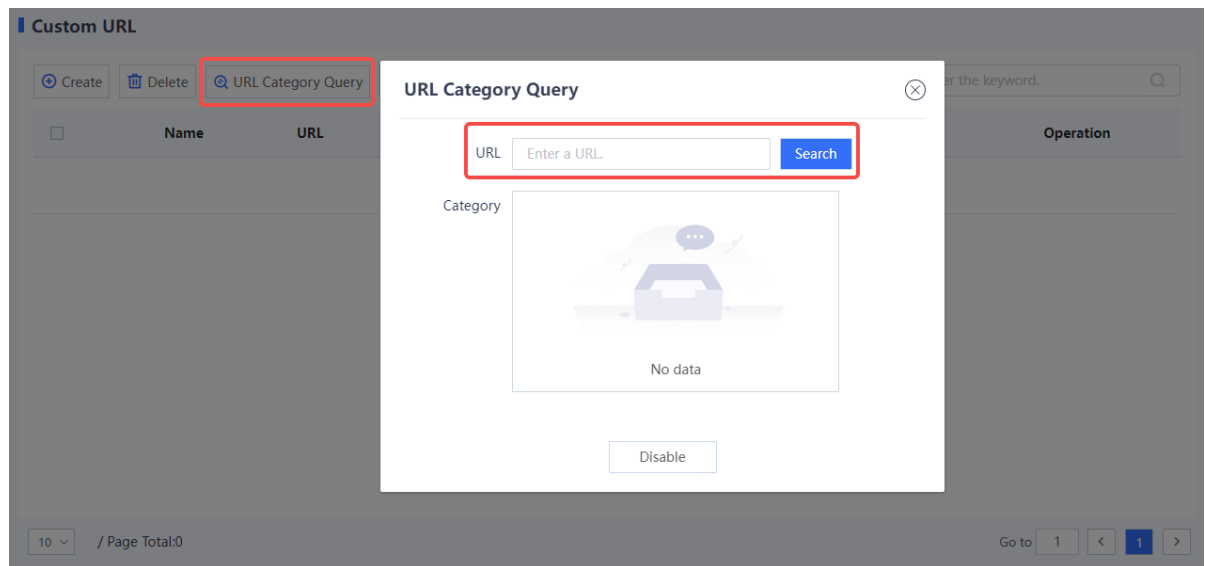
Item	Description	Remarks
Basic Info		

Item	Description	Remarks
Name	URL category name.	[Example] category_1
Description	Description of the URL category.	N/A
URL	<p>URLs in this category. A URL can contain the wildcard character (*). Enter one URL per line. Press Enter to separate lines.</p> <p>Note:</p> <ul style="list-style-type: none"> ● If a URL contains the pound sign (#), the sign and the string after the sign do not take effect for matching. For example, if www.test.com/#123 is configured, all the domain names that start with www.test.com/ will be matched. ● If a URL contains the characters http:// or https://, these characters will be automatically removed during matching. ● If an IPv6 address is configured as a URL, the input format should be [IPv6 address]. For example, [2001::1]. 	[Example] www.abc1.com www.abc2.com

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

Follow-up Procedure

- To delete multiple URL categories in a batch, select the categories and click **Delete**. Only URL categories with no reference can be deleted.
- Click **URL Category Query**. In the dialog box that is displayed, enter a URL to query its category.



6.4 Services

6.4.1 Overview

A service type refers to services that use one application protocol or a collection of application protocols. An application protocol is identified by the protocol type, source port, destination port, and other information.

You can combine multiple services into a service group to facilitate management.

The firewall can identify common application protocols based on services and service groups. If the protocol type and port number of data traffic match the conditions of a service type, the traffic is considered as the traffic of the specific application protocol. A security policy or traffic control policy can be applied to data flows that match the conditions based on services or service groups.

The Z-S series firewall supports the following two service types:

- **Predefined service**

Predefined services are default service types in the system and can be selected directly. They are services using common protocols such as HTTP, FTP, and Telnet. Typically, these services are defined by port. Therefore, if the port used by a protocol on the live network differs from the port predefined for the device, you need to create a custom service. For example, the port number of the predefined HTTP service is 80. However, port 80 is occupied on the live network. In this case, you need to configure a custom port number for the HTTP service and reference it in security policies to control packets of this application protocol.

 **Note**

Predefined services cannot be deleted.

- **Custom service**

The application protocol is defined by protocol type (for example, TCP, UDP, or ICMP), port number, or other information.

- For TCP and UDP packets, a series of ports or port ranges are used to identify the application protocol type.
- For ICMP packets, the ICMP type name and code fields are used to identify packets.
- For IP packets, protocol numbers are used to identify packets.

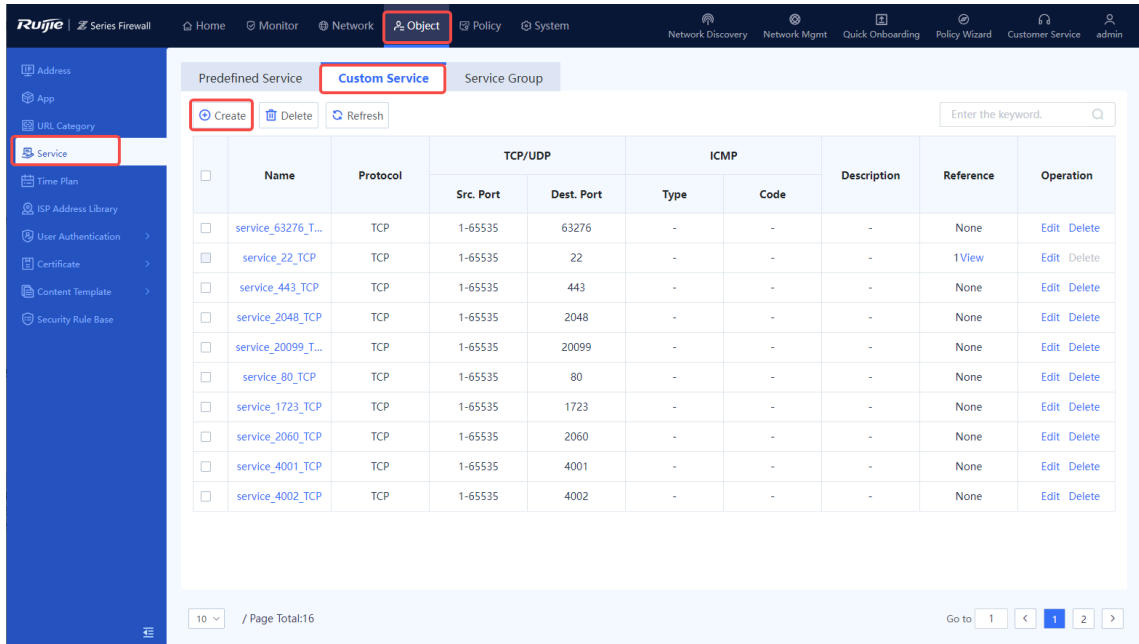
6.4.2 Configuring a Custom Service

Application Scenario

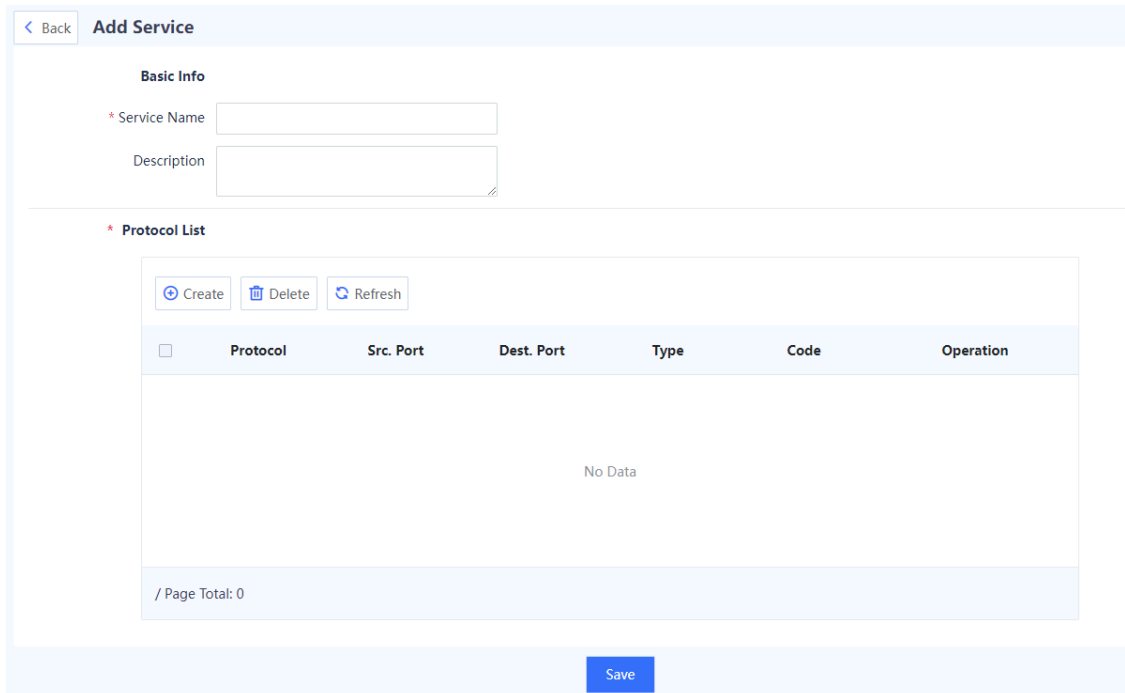
Define the application protocol by protocol type (for example, TCP, UDP, or ICMP), port number, or other information.

Procedure

- (1) Access the **Add Service** page.
 - a Choose **Object > Service > Custom Service**.
 - b Click **Create**.



(2) Set parameters for the service.



Item	Description	Remarks
Basic Info		

Item	Description	Remarks
Service Name	Name of the new service.	<ul style="list-style-type: none"> ● Characters such as `~!#%^&*+ \{};:'"/<>?` and spaces are not allowed. ● The name of an existing service cannot be used. ● After the service is created, the name cannot be modified. [Example] Service 1
Description	Description of the new service.	Characters such as `~!#%^&*+ \{};:'"/<>?` are not allowed. [Example] New service
Protocol List Protocols of the new service. Click Create . In the Add Protocol Config dialog box, configure parameters and click Confirm .		
TCP	Services that use the TCP protocol.	The parameters are as follows: <ul style="list-style-type: none"> ● Protocol Number ● Src. Port ● Dest. Port
UDP	Services that use the UDP protocol.	The parameters are as follows: <ul style="list-style-type: none"> ● Protocol Number ● Src. Port ● Dest. Port
ICMP	Services that use the ICMP protocol.	The parameters are as follows: <ul style="list-style-type: none"> ● Protocol Number ● Type ● Code
ICMPv6	Services that use the ICMPv6 protocol.	The parameters are as follows: <ul style="list-style-type: none"> ● Protocol Number: 58 ● Type ● Code
IP Protocol Number	IP protocol numbers used by services.	Protocol number range: 0–256. The value 256 indicates all protocol numbers in the range of 0–255, except 1, 6, 17, and 58.

(3) Click **Confirm**.

Follow-up Procedure

- You can only delete the service with no reference.

- You cannot add, delete, or modify predefined services. To view these services, choose **Object > Service > Predefined Service**. Predefined services are service types that are commonly used.

6.4.3 Creating a Service Group

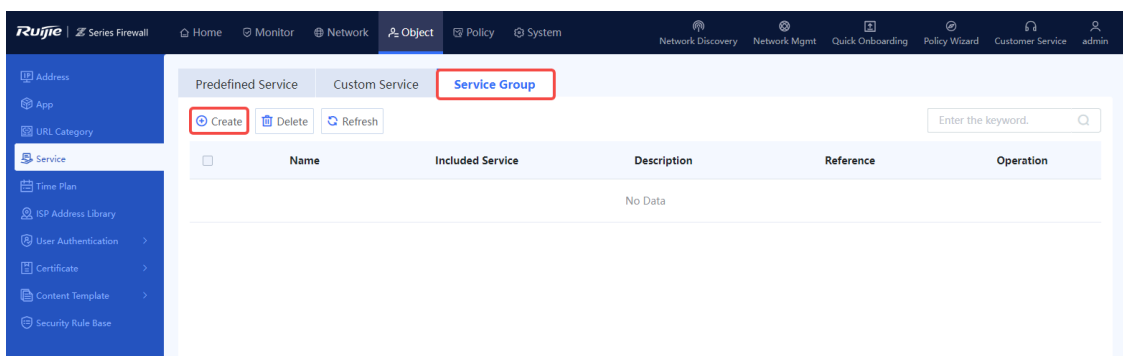
Application Scenario

You can create a service group to manage multiple services.

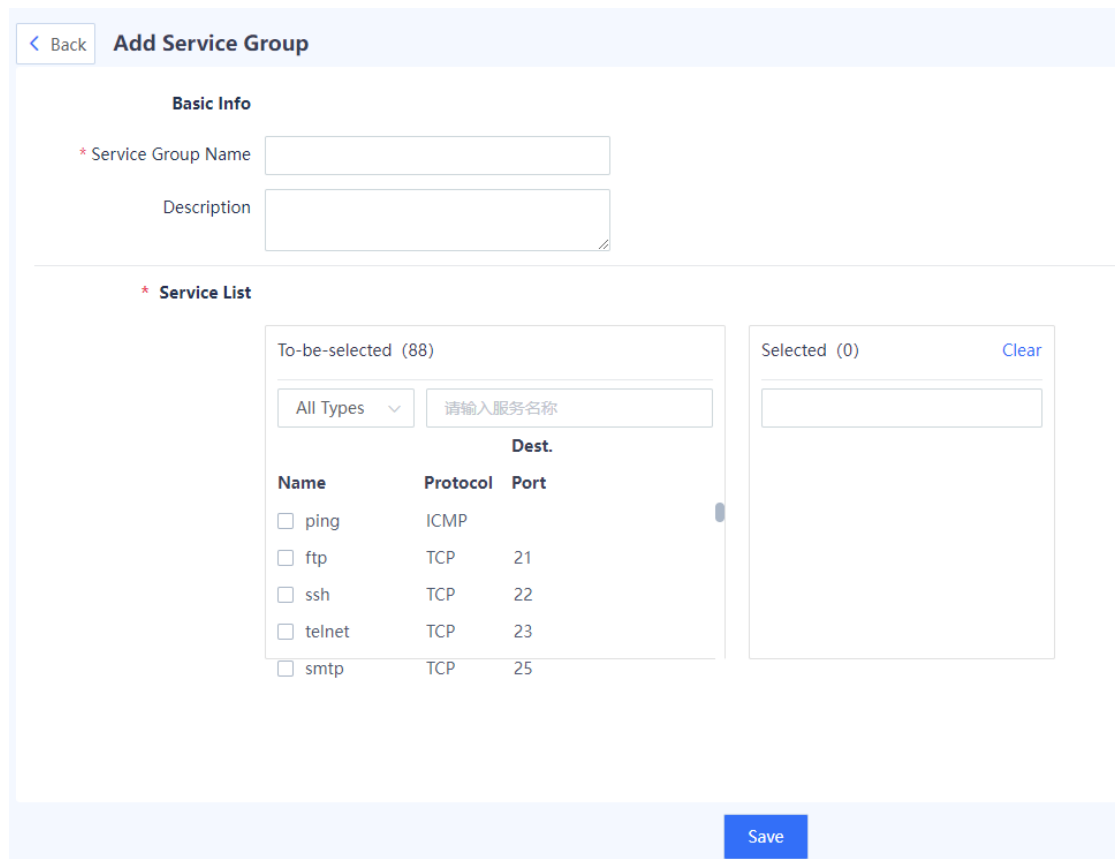
Both custom and predefined services can be added to service groups.

Procedure

- Access the **Add Service Group** page.
 - Choose **Object > Service > Service Group**.
 - In the operation area, click **Create**.



- Set parameters for the service group.



Item	Description	Remarks
Basic Info		
Service Group Name	Name of the new service group.	<ul style="list-style-type: none"> ● Characters such as `~!#%^&*+\\{};:~"/<>?` and spaces are not allowed. ● The name of an existing service group cannot be used. [Example] Service_group_1
Description	Description of the new service group.	Characters such as `~!#%^&*+\\{};:~"/<>?` are not allowed. [Example] New service group
Service List	Services in the new service group.	Select services in the To-be-selected area. The selected services are automatically added to the Selected area. [Example] ssh

(3) Click **Save**.

Follow-up Procedure

You can only delete the service group with no reference.

6.5 Time Plan

6.5.1 Overview

A time plan controls the effective time range of various policies to manage the network.

Time plan types:

- One-off time plan

Time range between the configured start time and end time. This plan does not have a cycle.

For example, you can define a one-off time plan to allow employees to access the extranet only from 2022-04-30 19:00:00 to 2022-05-01 24:00:00.

- Cyclic time plan

A fixed time period in each week, which is determined by the start time, end time, and weekly effective time.

For example, you can define a cyclic time plan to allow employees to access the extranet only from 19:00:00 to 22:00:00 every Friday night.

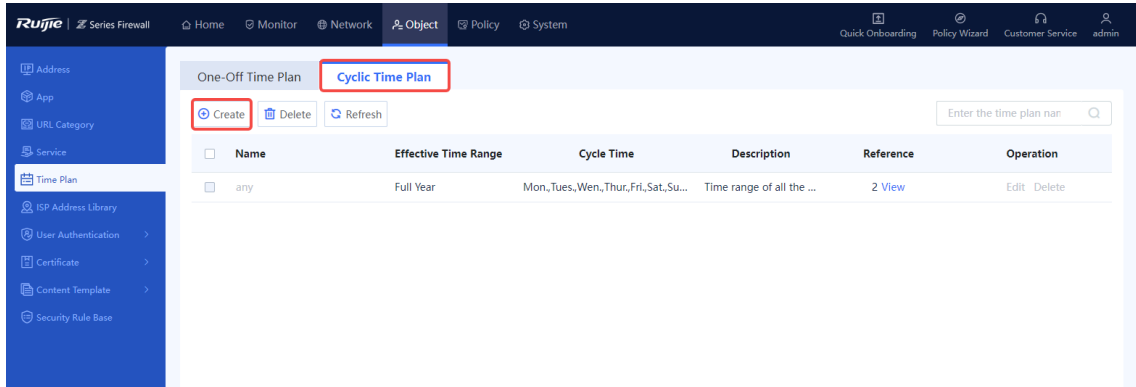
6.5.2 Creating a Cyclic Time Plan

Application Scenario

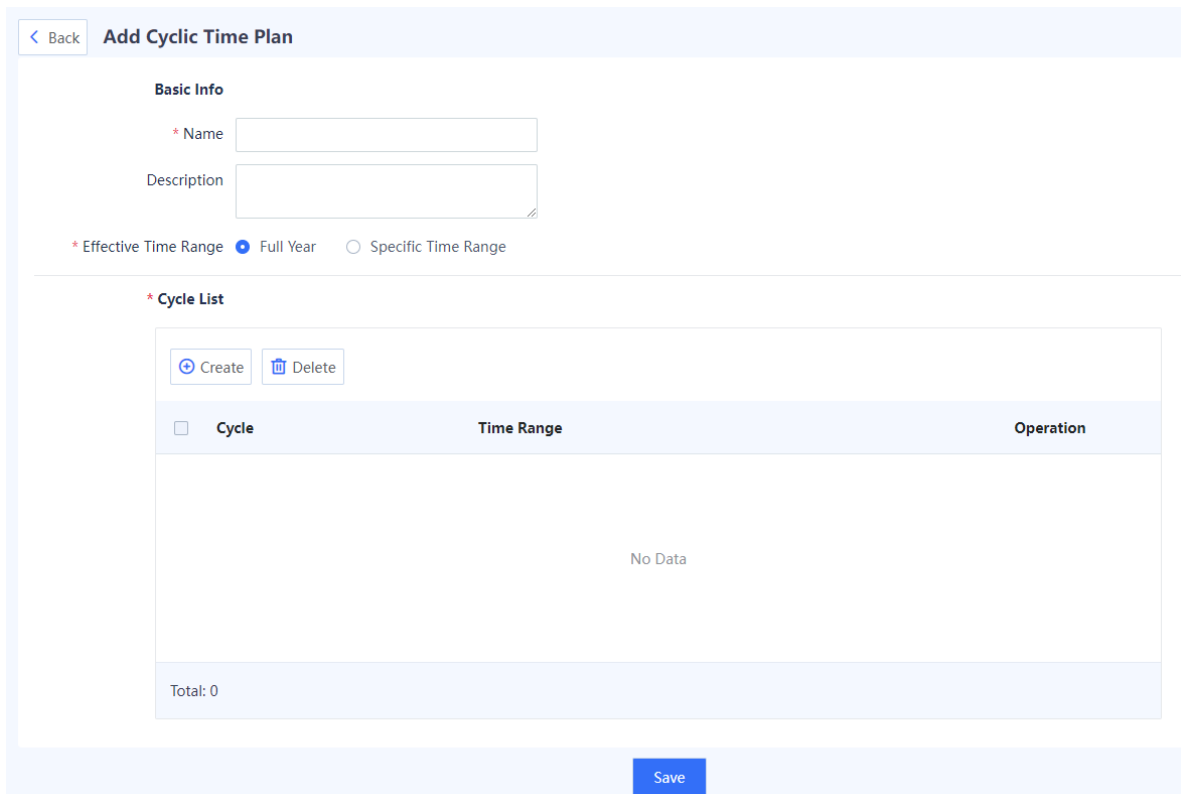
Configure a cyclic time plan to make policies take effect within the specified time range.

Procedure

- (1) Access the **Add Cyclic Time Plan** page.
 - a Choose **Object > Time Plan > Cyclic Time Plan**.
 - b In the operation area, click **Create**.



- (2) Set parameters for the cyclic time plan.



Item	Description	Remarks
Name	Name of the new cyclic time plan.	Characters such as `~!#%^&*+\\ {};:"'/<>?` and spaces are not allowed. [Example] Plan 1
Description	Description of the new cyclic time plan.	Characters such as `~!#%^&*+\\ {};:"'/<>?` are not allowed. [Example] Plan 1
Effective Time Range	Effective time range of the new cyclic time plan.	By default, a time plan takes effect all year round. You can set a specific effective time range. [Example] Full
Cycle List	Time policy of the cyclic time plan.	Click Create to select days per week and specific time period to execute the plan.

(3) Click **Save**.

Follow-up Procedure

You can only delete the cyclic time plan with no reference.

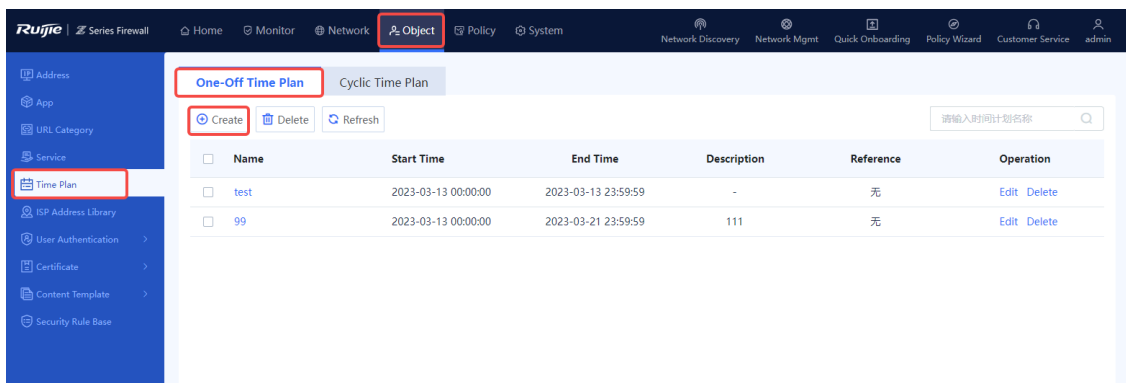
6.5.3 Creating a One-Off Time Plan

Application Scenario

Configure a one-off time plan to execute policies only once.

Procedure

- (1) Access the **Add One-Off Time Plan** page.
 - a Choose **Object > Time Plan > One-Off Time Plan**.
 - b In the operation area, click **Create**.



(2) Set parameters for the one-off time plan.

< Back
Add One-Off Time Plan

* Name

Description

* Start Time

* End Time

Item	Description	Remarks
Name	Name of the new one-off time plan.	Characters such as `~!#%^&*+\\ {};:"'/<>?` and spaces are not allowed. [Example] Plan 1
Description	Description of the new one-off time plan.	Characters such as `~!#%^&*+\\ {};:"'/<>?` are not allowed.
Start Time	Start time of the new one-off time plan.	[Example] 2022-02-16 00:00:00
End Time	End time of the new one-off time plan.	[Example] 2022-02-16 12:00:00

(3) Click **Save**.

Follow-up Procedure

You can only delete the one-off time plan with no reference.

6.6 ISP Address Library

6.6.1 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. In this way, 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 addresses or import addresses in file format to the library.

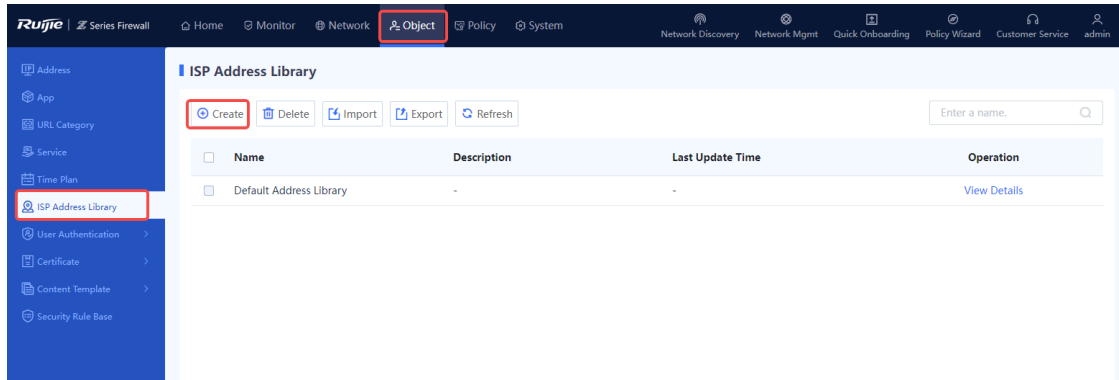
6.6.2 Creating an ISP Address Library Manually

Application Scenario

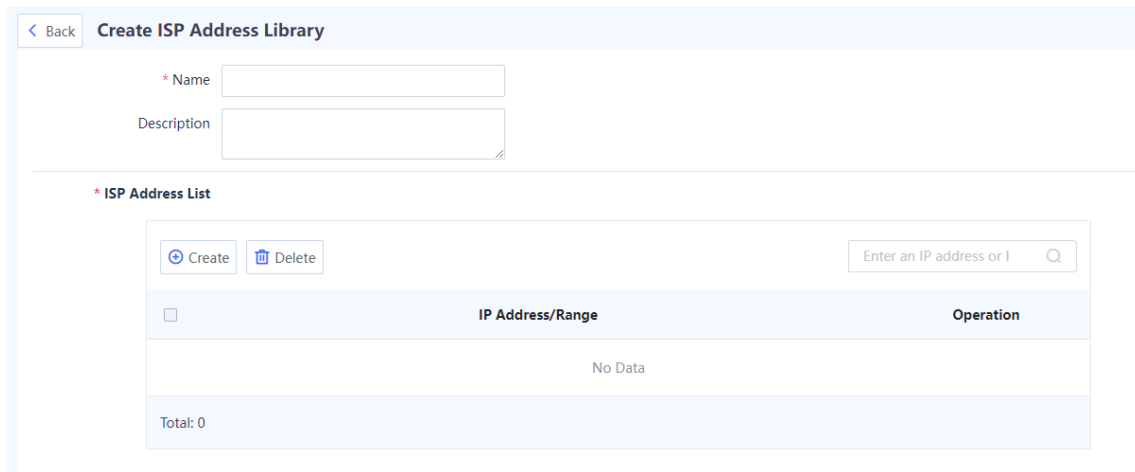
You can add addresses to the ISP address library one by one. This method is applicable to the address library containing a few addresses.

Procedure

- (1) Access the **Create ISP Address Library** page.
 - a Choose **Object > ISP Address Library**.
 - b In the operation area, click **Create**.



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



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.

Item	Description	Remarks
ISP Address List	IP addresses contained in the address library.	<p>Click Create to enter a single IP address or an IP address range. Three configuration methods are supported:</p> <ul style="list-style-type: none"> ● IP address: One or multiple IP addresses. Input an IP address per line. Press Enter to separate lines. Example: 192.168.20.3 ● IP 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. ● Subnet: IP network segment. Example: 192.168.1.0/24 or 192.168.1.0/255.255.255.0

(3) Click **Save**.

Follow-up Procedure

- To delete a created ISP address library, select the library and click **Delete**.

Caution

- The ISP address library in use (that is, associated with a device interface) cannot be deleted.
- The default address library predefined in the system cannot be deleted or modified.

- Select an ISP address library and click **Export** to export the ISP address library file to a local PC. Then, you can check the file or import the file to another firewall to create the ISP address library on the new firewall.

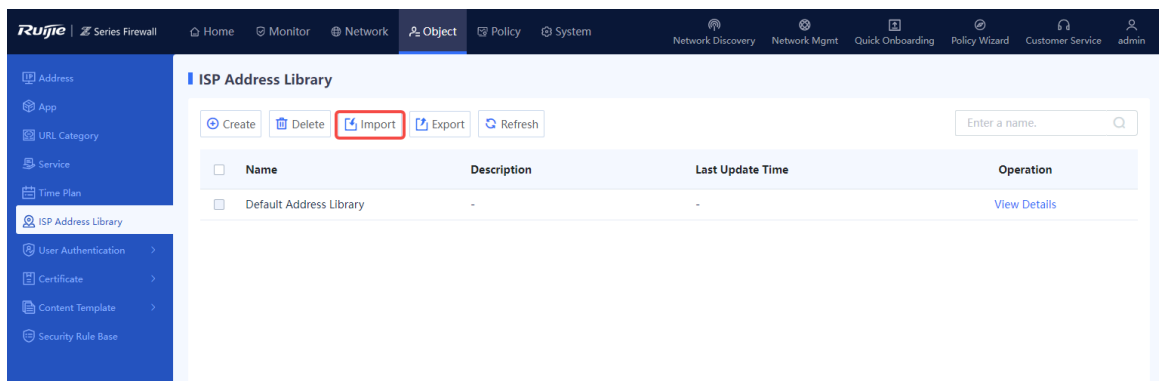
6.6.3 Creating an ISP Address Library by Importing an Address File

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**. In the operation area, click **Import**.



(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 an imported ISP address library, select the library and click **Delete**.

Caution

- The ISP address library in use (that is, associated with a device interface) cannot be deleted.
 - The default address library predefined in the system cannot be deleted or modified.
-

- To modify the IP addresses included in the address library, click **Edit**.

6.6.4 Upgrading an ISP Address Library

The ISP address library is continuously updated. After the ISP address library is upgraded, the device can obtain and generate the latest routes based on the library. For details about signature library upgrade, see [8.5 Signature Library Upgrade](#).

6.7 User Authentication

6.7.1 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:

- o 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.

6.7.2 User Management

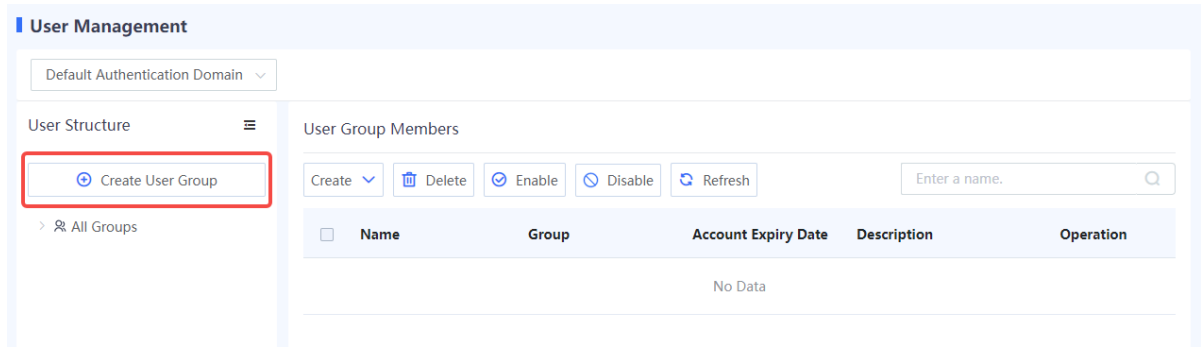
1. Configuring User Groups

Application Scenario

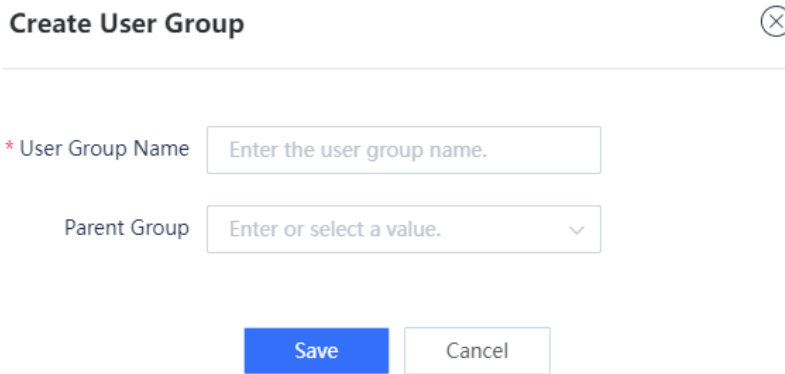
Add users with similar attributes such as the same resource access requirements to a user group to facilitate unified management.

Procedure

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



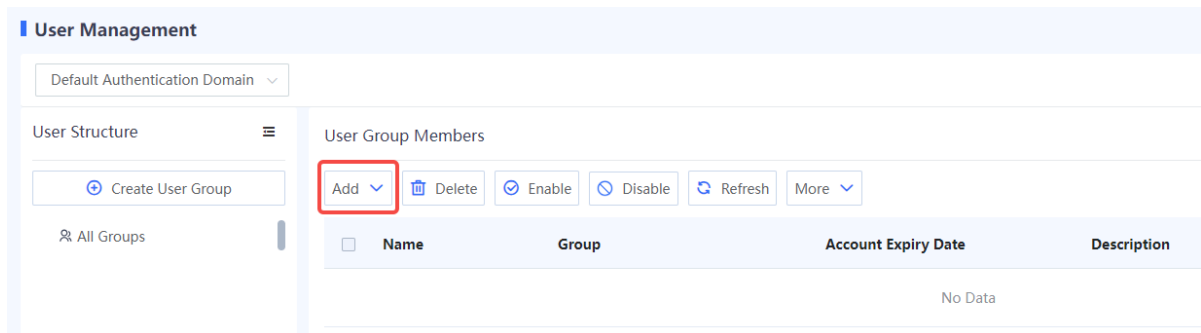
(3) Enter the user group name and select a parent group.



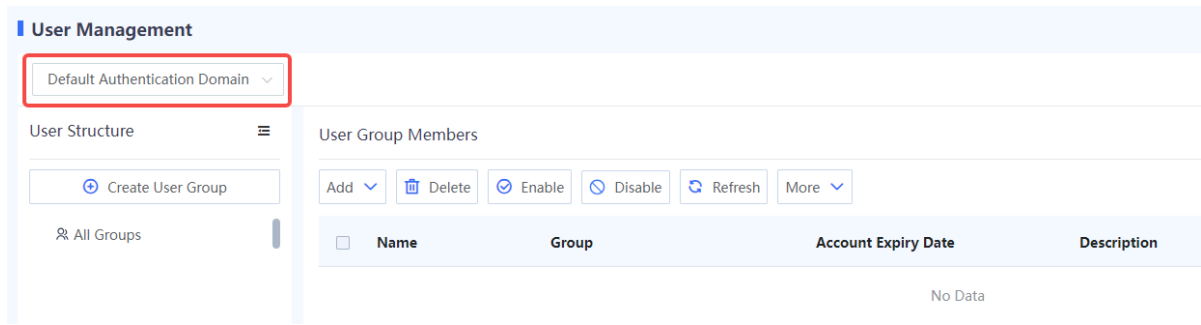
(4) After verifying the configuration, click **Save**.

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.



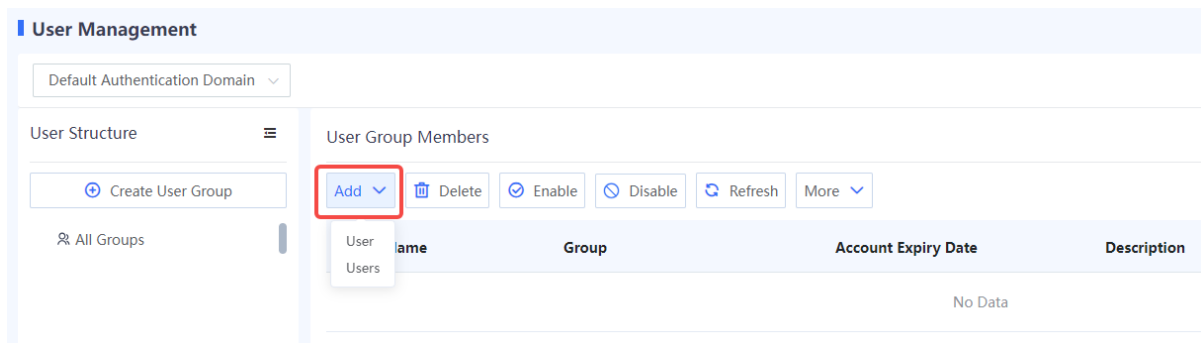
2. Configuring Users

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
Basic Info		
Login Username	Username for the remote user to log in to the virtual gateway.	[Example] user1
Enabled State	Whether to enable user information for authentication. Users in disabled status cannot be authenticated.	[Example] Enable
Displayed Username	Username displayed on the virtual gateway after authentication. The value can be the same as that of Login Username .	[Example] user1
Group	Group to which the user belongs.	[Example] /default
Description	User description.	N/A
Password		

Item	Description	Remarks
Password	Password for the remote user to log in to the virtual gateway. For details about password complexity requirements, see 6.7.7 Authentication Settings .	N/A
Confirm Password	The value must be the same as that of Password .	N/A
Advanced Settings		
Bind IP/MAC	Whether to specify the IP or MAC address for user login: <ul style="list-style-type: none"> ● Not Bind: Unrestricted. ● One-Way Binding: A user can log in to the virtual gateway using only the specified IP or MAC address. ● Two-Way Binding: A user can log in to the virtual gateway using only the specified IP and MAC addresses. 	N/A
Expiry Date	Expiry date of user identity information. When the expiry date is reached, the user is forced to go offline and cannot be authenticated again.	[Example] Permanent

- Adding users in a batch

< Back

Batch Add Users

Basic Info

* ⓘ Login Username

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
Basic Info		
Login Username	Usernames for the remote users to log in to the virtual gateway on the SSL VPN client. Separate usernames with commas.	[Example] user1,user2
Enabled State	Whether to enable user information for authentication. Users in disabled status cannot be authenticated.	[Example] Enable
Group	Group to which the user belongs.	[Example] /default
Description	User description.	N/A
Password		
Password	Shared password for the remote users to log in to the virtual gateway on the SSL VPN client.	N/A
Confirm Password	The value must be the same as that of Password .	N/A

Item	Description	Remarks
Advanced Settings		
Bind IP/MAC	Whether to specify the IP or MAC address for user login: <ul style="list-style-type: none"> ● Not Bind: Unrestricted. ● One-Way Binding: A user can log in to the virtual gateway using only the specified IP or MAC address. ● Two-Way Binding: A user can log in to the virtual gateway using only the specified IP and MAC addresses. 	N/A
Expiry Date	Expiry date of user identity information. When the expiry date is reached, the user is forced to go offline and cannot be authenticated again.	[Example] Permanent

(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.

6.7.3 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.

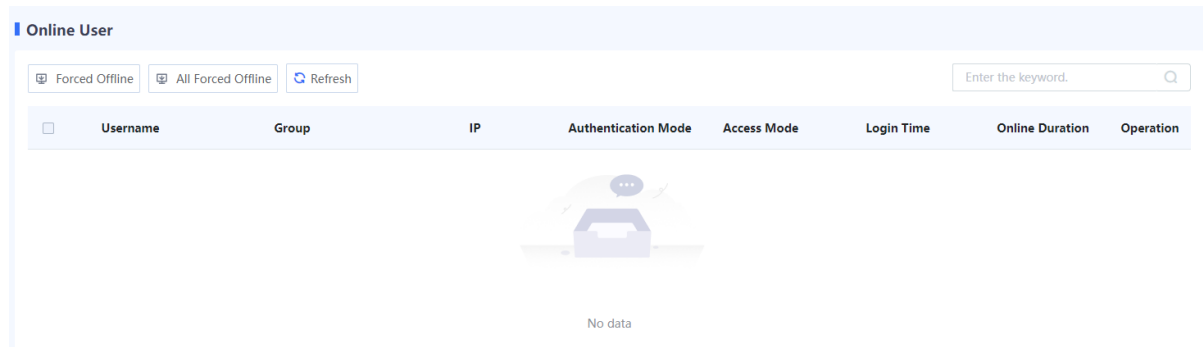
6.7.4 Online User

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**.



6.7.5 Authentication Domain Management

Application Scenario

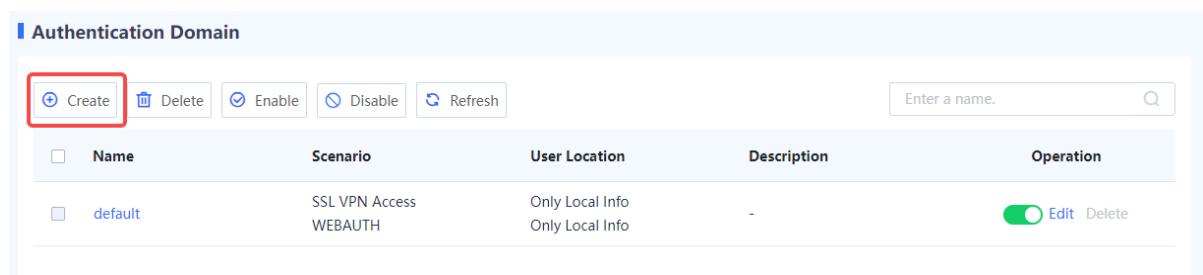
For SSL VPN access or scenarios requiring web authentication, the firewall implements the same policies, including login authentication and resource authorization, for users in the same authentication domain, facilitating unified management.

Prerequisites

You have configured user information on the firewall or authentication server. For details, see [6.7.2 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
Basic Info		
Name	Authentication domain name.	[Example] auth_domain_1
Enabled State	Whether to enable the authentication domain.	[Example] Enable
Description	Authentication domain description.	N/A
User Management		
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"> ● Prefer Info on Server: User identity information, including the username and password, is stored on the authentication server or local firewall. The information on the authentication server is preferentially used for authentication. ● Prefer Local Info: User identity information, including the username and password, is stored on the authentication server or local firewall. The information on the local firewall is preferentially used for authentication. ● Only Info on Server: User identity information, including the username and password, is stored on the authentication server for authentication. ● Only Local Info: User identity information, including the username and password, is stored on the local firewall for authentication. 	N/A
Authentication Server	Authentication server.	N/A
Advanced Settings (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**.

6.7.6 Authentication Policies

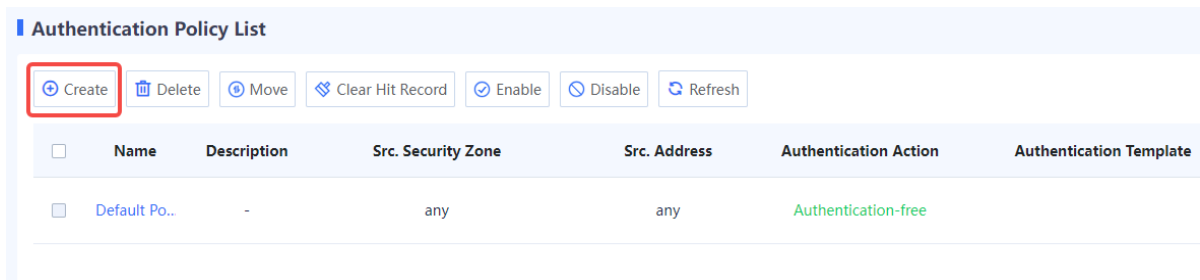
Application Scenario

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**.



- (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.	-

Item	Description	Remarks
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 Authentication is selected, authentication template needs to be specified.	[Example] Authentication
Authentication Template Name	Select the portal authentication template. For details, see 6.7.7 Authentication Settings .	

(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.

6.7.7 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.

Local Portal Authentication

① Authentication Port

Redirection upon Authentication No Redirection

Redirect to Previous Web Page

Redirect to Custom URL

App

i 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.

Local Portal
Custom Portal
Real-Name User Info Reception
Allowlist
Other Authentication Settings

Portal Authentication ON

Portal Authentication Template 1 Delete

Create

Basic Info

* Portal Authentication Template 1 Name

* Portal Server URL

URL Config Result

NAS Configuration Default ip Interface

Custom URL Parameters

User IP Field ON	Field Name <input type="text" value="Enter the field name."/>	Encryption Mode <input type="text" value="None"/>
MAC Field ON	Field Name <input type="text" value="Enter the field name."/>	Encryption Mode <input type="text" value="None"/>
	Address Format <input type="text" value="XX-XX-XX-XX-XX"/>	
NAS-IP Field ON	Field Name <input type="text" value="Enter the field name."/>	Encryption Mode <input type="text" value="None"/>
URL Field ON	Field Name <input type="text" value="Enter the field name."/>	Encryption Mode <input type="text" value="None"/>
Hostname Field ON	Field Name <input type="text" value="Enter the field name."/>	Encryption Mode <input type="text" value="None"/>

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 displayed.	[Example] http://www.123.com/
NAS Configuration	Select IP or Interface for the firewall to communicate with the server. If the firewall has multiple outbound interfaces, IP or Interface 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
Basic Info		
Portal Server IP	IPv4 address of the portal server.	[Example] 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
Advanced Settings		
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

Item	Description	Remarks
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.	
Escape	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. 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.	[Example] Enabled
Listening Port		
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 [6.7.2 2. Configuring Users](#).

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

6.7.8 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.

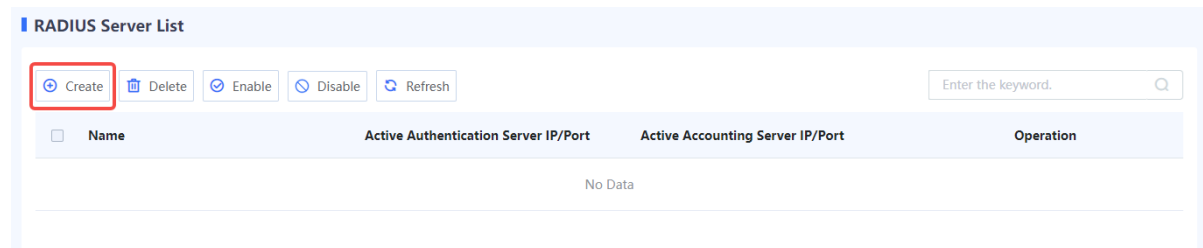
Precautions

- 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.

The screenshot shows the 'Add RADIUS Server' configuration page. The page is divided into two main sections: 'Basic Info' and 'Advanced Settings'.
Basic Info:
 - * Server Name: Enter the server name.
 - * Shared Password: Enter the password.
 - * Active Authentication Server IP: Enter an IP address. Authentication Port: 1812. Accounting Port: 1813. Tx Interface: Select an interface.
 - Standby Authentication Server IP: Enter an IP address. Authentication Port: Enter the port number. Accounting Port: Enter the port number. Tx Interface: Select an interface.
Advanced Settings:
 - Retransmission Times: 3
 - Unit: Byte
 - Response Timeout: 5
 - Enable Active Detection:
 - * Detection Username: Enter the username.
 At the bottom right, there is a 'Save' button.

Item	Description	Remarks
Basic Info		
Server Name	RADIUS server name.	[Example] server_1
Shared Password	Password for communication between the firewall and authentication server. The password must be the same as that set on the authentication server. Otherwise, authentication cannot be performed.	N/A
Active Authentication Server	Authentication server that performs authentication. <ul style="list-style-type: none"> ● IP: IP address of the authentication server. ● Authentication Port: Port on the authentication server that provides the authentication service. ● Accounting Port: Port on the authentication server that provides the accounting service. ● Tx Interface: Interface on the firewall for sending authentication packets. 	N/A
Standby Authentication Server	When the active authentication server fails or has no user information, the standby authentication server performs authentication. <ul style="list-style-type: none"> ● IP: IP address of the authentication server. ● Authentication Port: Port on the authentication server that provides the authentication service. ● Accounting Port: Port on the authentication server that provides the accounting service. ● Tx Interface: Interface on the firewall for sending authentication packets. 	N/A
Advanced Settings		
Retransmission Times	Maximum times of resending authentication request packets when the firewall does not receive a reply packet from the authentication server. If the retransmission times configured for both the active and standby servers are reached, the server is deemed as unreachable and the authentication fails.	[Example] 3
Unit	Unit of data flows that the firewall sends to the authentication server. The value must be the same as the traffic statistics unit on the server.	[Example] byte
Response Timeout	Timeout period in seconds for the firewall to receive a reply packet from the authentication server. When the timeout period expires, the firewall sends a request packet again.	[Example] 5
Enable Active Detection	After this function is enabled, the device sends a RADIUS packet every 10 minutes to detect whether the server can be connected.	-

Item	Description	Remarks
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**.

6.8 Certificate Management

6.8.1 Overview

Certificate is a digital signature issued by Certificate Authority (CA) for verifying the identity of network users. A certificate contains the owner's public key and other related identity information.

When a firewall functions as an SSL VPN gateway and a remote access user establishes an SSL connection with the SSL VPN gateway on the SSL VPN client, the SSL VPN 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.

When a firewall functions as an SSL proxy to decrypt and encrypt traffic, the intermediate firewall between the client and server needs to establish connections with both ends. In this interaction process, the firewall needs to establish a trusted relationship between the server and client using an SSL certificate.

SSL certificate types include:

- SSL proxy certificate: CA certificate used to issue an SSL proxy server certificate. This certificate needs to be configured when the client is protected by the SSL proxy function. It can be imported externally or generated manually on the firewall.
- Server certificate: Certificate on the server saved by the server administrator. When the server is protected by the SSL proxy function, the firewall needs to provide the server certificate to pass the identity verification of the client and decrypt packets. In this scenario, the server certificate needs to be imported on the firewall.

6.8.2 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.

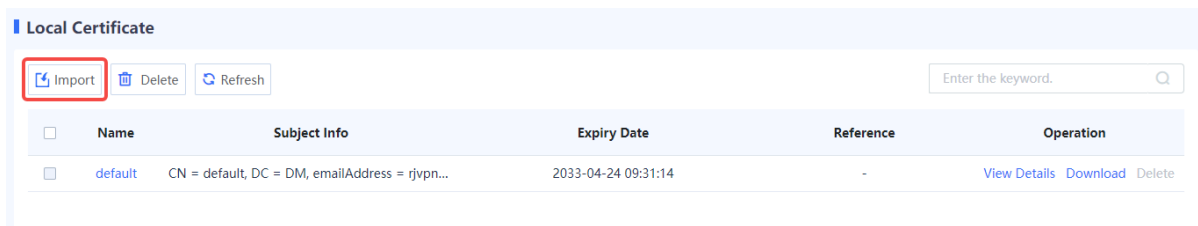
A firewall provides the default certificate **default**. You can import a new local certificate as required.

For details about the SSL VPN gateway, see [7.5 SSL VPN](#).

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.

6.8.3 SSL Certificate

1. Configuring an 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, which is set to a trusted certificate. You can also import a new certificate as needed.

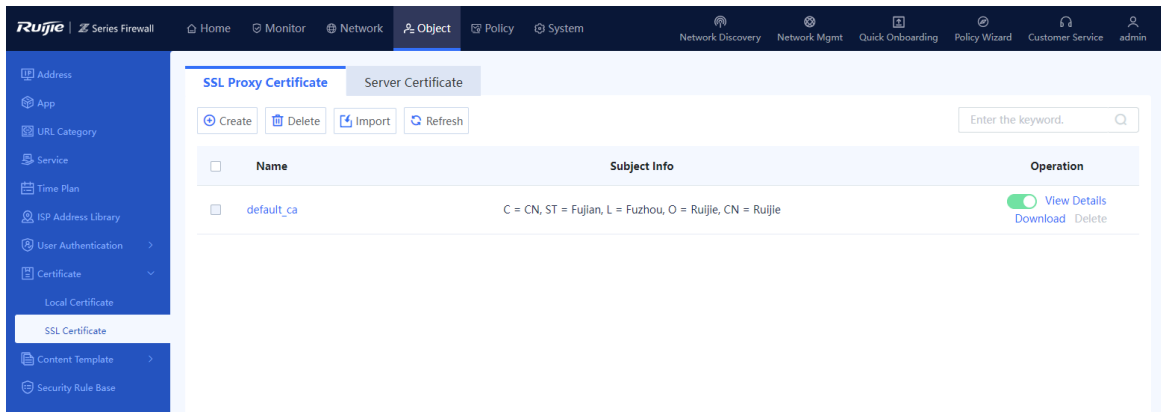
Precautions

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.



2. Importing an SSL Proxy Certificate

(1) Choose Object > Certificate > SSL Certificate > SSL Proxy Certificate.



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

Import SSL Proxy Certificate ✕

* Certificate ▼

Format

* Certificate


File

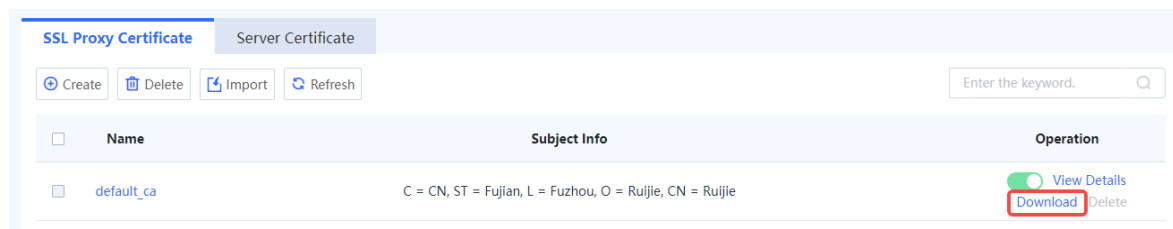
* Password

- (3) Select a certificate format. Click **Browse** and select an SSL proxy certificate file. Then, enter the password, and click **OK**.

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"> The certificate with the .p12 or .pem suffix already contains the key. You need to specify the password of the certificate when importing the certificate. The certificate with the .crt suffix does not contain a key and a separate key file is required. When you import the certificate, specify the key file and password of the key file. <p>[Example] P12</p>
Certificate File	Imported SSL proxy certificate file.	Click Browse to select a certificate file to be uploaded from the local device.
Key File	Separate key file attached with the certificate.	The certificate file with the .crt suffix does not contain a key. You need to upload the key file and specify the password for the key file when importing the certificate.
Password	Password of the key file.	<ul style="list-style-type: none"> Certificate with the .p12 or .pem suffix: You need to specify the password of the certificate when importing the certificate. Certificate with the .crt suffix: When you import the certificate, specify the key file and password of the key file.

Follow-up Procedure

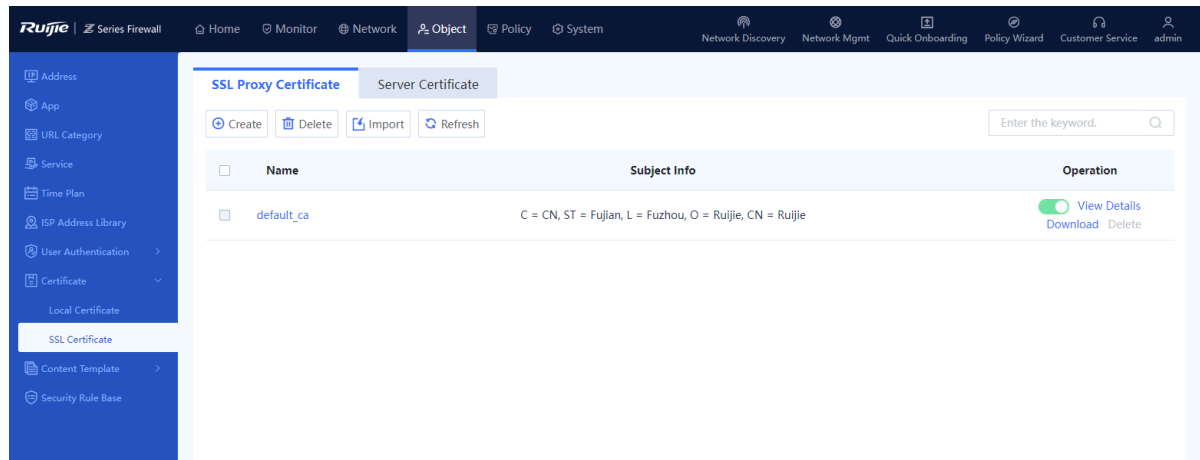
-  is used to configure whether to trust the SSL proxy certificate. When the icon is red, the certificate is not trusted; when the icon is green, the certificate is trusted. Click the icon to modify the credibility of the certificate. Only one trusted SSL proxy certificate can exist on the device.
- Download the SSL proxy certificate, and import it into the client to make the client trust it.



- 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.

3. Manually Creating an SSL Proxy Certificate

(1) Choose Object > Certificate > SSL Certificate > SSL Proxy Certificate.



(2) Click **Create**. The **Add SSL Proxy Certificate** page is displayed.

< Back

Add SSL Proxy Certificate

Basic Info

* Name

Location Info

* Public Name (CN)

Domain Name (DC)

Email Address

Country/Region (C)

State/Province (S)

Location (L)

Organization (O)


Department (OU)

(3) Configure parameters for the SSL proxy certificate. The certificate name and public name are mandatory, and the other parameters are optional.

Item	Description	Remarks
Name	Name of the SSL proxy certificate.	Chinese characters, spaces, and special characters such as `~!#%^&*+ \{};:'"/<>?` are not allowed. [Example] local_ca
Public Name (CN)	Common name of the SSL proxy certificate.	Spaces or special characters such as `~!#%^&*+ \{};:'"/<>?` are not allowed. [Example] Ruijie
Domain Name (DC)	Domain name of the certificate applicant.	[Example] www.abc.com.cn
Email Address	Email address of the certificate applicant.	[Example] test@ruijie.com.cn
Country/Region (C)	Country/Region code of the certificate applicant.	A standard two-character code should be used. [Example] CN
State/Province (S)	State or province of the certificate applicant.	Spaces or special characters such as `~!#%^&*+ \{};:'"/<>?` are not allowed. [Example] Fujian
Location (L)	Location of the certificate applicant.	Spaces or special characters such as `~!#%^&*+ \{};:'"/<>?` are not allowed. [Example] Fuzhou
Organization (O)	Organization of the certificate applicant.	Spaces or special characters such as `~!#%^&*+ \{};:'"/<>?` are not allowed. [Example] Ruijie
Department (OU)	Department of the certificate applicant.	Spaces or special characters such as `~!#%^&*+ \{};:'"/<>?` are not allowed. [Example] Department

- (4) Click **Save** to generate the SSL proxy certificate.

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 created 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.

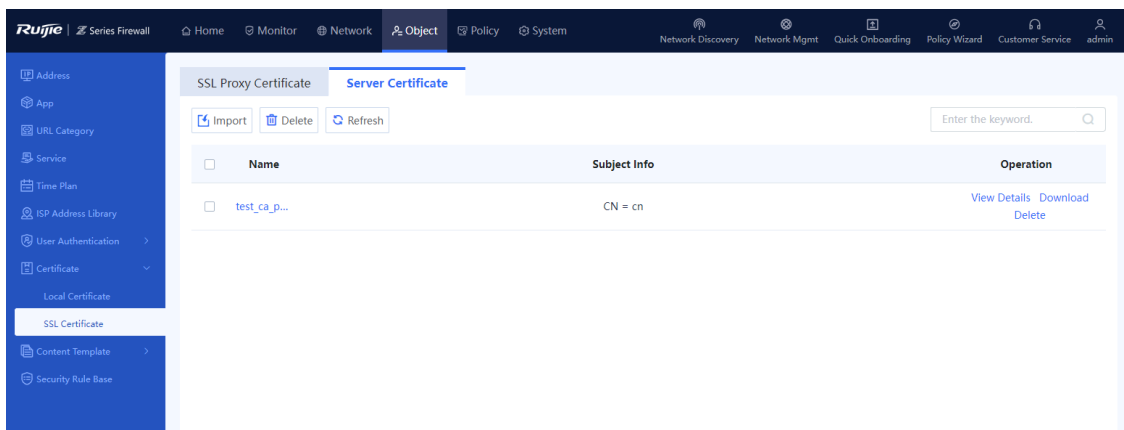
4. Importing a Server Certificate

Application Scenario

If HTTPS encrypted traffic needs to be decrypted 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**. The **Import Server Certificate** dialog box is displayed.

Import Server Certificate ⊗

* Certificate ▼
 Format

* Certificate
 File

* Password

(3) Select a certificate format. Click **Browse** and select a server certificate file. Then, enter the password, and click **OK**.

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"> ● The certificate with the .p12 or .pem suffix already contains the key. You need to specify the password of the certificate when importing the certificate. ● The certificate with the .crt suffix does not contain a key and a separate key file is required. When you import the certificate, specify the key file and password of the key file. [Example] P12
Certificate File	Imported server certificate file.	Click Browse to select a certificate file to be uploaded from the local device.
Key File	Separate key file attached with the certificate.	The certificate file with the .crt suffix does not contain a key. You need to upload the key file and specify the password for the key file when importing the certificate.
Password	Password of the key file.	<ul style="list-style-type: none"> ● Certificate with the .p12 or .pem suffix: You need to specify the password of the certificate when importing the certificate. ● Certificate with the .crt suffix: When you import the certificate, specify the key file and password of the key file.

Follow-up Procedure

- After certificate import, you can reference the certificate when the SSL proxy template type is **Protect Server**. For details, see [5.9.2 Configuring an SSL Proxy Template](#).

- To delete an imported server certificate, click **Delete**.
- You can enter the certificate name in the search box in the upper right corner of the page to search for a certificate.

6.9 Content Template

6.9.1 Virus Protection

1. Overview

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 HTTP, FTP, SMTP, and POP3.

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.

2. Adding a Custom Virus Protection Template

Application Scenario

The device provides a predefined template. You can also add custom templates for different virus protection scenarios.

Prerequisites

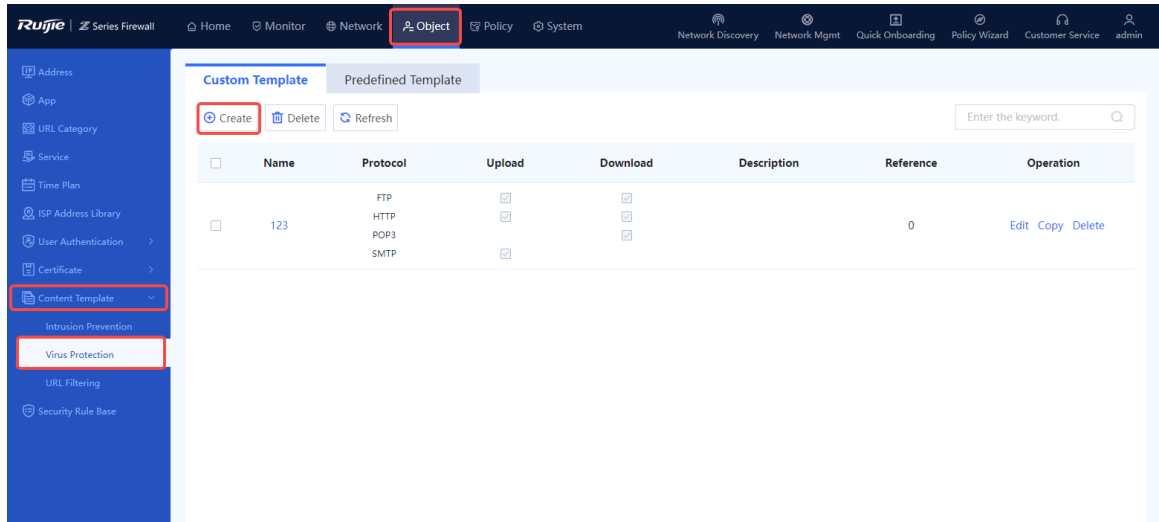
You have installed and activated the AV license. For details about license activation, see [8.3 Activating the License](#).

Note

- After the AV trial license expires, virus protection is unavailable, and virus protection libraries cannot be upgraded.
 - After the AV official license expires, virus protection is still available, but virus protection libraries cannot be upgraded.
-

Procedure

- (1) Choose **Object > Content Template > Virus Protection > Custom Template**.
- (2) In the operation area, click **Create**.



(3) Configure template parameters according to the following table.

< 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 checked="" type="checkbox"/>
SMTP	<input checked="" type="checkbox"/>	

Advanced Settings

Advanced Settings

① If a hash value is excluded, traffic matching the hash value is permitted. If a hash value is added to the blacklist, traffic matching the hash value is blocked.

Excluded Hash Settings

Enter an MD5 hash. Add

0 Added Clear

No Data

Hash Blocklist Settings

Enter an MD5 hash. Add

0 Added Clear


No Data

Excluded App

To-be-selected (48) <input type="checkbox"/> Select All <ul style="list-style-type: none"> <input type="checkbox"/> Email <input type="checkbox"/> NetworkStorage 	Selected (0) Clear
--	---

Save

Item	Description	Remarks
Basic Info		
Template Name	Name of the virus protection template.	Characters such as `~!#%^&*+V0:~/"<>? and spaces are not allowed. [Example] Template_1
Description	Description of the virus protection template.	Characters such as `~!#%^&*+~ ;:~/"<>? are not allowed. [Example] Only for detection of network-wide HTTP traffic
Scan Mode		

Item	Description	Remarks
Scan Mode	<p>The firewall supports two scan modes: quick scan and deep scan. Different modes use different virus protection signature libraries:</p> <ul style="list-style-type: none"> ● Quick scan: The virus detection rate is low but the performance overhead is small. ● Deep scan: The virus detection rate is high but the performance overhead is large. 	Quick Scan
Protocol	<p>Virus detection is performed on traffic of the specified protocols and directions.</p> <p>Traffic of the other protocols is directly permitted without being detected.</p>	<ul style="list-style-type: none"> ● FTP ● HTTP ● POP3 ● SMTP
<p>Advanced Settings</p> <p>Click  to expand advanced settings</p>		
Excluded Hash Settings	If an MD5 hash is added as an excluded hash, the firewall permits the packets that match the MD5 hash.	N/A
Custom Hash Settings	If an MD5 hash is added as a custom hash, the firewall blocks the packets that match the MD5 hash.	N/A
Excluded App	If an application is added as an excluded application, the firewall permits the packets of the application.	N/A

(4) After the configuration is completed, click **Save**.

Follow-up Procedure

Virus detection can be triggered only after a custom virus protection template is referenced by a security policy. For details about security policies, see [5.1 Security Policy](#).

3. Viewing the Predefined Virus Protection Template

Application Scenario

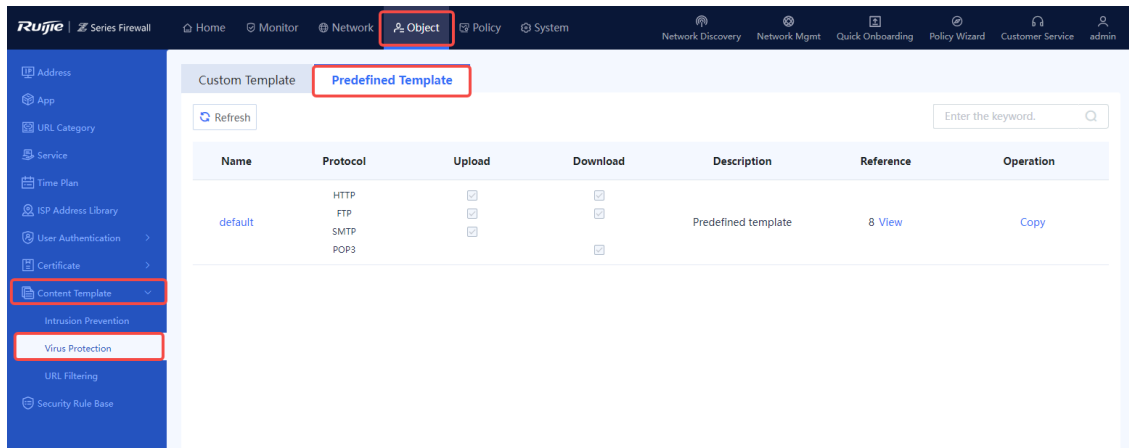
View the predefined content template to check the protocol traffic to be detected for subsequent configuration.

Prerequisites

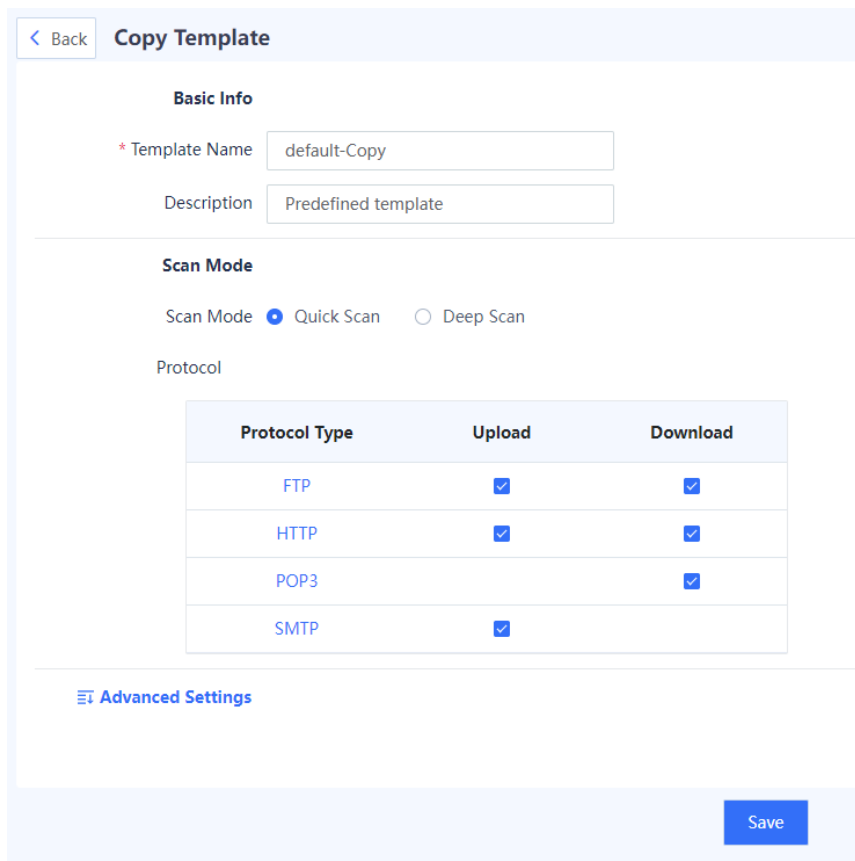
A predefined template cannot be deleted or edited, but you can copy it and then edit it as a custom template.

Procedure

(1) Choose **Object > Content Template > Virus Protection > Predefined Template**.



(2) Click the template name or click **Copy** in the **Operation** column to copy and then modify the parameters as required to quickly create a custom template.



(3) After the configuration is completed, click **Save**.

Follow-up Procedure

Virus detection can be triggered only after a custom virus protection template is referenced by a security policy. For details about security policies, see [5.1 Security Policy](#).

4. Upgrading a Virus Protection Signature Library

The virus protection signature library is continuously updated to guarantee high security. You can upgrade the virus protection signature library for detecting more types of viruses. For details about signature library upgrade, see [8.5 Signature Library Upgrade](#).

6.9.2 Intrusion Prevention

1. Overview

Intrusion Prevention System (IPS) is a security defense technology. IPS analyzes network traffic in real time to identify hidden malicious information, including buffer overflow attacks, trojans, and worms, and then generates alarms and block intrusions in real time.

When IPS is applied, intrusion packets can be automatically discarded and attack sources can be automatically blocked, thereby protecting enterprise information systems and network infrastructure against attacks.

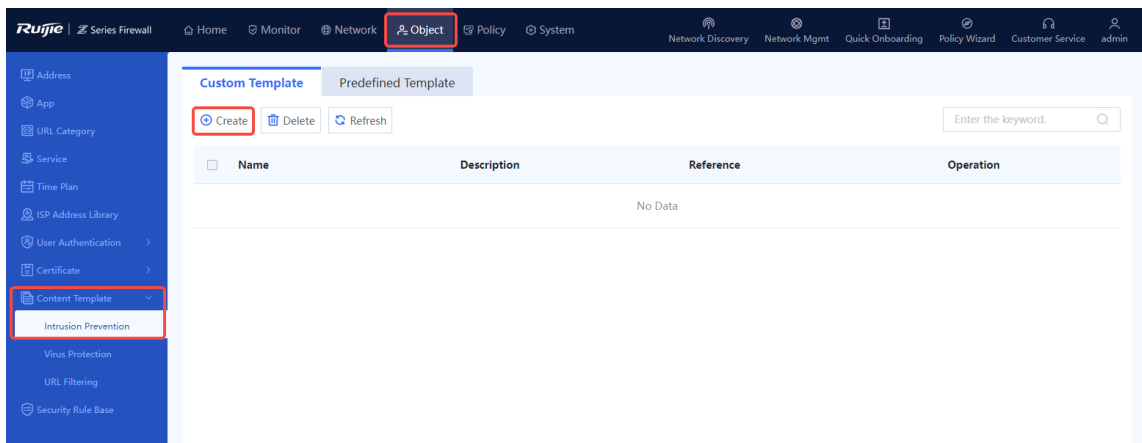
2. Creating a Custom IPS Content Template

Application Scenario

Create an IPS policy by using a custom template based on the protection scenario.

Procedure

- (1) Access the **Add Intrusion Prevention Template** page.
 - a Choose **Object > Content Template > Intrusion Prevention > Custom Template**.
 - b In the operation area, click **Create**.



- (2) Set parameters for the intrusion prevention template.

< Back **Add Intrusion Prevention Template**

Basic Info

* Template Name

Description

*** Rule Filter**

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

共 0 条

Advanced Settings

If a rule is excluded, the action of its signature has the highest priority.

Excluded Rule Settings

Select or enter data.

0 Added Action

- 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**. In the dialog box that is displayed, set parameters, and click **Confirm**.

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 (92) Select All

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


Selected (0) [Clear](#)


Item	Description	Remarks
Name	Name of the new rule filter.	<ul style="list-style-type: none"> ● Characters such as `~!#%^&*+V0::"/<>? and spaces are not allowed. ● You are advised to configure a name that can describe the filter function. <p>[Example] Filter1</p>
Object	Objects to be protected.	<p>[Example] All</p>

Item	Description	Remarks
Severity	Severity of the consequences of attacks. High, Medium, Low, and Tip can be selected. For example, if only High is selected, only the security rules with high severity can hit the filter.	[Example] High
Protocol	Protocols of traffic to be detected. Traffic of the other protocols does not hit the filter.	[Example] DNS
Threat Type	Types of threats to be detected. Traffic of the other threat types does not hit the filter.	[Example] Brute Force

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

Add

0 Added	Action	Clear

Save

(3) Click **Save**.

3. Viewing Predefined IPS Content Templates

Application Scenario

The device has multiple predefined IPS templates that meet different protection requirements in typical scenarios. You can refer to predefined IPS templates in security policies as required to detect and filter traffic.

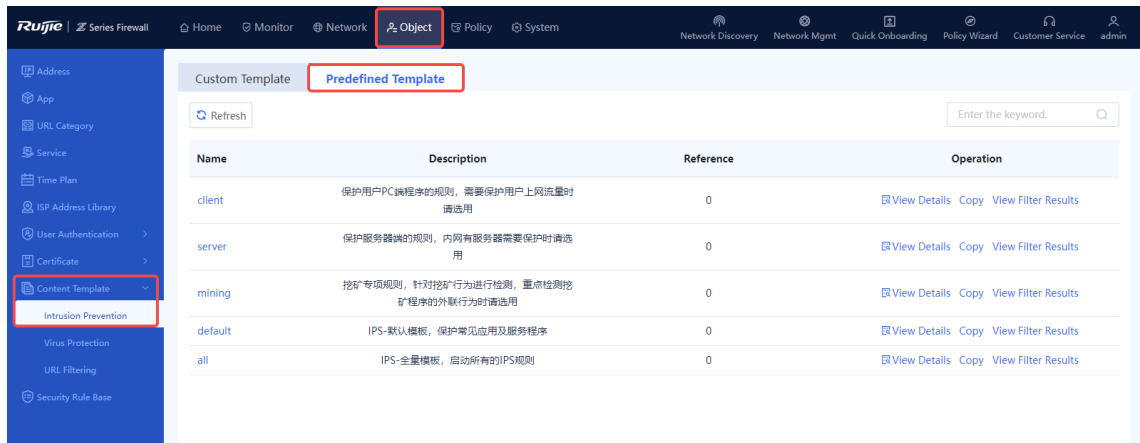
View the predefined content templates to check the features of intrusions to be detected for subsequent configuration.

Prerequisites

A predefined template cannot be deleted or edited, but you can copy it and then edit it as a custom template.

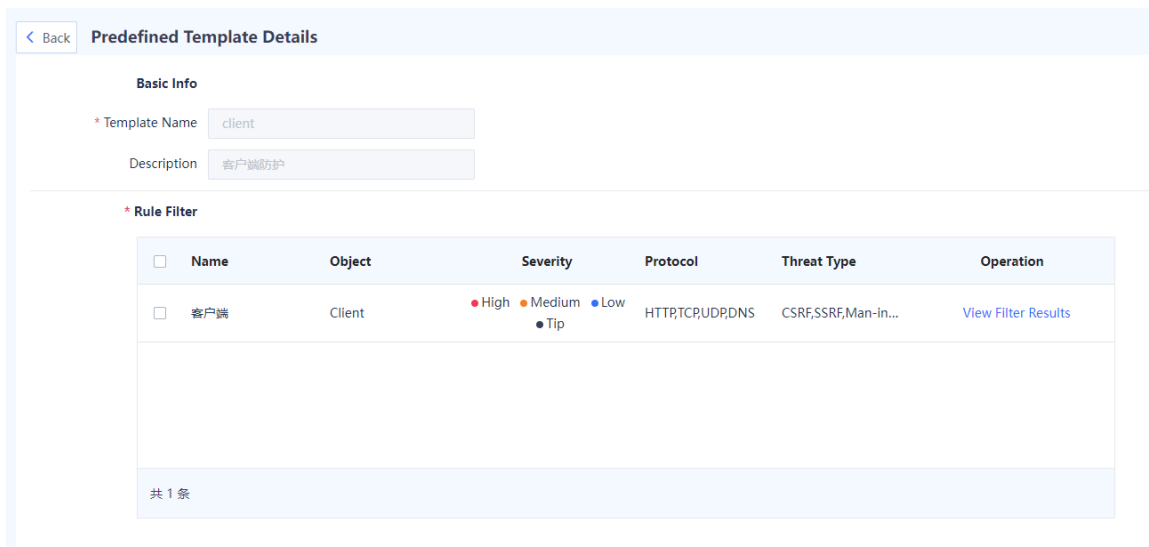
Procedure

(1) Choose **Object > Content Template > Intrusion Prevention > Predefined Template**.



(2) Select a predefined template and perform the following operations.

- Click **View Details** to view details about the predefined template, including the name, description, and rule filter information.



Item	Description
Basic Info	
Template Name	Name of the predefined template.
Description	Description of the predefined template.
Rule Filter	
Name	Name of the predefined template.

Item	Description
Object	<p>Attack object of network threats.</p> <ul style="list-style-type: none"> ● Server: The end being accessed. If this value is set, rules that detect attacks targeting server vulnerabilities are hit. For example, when the local end is accessed and attacked by a remote end, the local end is the server end. ● Client: The end that initiates an access request. If this value is set, rules that detect attacks targeting client (such as PC) vulnerabilities are hit. For example, when a user initiates a request to access a server with malicious codes and is attacked, the user is considered as a client.
Severity	<p>Severity of the consequences of attacks. High, Medium, Low, and Tip can be selected.</p> <p>For example, if only High is selected, only the security rules with high severity can hit the filter.</p>
Protocol	<p>Protocol types of network threats to be detected by the predefined content template.</p>
Threat Type	<p>Types of network threats.</p>

- Click **View Filter Results** to view the filter results.

Rule Filter Result



[+ Add Search Criteria](#)

ID	Threat Type	Threat Subtype	Name	Object	Severity	Protocol	Action
30146561	Memory Co...	Heap Overfl...	GNU Glibc ...	server	● High	TCP	Block
38141953	Other	Bypass Vuln...	Elasticsearc...	client	● Medium	TLS	Alarm
38141954	Other	Bypass Vuln...	Multi-Mozil...	client	● Medium	HTTP	Alarm
38141955	Other	Bypass Vuln...	Multi-Mozil...	client	● Medium	HTTP	Alarm
30146563	Memory Co...	Heap Overfl...	Microsoft I...	client	● High	HTTP	Block
30212097	Memory Co...	Integer Ove...	Android Sta...	client	● High	HTTP	Block
30212098	Memory Co...	Integer Ove...	Android Sta...	client	● High	HTTP	Block
30081025	Memory Co...	Stack Overfl...	OpenSSH S...	server	● Medium	TCP	Alarm
29753345	Memory Co...	Type Confu...	Microsoft B...	client	● Medium	HTTP	Alarm
30081027	Memory Co...	Stack Overfl...	GLIBC Buffe...	both	● High	UDP	Block

10 / Page Total:5992

Go to 1 < 1 2 3 4 5 6 ... 600 >

Item	Description
ID	ID of the rule.
Threat	Types of threats to be detected by the rule.
Threat Subtype	Subtypes of threats to be detected by rule.
Name	Name of the rule.
Object	Attack object of network threats to be detected by the rule.
Severity	Severity of the consequences of attacks. High, Medium, Low, and Tip can be selected.
Protocol	Protocol types of network threats to be detected by the rule.
Action	Action of the rule. <ul style="list-style-type: none"> ● Permit: When a packet hits this rule, it is allowed to pass through and no log is recorded. ● Alarm: When a packet hits this rule, it is allowed to pass through and a log is recorded. ● Block: When a packet hits this rule, it is discarded and a log is recorded.

 Note

Click **Add Search Criteria** to set search criteria for query. Only rules matching the search criteria are displayed.

- Click **Copy** to copy the content of the predefined template and edit it as required.

4. Upgrading an IPS Signature Library

The IPS signature library is continuously updated to guarantee high security. Upgrade the IPS signature library timely to ensure constant intrusion prevention. For details about signature library upgrade, see [8.5 Signature Library Upgrade](#).

6.9.3 URL Filtering

Application Scenario

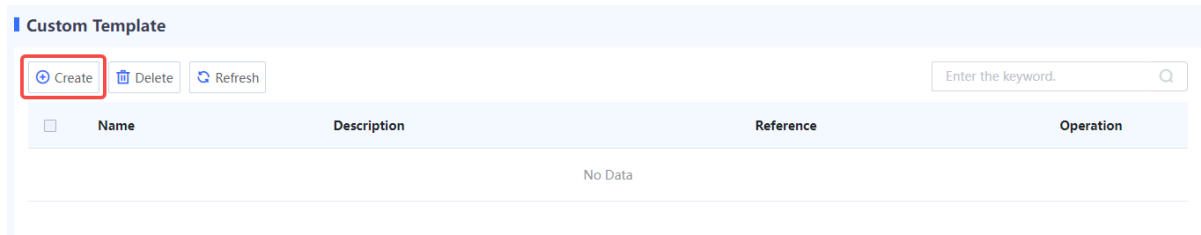
Configure a URL filtering template to block or report alarms for specific URL categories. Detection can be triggered only after a URL filtering template is referenced by a security policy. For details about security policies, see [5.1 Security Policy](#).

Precautions

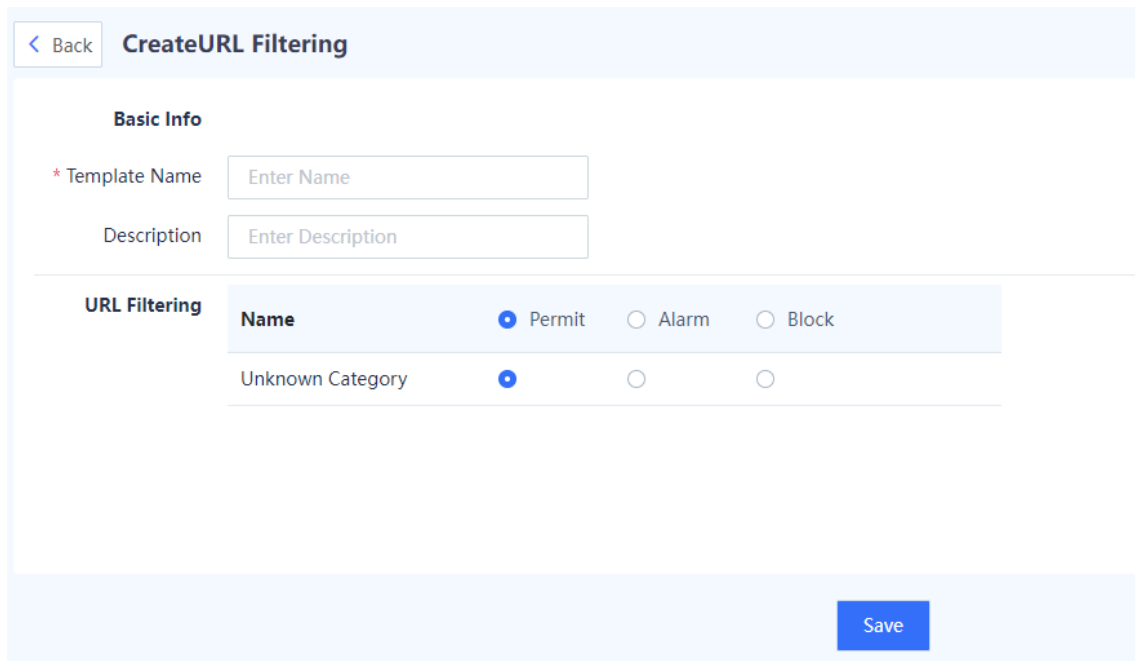
- To detect HTTPS-based URLs, you need to configure an SSL proxy policy. For details about SSL proxy, see [5.9 SSL Proxy](#).
- After you configure custom URL categories, URLs that are not in the custom categories are classified as uncategorized. When detecting traffic that accesses uncategorized URLs, the device processes the traffic according to the action set for uncategorized URLs.

Procedure

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



- (3) Enter URL filtering template information.



Item	Description	Remarks
Basic Info		
Template Name	Name of the URL filtering template.	[Example] Template_1
Description	Description of the URL filtering template.	N/A
Blocklist and Allowlist		

Item	Description	Remarks
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 Enter 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 www.test.com/#123 is configured, all the domain names that start with www.test.com/ will be matched.</p> <p>If a URL contains the characters http:// or https://, 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, [2001::1].</p>	<p>[Example]</p> <p>www.abc1.com</p>
URL Blocklist	<p>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.</p>	<p>[Example]</p> <p>www.abc2.com</p>
URL Filtering		
URL Filtering	<p>Set processing actions for different URL categories:</p> <ul style="list-style-type: none"> ● Permit: Permit traffic that accesses the URLs of the specific categories. ● Alarm: Permit traffic that accesses the URLs of the specific categories and generate an alarm log. ● Block: Block traffic that accesses the URLs of the specific categories and generate an alarm log. 	N/A

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

Follow-up Procedure

Refer to a URL filtering template in a security policy. For details about security policies, see [5.1 Security Policy](#).

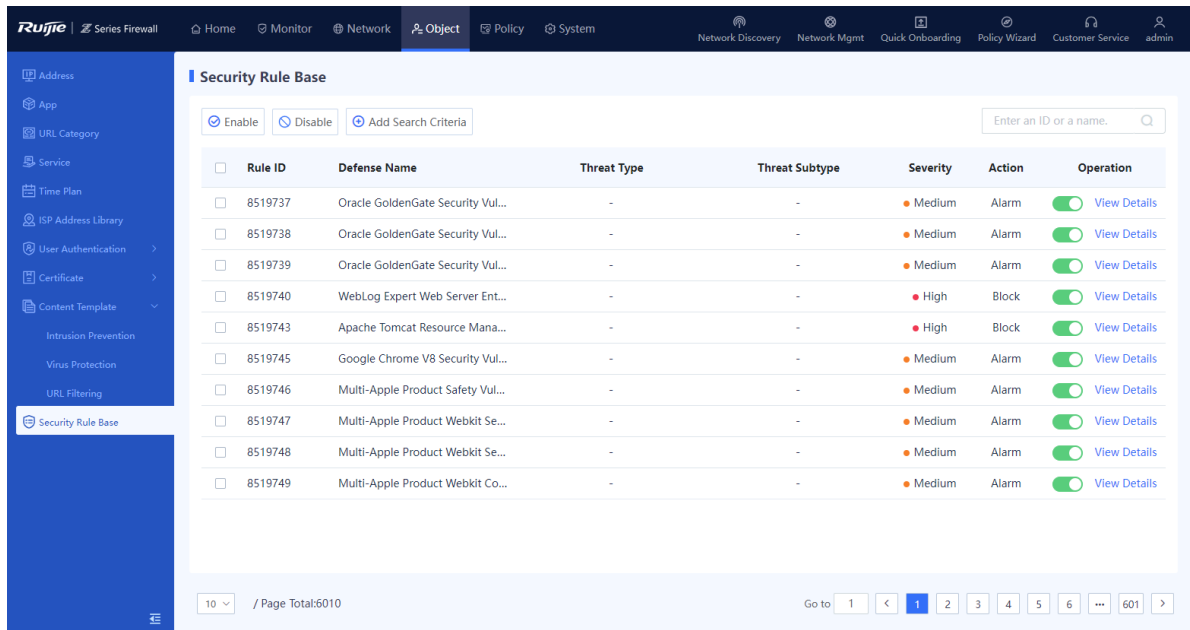
6.10 Security Rule Base

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 Network Configuration

7.1 Interface

7.1.1 Configuring a Physical Interface

Application Scenario

The physical interface on the device panel is used to connect to the network cable. The status of the network cable and the RJ45 connector affects the function of the physical interface.

Prerequisites


The network cable has been properly connected.

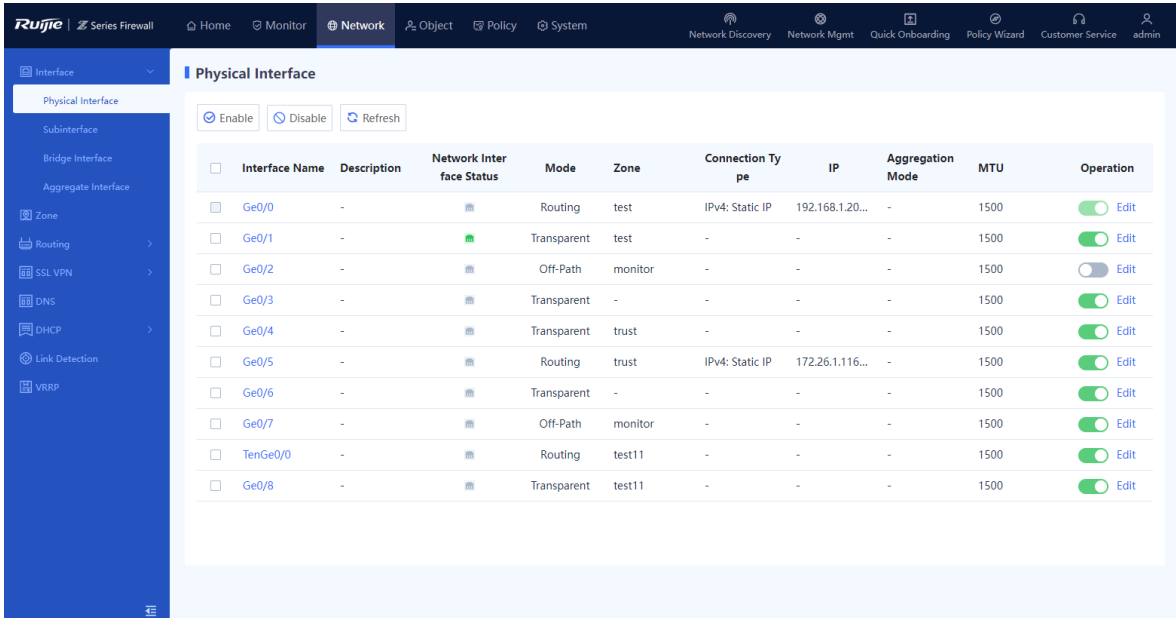
Procedure

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





















Caution

Disabling an interface or modifying the interface configuration may cause network interruption on all terminals connected to the interface. Exercise caution when performing this operation.

If the icon in the **Network Interface Status** column is green, the interface is connected. If it is gray, the interface is disconnected. By default, all interfaces are enabled. To disable an interface, toggle off . You cannot disable the management interface Ge0/0.



The screenshot shows the Ruijie Network Configuration interface. The left sidebar contains navigation options: Interface, Subinterface, Bridge Interface, Aggregate Interface, Zone, Routing, SSL VPN, DNS, DHCP, Link Detection, and VRRP. The main content area is titled "Physical Interface" and includes buttons for "Enable", "Disable", and "Refresh". Below these buttons is a table with the following columns: Interface Name, Description, Network Interface Status, Mode, Zone, Connection Type, IP, Aggregation Mode, MTU, and Operation. The table lists several interfaces, including Ge0/0 through Ge0/8 and TenGe0/0. The "Network Interface Status" column shows icons representing the connection status (green for connected, gray for disconnected). The "Operation" column contains "Edit" links for each interface.

Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mode	MTU	Operation
Ge0/0	-		Routing	test	IPv4: Static IP	192.168.1.20...	-	1500	 Edit
Ge0/1	-		Transparent	test	-	-	-	1500	 Edit
Ge0/2	-		Off-Path	monitor	-	-	-	1500	 Edit
Ge0/3	-		Transparent	-	-	-	-	1500	 Edit
Ge0/4	-		Transparent	trust	-	-	-	1500	 Edit
Ge0/5	-		Routing	trust	IPv4: Static IP	172.26.1.116...	-	1500	 Edit
Ge0/6	-		Transparent	-	-	-	-	1500	 Edit
Ge0/7	-		Off-Path	monitor	-	-	-	1500	 Edit
TenGe0/0	-		Routing	test11	-	-	-	1500	 Edit
Ge0/8	-		Transparent	test11	-	-	-	1500	 Edit

(2) In the **Operation** column of an interface, click **Edit**.

The **Edit Physical Interface** page is displayed.

< 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](#)

(3) Set parameters for the physical interface.

Item	Description	Remarks
Interface Name	Name of the physical interface.	The system displays the name automatically. [Example] Ge0/1
Description	Interface description, indicating the function of the interface.	[Example] Interface for connecting to the extranet
Connection Status	Enables or disables the interface.	[Example] Enable

Item	Description	Remarks
Mode	Interface access mode. <ul style="list-style-type: none"> ● Routing Mode: forwards traffic based on IP addresses. ● Transparent Mode: forwards traffic based on MAC addresses. ● Off-Path Mode: only receives mirrored traffic, but does not forward traffic. 	[Example] Transparent Mode
Bridge Interface	Bridge interface 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
IP Type	IP address type of the interface. Valid values: IPv4 and IPv6 .	[Example] IPv4
IPv4		
Connection Type	Network connection type of the interface. Valid values: Static Address , DHCP , and PPPoE .	[Example] Static Address
IP/Mask	IP address and mask of the interface.	This parameter is available when Connection Type is set to Static Address . [Example] 192.168.1.1/24
Next-Hop Address	Next-hop address of the forwarded data. Generally, it is the address of the next routing device.	This parameter is available when Connection Type is set to Static Address . [Example] 192.168.1.2/24
Account	Account that is required to obtain an IP address through PPPoE.	This parameter is available when Connection Type is set to PPPoE . [Example] Admin

Item	Description	Remarks
Password	Password that is required to obtain an IP address through PPPoE.	This parameter is available when Connection Type is set to PPPoE . [Example] Ruijie@123
IPv6		
IPv6	When you set IP Type to IPv6 , you must enable IPv6 . Otherwise, the IPv6 address does not take effect.	N/A
Connection Type	Network connection type of the interface. Valid values: Static Address , ND-RA , and DHCP .	[Example] Static Address
IP/Prefix Length	IPv6 address and address prefix of the interface.	This parameter is available when Connection Type is set to Static Address . [Example] 2001::1/64
Link-Local Address	Link-local address of the interface, which is automatically generated.	N/A
Advertise RA	Whether to allow the device to send RA packets on the interface. When this function is enabled, the device periodically sends RA packets, including prefix information options and information about certain flag bits, to advertise its presence.	[Example] Enable
Static Neighbor Entry	Specifies the static neighbor for the interface. To communicate with another node, a node must obtain the link layer address of the node. You can manually configure static neighbor entries to resolve IPv6 addresses of neighbor nodes to corresponding link layer addresses.	Each neighbor entry consists of a neighbor's IPv6 address and MAC address. Input one neighbor entry per line, and press Enter to separate multiple entries. Valid format: <i>IPv6 address MAC address</i> [Example] 1234::100 00:11:22:33:44:55
Advanced Address Settings		
Click  to expand Advanced IPv6 Settings .		

Item	Description	Remarks
Address Conflict Detection	Number of address conflict detections. When this function is enabled, the interface will send Neighbor Solicitation (NS) messages to determine if the configured IPv6 address is unique on the network. If an address conflict is detected, the interface rechecks the addresses based on the configured detection times and NS message sending interval.	Value range: 0–600. 0 indicates that conflict detection is disabled. [Example] 0
NS Sending Interval	Interval between two NS messages being sent. After the device sends an NS message, the NS message is resent if a response is not received within the specified time interval.	Value range: 1000–4294967295. Unit: millisecond. [Example] 1000
RA Sending Interval	Interval between two periodically sent RA messages.	Value range: 1–1800. Unit: second. [Example] 200
RA TTL	Lifetime of a router, that is, whether the device acts as the default router on the local link and the duration for acting as the default router.	Value range: 0–9000. Unit: second. [Example] 1800
RA Reachable Time	Period in which the device regards a neighbor reachable after detecting the neighbor reachability event.	Value range: 1–3600000. Unit: millisecond. [Example] 30000

Item	Description	Remarks
RA Prefix Info	<p>Prefix information that is advertised in the RA message.</p> <p>The following options can be configured:</p> <ul style="list-style-type: none"> ● Address: The prefix address that will be advertised. ● Effective Time: lifetime of the prefix considered valid by a host after the host receives the RA message, in seconds. ● Preferred Time: lifetime of the prefix considered as a preferred address for use by a host after the host receives the RA message, in seconds. ● Enable Router Address Flag: When enabled, this flag indicates that the prefix address field not only contains the prefix information, but also includes the address of the router that sends the RA message. ● Enable Direct Route Flag: When enabled, this flag indicates that the advertised prefix can be used to determine whether a destination is on the same link (on-link) and can be reached directly without using a router. When disabled, this flag indicates that the prefix will not be used for on-link determination. ● Enable Auto Config Flag: When enabled, this flag indicates that the advertised prefix can be used for stateless address configuration. When disabled, this flag indicates that the prefix will be used for stateful address configuration. 	Click Create to configure the RA prefix information.
Line Bandwidth	Limits interface bandwidth, including upload bandwidth and download bandwidth.	<p>Enter the bandwidth value and select a unit.</p> <ul style="list-style-type: none"> ● The unit can be kbps or Mbps. ● When kbps is selected, the value ranges from 1 to 100,000,000. ● When Mbps is selected, the value ranges from 1 to 100,000. <p>[Example]</p> <p>100 kbps</p>
Access Management	Whether the interface supports HTTPS, ping, and SSH.	<p>The configuration takes effect when local defense is enabled on the device.</p> <p>[Example]</p> <p>Select HTTPS.</p>
Advanced		

Item	Description	Remarks
ISP Address Library	ISP network connected to the interface. The interface generates ISP routes based on the associated ISP address set so that the traffic with the destination addresses on different ISP networks can be forwarded through the corresponding outbound interfaces.	This parameter is valid only if WAN Interface is configured for the interface. [Example] China Telecom
MTU	Maximum number of data bytes for individual packets transmitted 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 detect the network connectivity between the interface and the next hop in real time.	For details about link detection, see 7.9 Link Detection .

(4) Click **Save**.

7.1.2 Configuring a Subinterface

Application Scenario

A subinterface is a virtual interface created based on a physical interface and is identified by a VLAN. When a physical interface receives a packet, it checks the VLAN fields in the packet forwards the packet to the corresponding subinterface to process the packet. To create multiple IP addresses on a single physical interface for communication, you can create subinterfaces by assigning different VLAN IDs to subinterfaces. On the peer device, create corresponding subinterfaces to enable communication across network segments.

Procedure

- (1) Choose **Network > Interface > Subinterface**.
- (2) Click **Create**.

The **Add Subinterface** page is displayed.

< Back
Add Subinterface

Basic Info

* Physical Interface

Interface Type

* VLAN ID

Description

Zone [Add Security Zone](#)

Address

IP Type IPv4 IPv6

* Connection Type Static Address DHCP PPPoE

* IP/Mask

* Next-Hop Address

Default Route

Access Management

ⓘ When local defense is disabled, access management cannot be configured, and existing configurations become invalid. To configure access management, please go to [Security Defense - Local Defense](#) Enable Local Defense


Permit HTTPS PING SSH

Save

(3) Set parameters for the subinterface.

Item	Description	Remarks
Physical Interface	Physical interface on which you want to create a subinterface.	[Example] Ge0/1
Interface Type	Logical type of the subinterface.	The logical type of a subinterface must be the same as that of the physical interface.
VLAN ID	VLAN ID that the subinterface corresponds to.	[Example] 1
Description	Description of the subinterface.	[Example] Interface connected to the extranet.
Zone	Security zone to which the interface belongs.	[Example] trust
IP Type	IP address type of the subinterface. Valid values are IPv4 and IPv6 .	[Example] IPv4
IPv4		

Item	Description	Remarks
Connection Type	Method used for the physical interface to connect to the network. Valid values are Static Address , DHCP , and PPPoE .	[Example] Static Address
IP/Mask	Assigned IP address and mask for the physical interface.	This parameter is valid when Connection Type is set to Static Address . [Example] 192.168.1.1/24
Next-Hop Address	Next-hop address of the forwarded data. Generally, it is the address of the next routing device.	This parameter is valid when Connection Type is set to Static Address . [Example] 192.168.1.2/24
Account	Login account used when connecting over PPPoE.	This parameter is valid when Connection Type is set to PPPoE . [Example] Admin
Password	Password that is required to obtain an IP address through PPPoE.	This parameter is valid when Connection Type is set to PPPoE . [Example] Ruijie@123
IPv6		
IPv6	When you set IP Type to IPv6 , you must enable IPv6 . Otherwise, the IPv6 address does not take effect.	N/A
Connection Type	Network connection type of the interface. Valid values: Static Address , ND-RA , and DHCP .	[Example] Static Address
IP/Prefix Length	IPv6 address and mask of the interface.	This parameter is valid when Connection Type is set to Static Address . [Example] 2001::1/64
Link-Local Address	Link-local address of the interface, which is automatically generated.	N/A

Item	Description	Remarks
Advertise RA	Whether to allow the device to send Router Advertisement (RA) packets on the interface. When this function is enabled, the device periodically sends RA packets, including prefix information options and information about certain flag bits, to advertise its presence.	[Example] Enabled
Static Neighbor Entry	Specifies the static neighbor entry for the interface. To communicate with another node, a node must obtain the link layer address of the other node. You can manually configure static neighbor entries to resolve IPv6 addresses of neighbor nodes to corresponding link layer addresses.	Each neighbor table entry consists of a neighbor's IPv6 address and MAC address. Input one neighbor entry per line, and press Enter to separate multiple entries. Valid format: <i>IPv6 address MAC address</i> [Example] 1234::100 00:11:22:33:44:55
Advanced Address Settings		
Click  to expand Advanced IPv6 Settings .		
Address Conflict Detection	Number of address conflict detections. When this function is enabled, the interface will send NS messages to determine if the configured IPv6 address is unique on the network. If an address conflict is detected, the interface rechecks the address based on the configured detection times and NS message sending interval.	Value range: 0–600. 0 indicates that conflict detection is disabled. [Example] 0
NS Sending Interval	Interval between two NS messages being sent. After the device sends an NS message, the NS message is resent if a response is not received within the specified time interval.	Value range: 1000–4294967295. Unit: millisecond. [Example] 1000
RA Sending Interval	Interval between two periodically sent RA messages.	Value range: 1–1800. Unit: second. [Example] 200

Item	Description	Remarks
RA TTL	Lifetime of a router, that is, whether the device acts as the default router on the local link and the duration for acting as the default router.	Value range: 0–9000. Unit: second. [Example] 1800
RA Reachable Time	Period in which the device regards a neighbor reachable after detecting the neighbor reachability event.	Value range: 1–3600000. Unit: millisecond. [Example] 30000
RA Prefix Info	<p>Prefix information that is advertised in the RA message. The following options can be configured:</p> <ul style="list-style-type: none"> ● Address: The prefix address that will be advertised. ● Effective Time: lifetime of the prefix considered valid by a host after the host receives the RA message, in seconds. ● Preferred Time: lifetime of the prefix considered a preferred address for use by a host after the host receives the RA message, in seconds. ● Enable Router Address Flag: When enabled, this flag indicates that the prefix address field not only contains the prefix information, but also includes the address of the router that sends the RA message. ● Enable Direct Route Flag: When enabled, this flag indicates that the advertised prefix can be used to determine whether a destination is on the same network segment (on-link), and can be reached directly without using a router. When disabled, this flag indicates that the prefix will not be used for on-link determination. ● Enable Auto Config Flag: When enabled, this flag indicates that the advertised prefix can be used for stateless address configuration. When disabled, this flag indicates that the prefix will be used for stateful address configuration. 	Click Create to configure the RA prefix information.

Item	Description	Remarks
Access Management	Whether the interface supports HTTPS, ping, and SSH.	The configuration takes effect when local protection is enabled on the device. [Example] Select HTTPS.

(4) Click **Save**.

Follow-up Procedure

(1) On the **Subinterface** page, you can delete or modify subinterfaces.

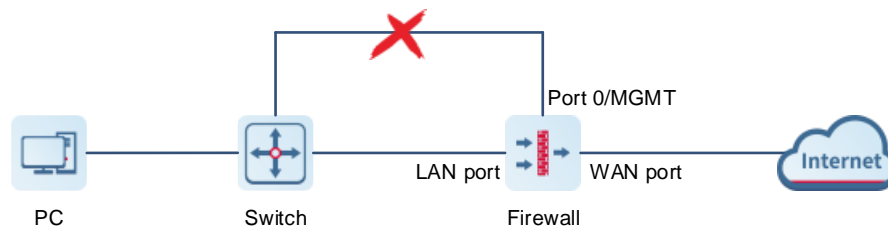
7.1.3 Configuring a Bridge Interface

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.

The screenshot shows the 'Bridge Interface' configuration page in the Ruijie Series Firewall management console. The left sidebar contains navigation options: Interface (Physical Interface, Subinterface, Bridge Interface, Aggregate Interface), Zone, Routing, SSL VPN, DNS, DHCP, Link Detection, and VRRP. The main content area is titled 'Bridge Interface' and includes a note: 'Member interfaces are interfaces configured with the transparent mode.' Below this are buttons for 'Create', 'Delete', 'Refresh', 'Enable', and 'Disable'. A table lists the bridge interface 'br0' with its member interfaces (Ge0/1, Ge0/3, Ge0/4, Ge0/6, Ge0/8), connection type (DHCP), IP address (172.20.36.3/24), and next-hop address (-). The 'Operation' column shows a toggle switch set to 'On' and links for 'Edit' and 'Delete'.

Bridge Interface	Member Interface	Connection Type	IP	Next-Hop Address	Operation
<input type="checkbox"/> br0	Ge0/1, Ge0/3, Ge0/4 Ge0/6, Ge0/8	DHCP	172.20.36.3/24	-	<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
Edit Bridge Interface

Basic Info

* Interface Name

Connection Status Enable Disable

Member Interface Ge0/1 Ge0/3 Ge0/4 Ge0/6 Ge0/8

Address

Connection Type Static Address DHCP

Src. MAC Consistency

Check

Src. MAC Consistency

Check

Access Management

ⓘ When local defense is disabled, access management cannot be configured, and existing configurations become invalid. To configure access management, please go to [Security Defense - Local Defense](#) Enable Local Defense

Permit HTTPS PING SSH

Save

Item	Description	Remarks
Interface Name	Name of a bridge interface.	<ul style="list-style-type: none"> ● Characters such as `~!#%^&*+ \{};:"'<>?` and spaces are not allowed. ● The name is specified when you create a bridge interface and cannot be modified in later steps. <p>[Example]</p> <p>br1</p>
Connection Status	Whether to enable the bridge interface.	<p>[Example]</p> <p>Enable</p>
Member Interface	Member interface in the bridge interface. Members of the bridge interface are interfaces set to transparent mode. One bridge interface can contain multiple transparent interfaces, but each transparent interface can belong to only one bridge interface.	<p>To add a member to the bridge interface, set Bridge Interface to the current bridge interface when you configure the corresponding member interface (such as a physical interface or aggregate interface).</p> <p>[Example]</p> <p>Ge0/2</p>
Address		

Item	Description	Remarks
Connection Type	<p>Connection type for the bridge interface, including:</p> <ul style="list-style-type: none"> ● 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. You need to configure IP/Mask and Next-Hop Address as well. ● DHCP: Applicable when the network administrator is not professional. The bridge interface automatically obtains an IP address from the upper-layer DHCP server for Internet access. 	<p>[Example] Static Address</p>
IP/Mask	IP address and mask of the interface.	<p>You need to set this parameter when Connection Type is set to Static Address.</p> <p>[Example] 192.168.20.1/24</p>
Next-Hop Address	Next router address to reach the router with the destination address.	<p>You need to set this parameter when Connection Type is set to Static Address.</p> <p>[Example] 192.168.20.2/24</p>
Default Route	Whether to enable the default route.	<p>[Example] Enabled</p>
Src. MAC Consistency Check	Whether to enable source MAC address consistency check. If you select Enable, the firewall checks the source MAC address of the packet with the source MAC address in the session. If they are different, the firewall does not check the session status of the packet but transparently forwards the packet over the bridge network directly.	<p>[Example] Enabled</p>
Access Management	Whether the bridge interface supports HTTPS, ping, and SSH.	<p>The configuration takes effect when local defense is enabled on the device.</p> <p>[Example] Select HTTPS.</p>

7.1.4 Configuring an Aggregate Interface

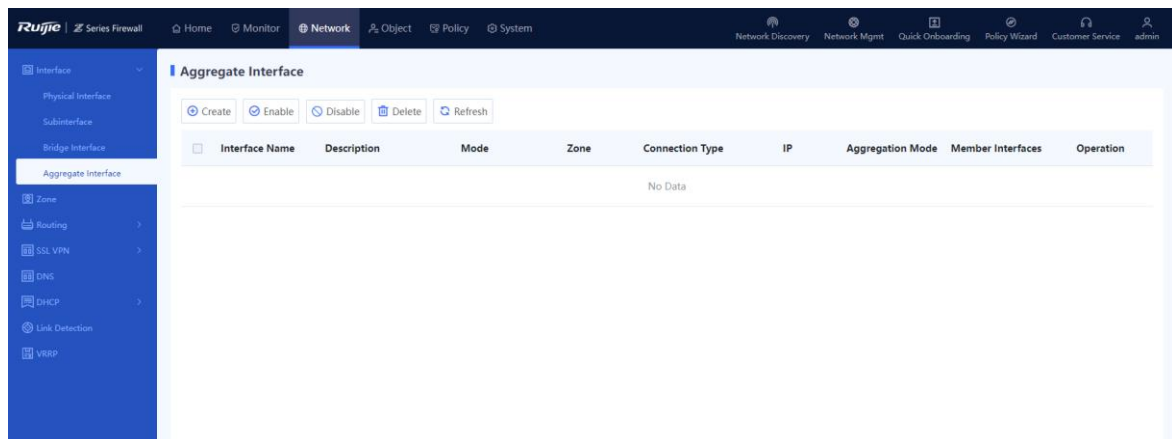
Application Scenario

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, the excess traffic is discarded. An aggregate interface can solve the problem of insufficient bandwidth: 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 **Add Aggregate Interface** page is displayed.

< 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

[Security Defense - Local Defense](#) Enable Local Defense

Permit HTTPS PING SSH

Advanced Settings

Aggregation Mode

ISP Address Library

MTU

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 numbers. [Example] Ag1

Item	Description	Remarks
Connection Status	Enables or disables the interface.	[Example] Enable
Mode	Interface access mode. <ul style="list-style-type: none"> ● Routing Mode: forwards traffic based on IP addresses. ● Transparent Mode: forwards traffic based on MAC addresses. ● Off-Path Mode: only receives mirrored traffic, but does not forward traffic. 	[Example] Transparent 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.
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. Valid values: Static Address and DHCP .	[Example] Static Address
IP/Mask	IPv4 address and mask of the interface.	This parameter is available when Connection Type is set to Static Address . [Example] 192.168.1.1/24

Item	Description	Remarks
Next-Hop Address	Next address of the forwarded data. Generally, it is the address of the next routing device.	This parameter is available when Connection Type is set to Static Address . [Example] 192.168.1.2/24
Default Route	Whether to generate the default route.	[Example] Enabled
Line Bandwidth	Limited interface bandwidth, including upload bandwidth and download 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. [Example] 100 kbps
Access Management	Whether the interface supports HTTPS, ping, and SSH.	The configuration takes effect when local protection is enabled on the device. [Example] Select HTTPS .
Advanced Settings		
Aggregation Mode	For the manually configured aggregate interface, the aggregation mode is displayed as Static Aggregation .	Only the Static Aggregation is supported currently.
ISP Address Library	ISP network connected to the interface. The interface generates ISP routes based on the associated ISP address set, and the traffic with the destination addresses in different ISP networks is forwarded through the corresponding outbound interfaces.	This configuration takes effect only when the interface is configured as a WAN interface. [Example] China Telecom


Item	Description	Remarks
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 detect the network connectivity between the interface and the next hop in real time.	For details about link detection, see 7.9 Link Detection .

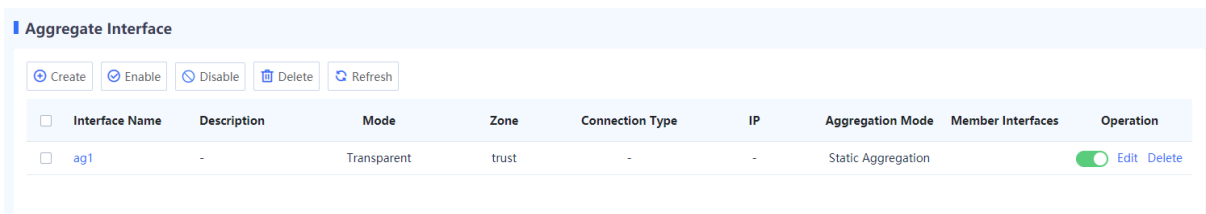
 Caution

- A management interface 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** page, you can modify or delete 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**.



Aggregate Interface

Interface Name	Description	Mode	Zone	Connection Type	IP	Aggregation Mode	Member Interfaces	Operation
<input type="checkbox"/> ag1	-	Transparent	trust	-	-	Static Aggregation		<input checked="" type="checkbox"/> Edit Delete

7.1.5 Configuring a Tunnel interface

Application Scenario

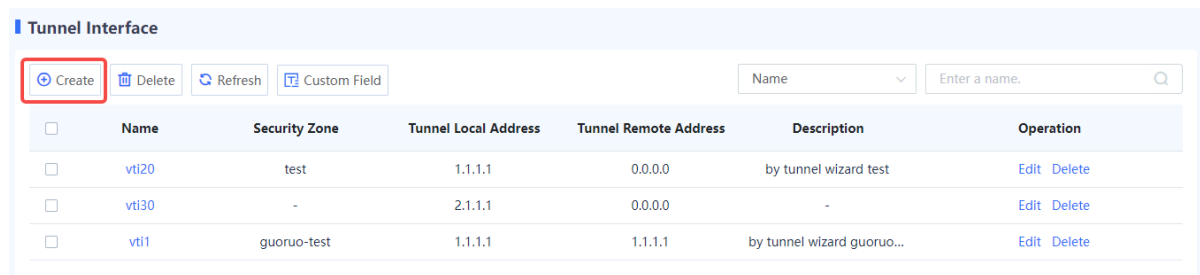
Tunneling is a technology that encapsulates packets of a protocol into packets of a different protocol and then transmits these packets over the network. This technology enables transmission of specific protocol packets on

an incompatible network and provides a secure path for data transmission on an insecure network. A tunnel interface is a Layer 3 virtual interface used to implement tunneling, and each tunnel interface represents a transmission link. The devices at both ends of a tunnel create tunnel interfaces to encapsulate, transmit, and decapsulate data packets.

In an IPsec VPN scenario, you can establish an IPsec tunnel by creating a tunnel interface and applying it to an IPsec tunnel policy. This tunnel enables encrypted transmission of data flows that are routed to the tunnel interface and match the defined interesting traffic.

Procedure

- (1) Choose **Network > Interface > Tunnel Interface**.



- (2) Click **Create**.

The **Create Tunnel Interface Details** page is displayed.

Create Tunnel Interface Details

* Interface Name

Security Zone

* Tunnel Local Address

Tunnel Remote Address IP Dynamic

Description

- (3) Set parameters for the tunnel interface.

Item	Description	Remarks
Interface Name	Name of the tunnel interface.	The interface name must consist of uppercase and lowercase letters and digits and contain at least one letter. [Example] vti1
Security Zone	Security zone to which the interface belongs.	[Example] trust
Tunnel Local Address	Local address of the tunnel, which is the source IP address of encapsulated tunnel packets.	Do not configure the same local and remote addresses for two tunnel interfaces. [Example] 10.1.1.10
Tunnel Remote Address	Remote address of the tunnel, which is the destination IP address of encapsulated tunnel packets.	<ul style="list-style-type: none"> Optional. In some scenarios, the local end of a tunnel can dynamically learn the tunnel remote address from packets sent from the peer end. In this case, this parameter can be set to Dynamic. Do not configure the same local and remote addresses for two tunnel interfaces. [Example] 10.1.1.20
Description	Interface description, showing the purpose of the interface.	Characters such as `~!#%^&*+ \{};:~"/<>?` are not allowed. [Example] IPsec tunnel

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

Follow-up Procedure

- Enter a tunnel interface name in the search box in the upper right corner to query tunnel interface information.
- Click **Custom Field** to set the fields to be displayed on the page.
- In the tunnel interface list, click **Edit** to modify interface configurations, and click **Delete** to delete a tunnel interface.
- Click **Refresh** to obtain the latest tunnel interface information.
- To delete multiple tunnel interfaces in a batch, select the interface entries and click **Delete**.

7.2 Security Zone

7.2.1 Overview

A security zone is a security term introduced for devices. A security zone is a collection of networks connected by interfaces where users have the same security attributes.

Security level requirements vary based on network devices due to various network deployments and service needs. With security zones, network administrators can divide network devices with the same security level requirements into one security zone. Since network devices within the same security zone are considered equally secure, firewalls assume that data flows inside the same security zone do not have security risks and do not require additional security policies. When data flows occur between different security zones, the security check of devices is triggered and corresponding security policies are implemented.

Three default security zones named trust, untrust, and DMZ are provided in the system. If a device has an interface in off-path mode, the system automatically creates a monitor security zone.

Security Zone Name	Description
trust	A security zone with a higher security level, which is typically used to define the area of end users on an intranet.
untrust	A security zone with a lower security level, which is typically used to define non-secure networks such as the Internet.
DMZ	A security zone typically used to define an area where intranet servers are located. The devices in this area are deployed on an intranet but need to be accessed by external hosts, which leads to significant security risks. In addition, intranet servers are usually not allowed to initiate external connections. Therefore, they need to be deployed in DMZ, with a priority lower than trust but higher than untrust.
monitor	A security zone used to define the area where traffic monitoring is required. A monitor security zone contains all the interfaces deployed in off-path mode.

Data flows between security zones are in inbound or outbound direction.

- Inbound direction: Data is transferred from a low-priority security zone to a high-priority security zone.
- Outbound direction: Data is transferred from a high-priority security zone to a low-priority security zone.

In general, packets are transmitted in both the inbound and outbound directions between security zones. The direction of a traffic flow is determined by the first packet sent out when the communication is initiated.

For example, if a terminal in the trust security zone sends the first packet to a web server in the untrust security zone to establish an HTTP connection, this packet is considered as an outbound packet because the untrust security zone has a lower priority than the trust security zone. The firewall then decides whether to further process the data flow based on the configuration in the outbound direction.

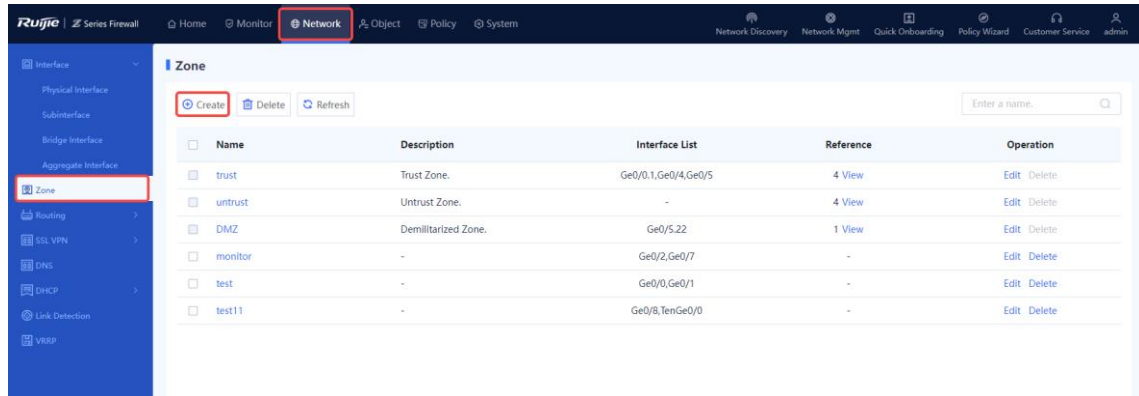
7.2.2 Creating a Security Zone

Application Scenario

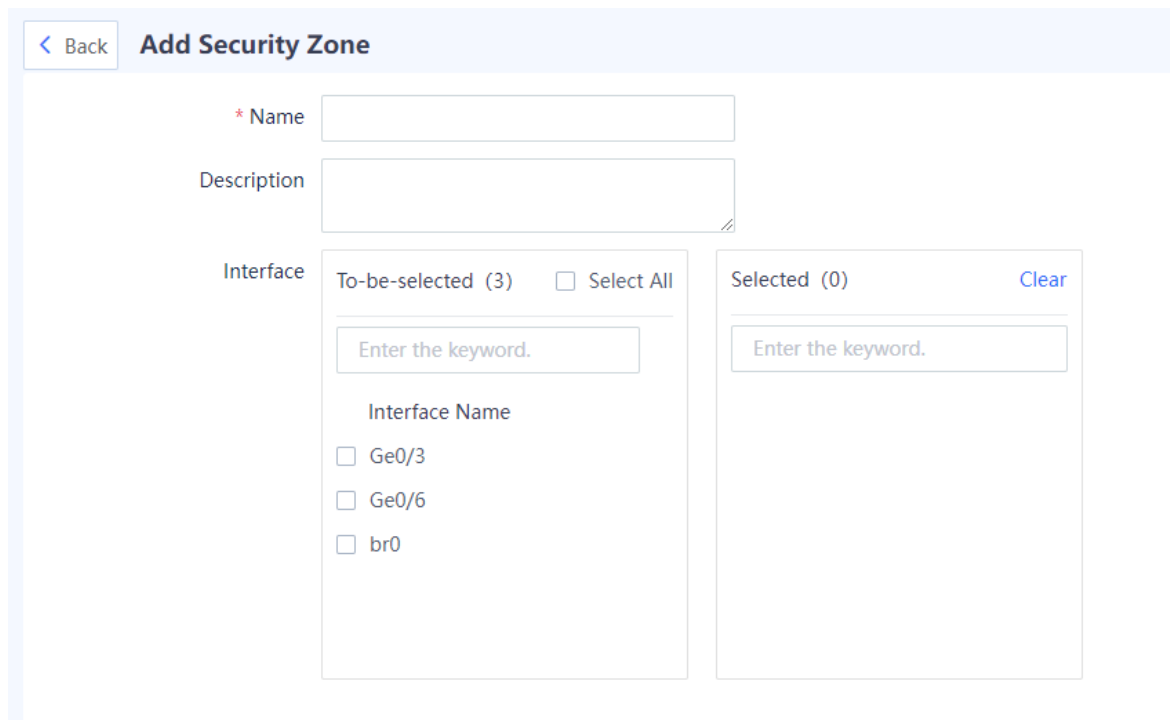
You can create security zones and add interfaces to the security zones as required. You can also create policies to manage mutual access traffic between different security zones.

Procedure

- (1) Access the **Add Security Zone** page.
 - a Choose **Network > Zone**.
 - b In the operation area, click **Create**.



- (2) Configure parameters for the security zone.



Item	Description	Remarks
Name	Security zone name.	Characters such as `~!#%^&*+V0::"/<>?` and spaces are not allowed. [Example] Zone1
Description	Description of the security zone, which is used to distinguish different security zones.	Characters such as `~!#%^&*+V0::"/<>?` are not allowed. [Example] New zone
Interface	Interfaces to be added to the security zone.	<ul style="list-style-type: none"> ● Select one or more interfaces in the To-be-selected area. The selected interfaces are automatically added to the Selected area. ● An interface cannot be added to different security zones. ● If an interface is not added to a security zone, packets cannot be forwarded through this interface. [Example] Ge0/1

(3) Click **Save**.

Follow-up Procedure

- You can only delete the address with no reference.
- The default security zones (trust, untrust, and DMZ) and security zones whose reference is not 0 cannot be deleted.
- To delete multiple security zones in a batch, select the security zones that you want to delete and click **Delete**.

7.3 Route Management

7.3.1 Overview

Routing is a crucial element of data communication networks. Routing information is the transmission paths of packets, and routing is the process of forwarding packets.

Z-S series firewalls support the following routing modes:

- **Static routing:** With static routing, packets are forwarded from one interface to another based on the destination address.
- **Intelligent routing:** Intelligent routing, also called policy-based routing (PBR) and application-based routing, is used for routing and forwarding packets based on user-specified policies. For example, you can specify outbound interfaces for forwarding packets that meet specific conditions such as the source security zone, source address, destination address, service, or application.
- **Address library-based routing:** After the ISP network is set for each line, the data flow is automatically routed

based on the ISP's address library. This method ensures that traffic of different ISPs is transmitted through their own networks, enabling faster network access and avoiding inter-ISP access.

In a scenario where multiple routing modes are available, the priorities in a descending order are as follows: intelligent routing, static routing, address -library-based routing. On a network with a simple topology, you can configure only static routes to enable communication. Static routes are easy to configure and suitable for small networks with simple and stable topologies. However, static routes cannot automatically adapt to changes in the network topology and require manual intervention.

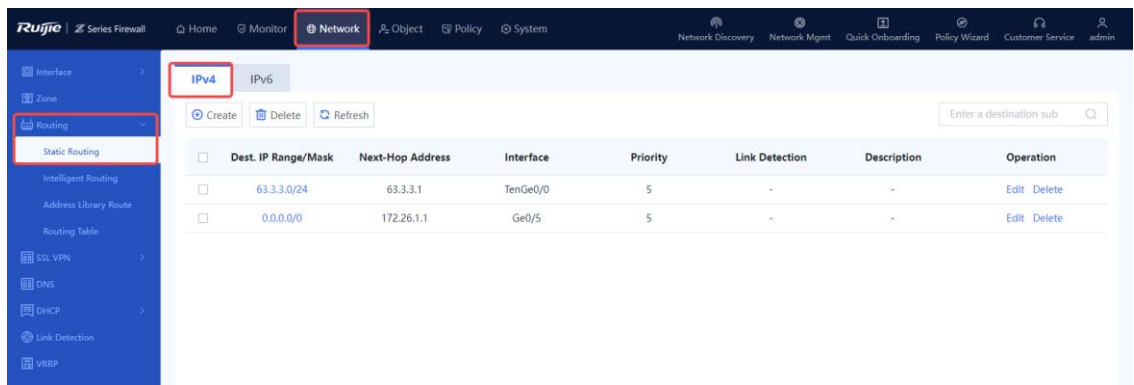
7.3.2 Creating a Static Route

Application Scenario

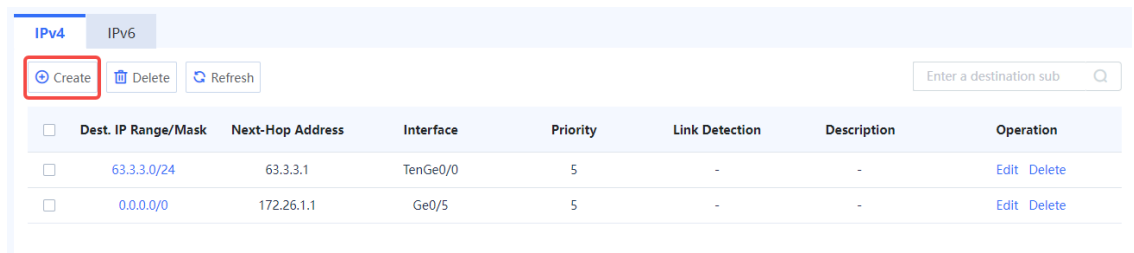
You can configure the IP address, next-hop address, and interface to create a static route for network interconnection and packet forwarding.

Procedure

- (1) Access the **Create Static Routing** page.
 - a Choose **Network > Routing > Static Routing**.
 - b Click the **IPv4** or **IPv6** tab to create an IPv4 or IPv6 static route as needed.



- c Click **Create**.



- (2) Set parameters of the static route.

< Back

Create Static Routing

IP Type IPv4

* Dest. IP Range/Mask

Next-Hop Address

Interface Select v

* i Priority

Link Detection Link Detection v

Description

Item	Description	Remarks
IP Type	IP type of the static route.	N/A
Dest. IP Range/Mask	Destination network segment of the packets that the static route matches with.	[Example] 192.168.10.0/24
Next-Hop Address	Next address of the forwarded data. Generally, it is the address of the next routing device.	[Example] 192.168.20.1
Interface	Outbound interface for packet forwarding.	When configuring a static route, you can specify both the next-hop address and the outbound interface, or you can specify only the outbound interface or the next-hop address as needed. [Example] Ge0/1

Item	Description	Remarks
Priority	Priority of the route. In cases where the destination network segments are the same, the static route with a higher priority is matched first. The default value is 5.	<ul style="list-style-type: none"> The value ranges from 1 to 255. A smaller value indicates a higher priority. If multiple static routes have the same priority value, the one with a larger subnet mask has a higher priority. <p>[Example] 15</p>
Link Detection	Link detection policy associated with the outbound interface. This configuration can detect the network connectivity between the outbound interface and the next hop in real time. When the network between the outbound interface and the next hop is unreachable, this static route becomes invalid.	For details about link detection, see 7.9 Link Detection .
Description	Description of the static route.	Characters such as `~!#%^&*+ :;"/<>?` are not allowed.

(3) Click **Save**.

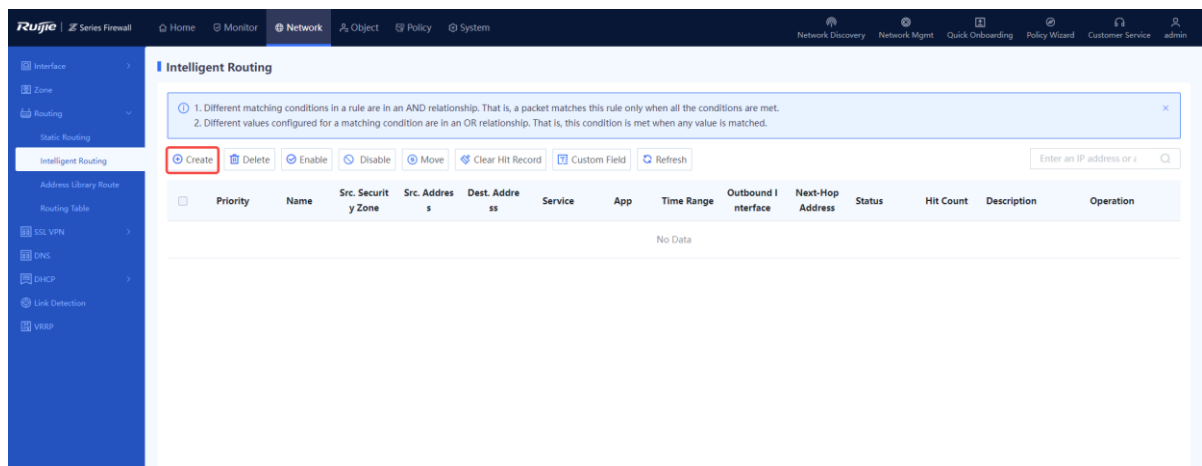
7.3.3 Creating an Intelligent Routing Policy

Application Scenario

By using intelligent routing, you can redirect the packets that meet the matching conditions to the specified outbound interface and next hop.

Procedure

- Choose **Network > Routing > Intelligent Routing**. The **Intelligent Routing** page is displayed.
- Click **Create** to access the Create Intelligent Routing page.



(3) Set parameters for the intelligent routing policy.

< Back

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

Item	Description	Remarks
Basic Info		
Name	Name of the intelligent routing policy.	Characters such as `~!#%^&*+V0:/"<>? and spaces are not allowed. [Example] Policy_1
Enabled State	Whether to enable the intelligent routing policy.	[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 in matching.	N/A
Description	Route description.	Characters such as `~!#%^&*+{ };:"/<>? are not allowed.

Item	Description	Remarks
Matching Conditions		
Src. Security Zone	Forwards the packets from this source security zone based on the policy.	<ul style="list-style-type: none"> Click the drop-down list, and select a source security zone in the To-be-selected area. The selected zone is automatically added to the Selected area. Click Add Security Zone to add a custom security zone. [Example] trust
Src. Address	Forwards the packets from this source address or address group based on the policy.	<p>Click the drop-down list, and select a source address in the To-be-selected area. The selected address is automatically added to the Selected area.</p> <p>[Example] Any</p>
Dest. Address	Forwards the packets to this destination address or address group based on the policy.	<p>Click the drop-down list, and select a destination address in the To-be-selected area. The selected address is automatically added to the Selected area.</p> <p>[Example] Any</p>
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 policy is effective.	[Example] Any
Action Settings		
Action Option	Whether to forward the matched packets based on the policy. If you click Forwarding , you also need to configure Outbound Interface and Next-Hop Address .	[Example] Forwarding

Item	Description	Remarks
Link Detection	Link detection policy associated with the outbound interface. This configuration can detect the network connectivity between the outbound interface and the next hop in real time. When the network between the outbound interface and the next hop is unreachable, this intelligent route becomes invalid.	For details about link detection, see 7.9 Link Detection .

(4) Click **Save**.

7.3.4 Viewing Address Library Routes

Application Scenario

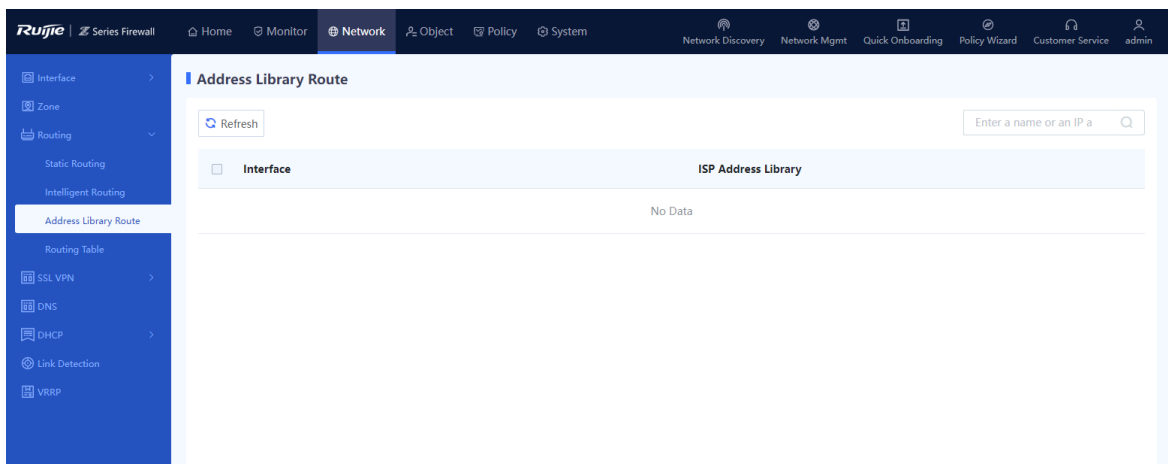
The routes in address library are automatically generated after the ISP network to which the interface is connected is configured, and cannot be manually created. After an interface is associated with an ISP address set, routes are automatically generated in the address library, which are used for routing 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.

Prerequisites

- You have completed the configuration of the ISP address library. For details, see [6.6 ISP Address Library](#).
- You have configured an ISP address library to be associated with WAN interfaces. For details, see [7.1 Interface](#).

Procedure

- (1) Choose **Network > Routing > Address Library Route**.
- (2) View the address library routing entries on the firewall.



7.3.5 Viewing Route Tables

Procedure

- (1) Choose **Network > Routing > Routing Table**.
- (2) View the routing entries on the firewall. Click the **IPv4** or **IPv6** tab to view the IPv4 or IPv6 routing tables.

The system automatically generates direct routes with a priority of 0.

Type	Dest. IP Range/Mask	Next-Hop Address	Priority	Interface
Static route	0.0.0.0/0	172.20.36.1	5	br0
Direct route	172.20.36.0/24	-	-	br0

7.4 Outbound Interface Load Balancing

7.4.1 Overview

When there are multiple equivalent egresses (that is, multiple links) for intranet users to access the extranet, you can configure outbound interface load balancing on the firewall to guarantee both service continuity and network quality.

The load balancing function does not forward data flows, but selects a proper outbound interface as the forwarding interface for the routing module. Therefore, outbound interface load balancing needs to be used with routing modules. The application scenarios include but not is limited to the following:

- Static routing: There are multiple equal-cost routes to the destination network.
- ISP routing: Multiple interfaces are associated with the same address library.
- PBR: The PBR rule that data flows match has multiple equivalent outbound interfaces.

Load balancing brings the following benefits:

- Network resources are fully utilized.
- The total bandwidth is increased.
- Link reliability is enhanced. When a link fails, traffic is switched to other load-balanced links, ensuring service continuity.

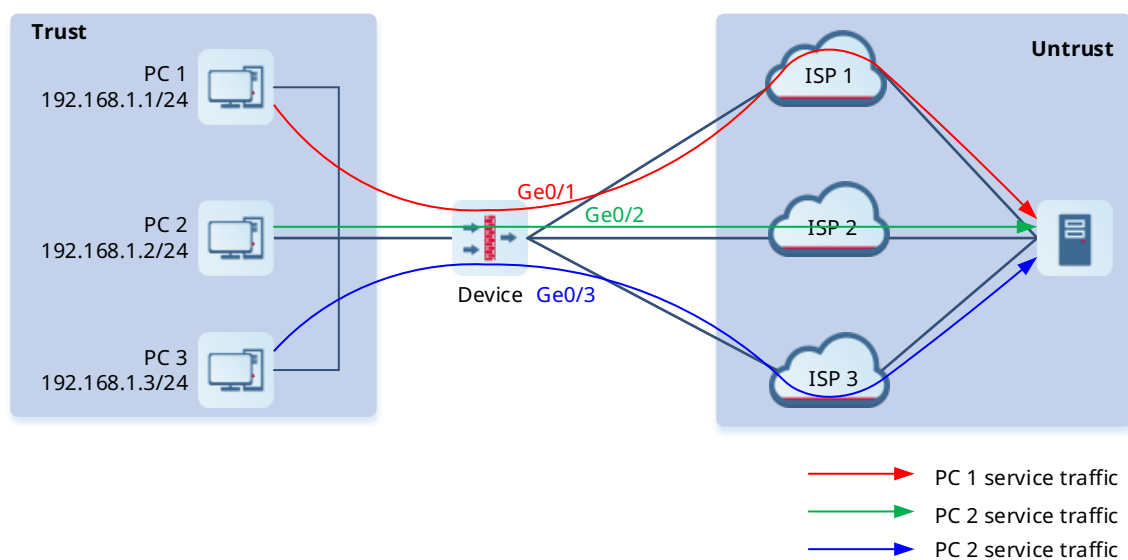
The device supports load balancing based on the source IP address or bandwidth. You can select one load balancing mode as required. The load balancing mode can be switched. After switching, the new load balancing mode is applied to newly generated data flows, and the old mode is still applied to existing data flows until they ages.

7.4.2 Configuring Source IP-based Load Balancing

Application Scenario

As shown in the following figure, interfaces Ge0/1, Ge0/2, and Ge0/3 on the firewall are configured with the same routing rule. When source IP-based load balancing is enabled, packets from the same source IP address are sent by the same interface. When traffic reaches the threshold of an interface, the interface does not participate in the load balancing of newly generated traffic. When the traffic reaches the thresholds of all the interfaces, all the interfaces participate in the load balancing of newly generated traffic.

This load balancing mode applies to scenarios where the link bandwidth and quality of multiple egresses are similar. In this mode, multiple data flows of the same service are transmitted on the same path, and packets of different services are evenly distributed among multiple outbound interfaces. In this way, service quality can be guaranteed.



Prerequisites

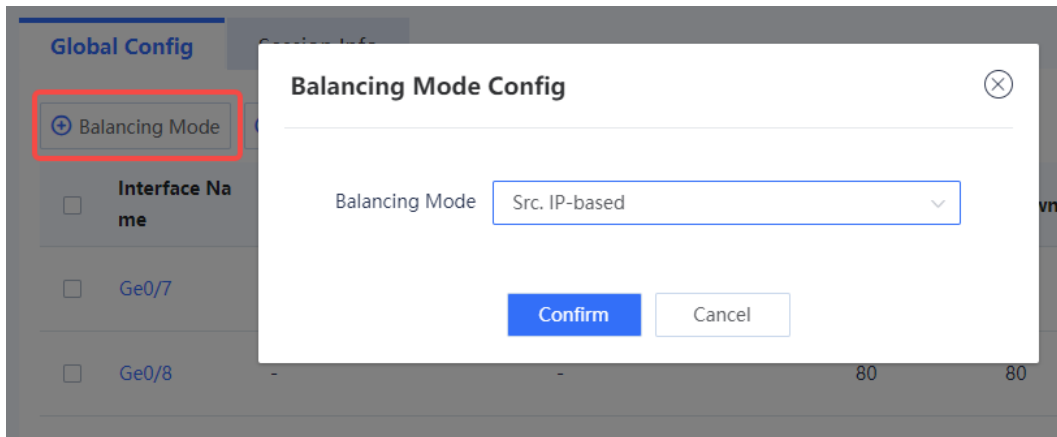
- More than one equivalent outbound interfaces are available for accessing the same destination network, and the interfaces are configured with the same routing rule.
- The outbound interface must be a WAN interface configured with correct basic information, including the IP address and next hop.

Precautions

Load balancing is not performed on traffic that enters an SSL VPN or IPsec VPN tunnel. This traffic is forwarded by specified tunnel interfaces.

Procedure

- (1) Choose **Network > Routing > Egress Load Balancing > Global Config**.
- (2) Click **Balancing Mode**. Select **Src. IP-based** from the **Balancing Mode** drop-down list.



(3) (Optional) Click **Edit** in the **Operation** column to modify the uplink and downlink bandwidths and load thresholds of the interface.

Interface Name	Uplink Bandwidth	Downlink Bandwidth	Uplink Load Threshold	Downlink Load Threshold	Status	Operation
Ge0/7	-	-	80	80	Load Balanced	🔴 Edit
Ge0/8	-	-	80	80	Load Balanced	🟢 Edit
Ge0/7.2	-	-	80	80	Load Balanced	🟢 Edit

a Modify the uplink and downlink bandwidths and load thresholds of the interface as required.

< Back

Edit Interface

Basic Info

Interface Name Ge0/7

Interface Bandwidth

Uplink Bandwidth

Mbps

Enter the uplink bandwidth.

Downlink Bandwidth

Mbps

Threshold

* Uplink Load Threshold

%

* Downlink Load

%

Threshold

Save

Note

When traffic on the interface reaches the specified load threshold, the interface does not participate in load balancing. For example, if the uplink bandwidth is 100 Mbps and the load threshold is 80%, when the occupied uplink bandwidth of the interface reaches 80 Mbps, the interface does not participate in load balancing.

- b After verifying the configuration, click **Save**.

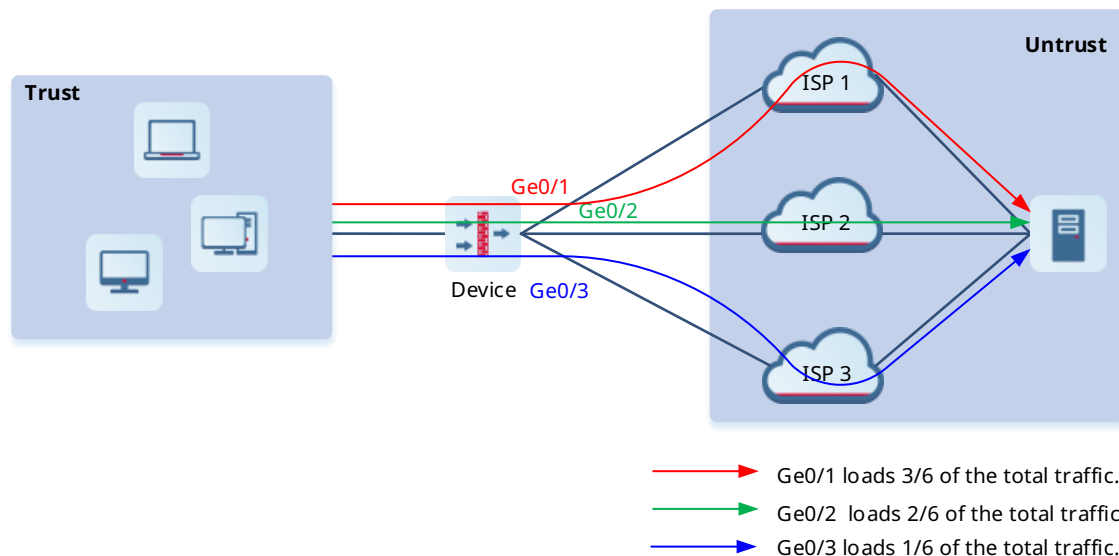
7.4.3 Configuring Bandwidth-based Load Balancing

Application Scenario

As shown in the following figure, interfaces Ge0/1, Ge0/2, and Ge0/3 on the firewall are configured with the same routing rule A. For Ge0/1, the bandwidth is 300 Mbps, and the load threshold is 90%. For Ge0/2, the bandwidth is 200 Mbps, and the load threshold is 90%. For Ge0/3, the bandwidth is 100 Mbps, and the load threshold is 80%.

When no interface traffic reaches the threshold, traffic that hits routing rule A is load balanced on Ge0/1, Ge0/2, and Ge0/3 at a ratio of 3:2:1. When traffic on Ge0/3 reaches its threshold, the interface does not participate in the load balancing of newly generated data flows. Subsequent traffic that hits routing rule A is only load balanced on Ge0/1 and Ge0/2 at a ratio of 3:2. When the traffic reaches the thresholds of all the interfaces, newly generated traffic that hits routing rule A is load balanced on the three interfaces at a ratio of 3:2:1 again.

In this mode, outbound interfaces with higher bandwidths load more traffic, and all interfaces participate in load balancing, fully utilizing interface bandwidths.



Prerequisites

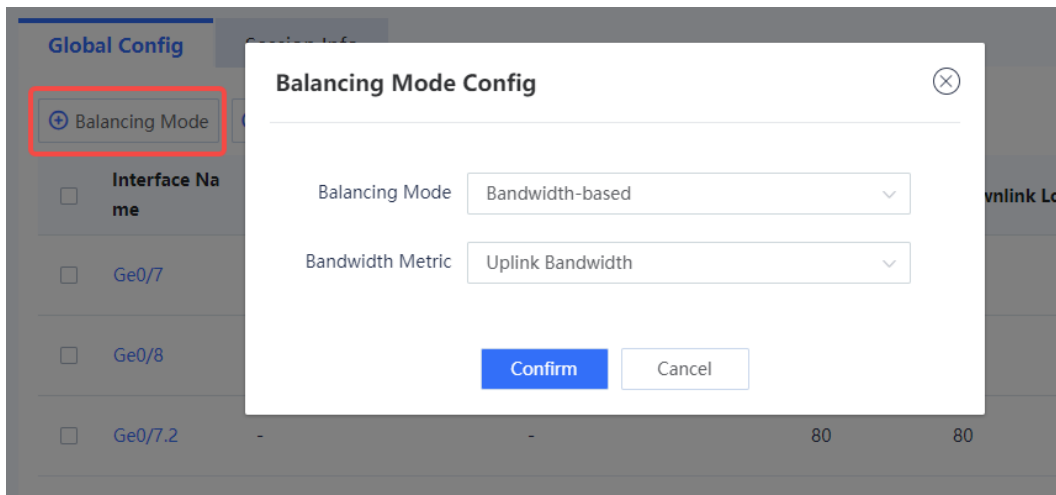
- More than one equivalent outbound interfaces are available for accessing the same destination network, and the interfaces are configured with the same routing rule.
- The outbound interface must be a WAN interface configured with correct basic information, including the IP address and next hop.

Precautions

Load balancing is not performed on traffic that enters an SSL VPN or IPsec VPN tunnel. This traffic is forwarded by specified tunnel interfaces.

Procedure

- (1) Choose **Network > Routing > Egress Load Balancing > Global Config**.
- (2) Click **Balancing Mode**. Select **Bandwidth-based** from the **Balancing Mode** drop-down list. Set **Bandwidth Metric** to **Uplink Bandwidth** or **Downlink Bandwidth**. (The following uses **Uplink Bandwidth** as an example).



- (3) Click **Edit** in the **Operation** column to modify the uplink bandwidth and load threshold of the interface.

Interface Name	Uplink Bandwidth	Downlink Bandwidth	Uplink Load Threshold	Downlink Load Threshold	Status	Operation
<input type="checkbox"/> Ge0/7	-	-	80	80	Load Balanced	<input checked="" type="checkbox"/> Edit
<input type="checkbox"/> Ge0/8	-	-	80	80	Load Balanced	<input checked="" type="checkbox"/> Edit
<input type="checkbox"/> Ge0/7.2	-	-	80	80	Load Balanced	<input checked="" type="checkbox"/> Edit

- a Modify the uplink bandwidth and load threshold of the interface as required.

Note

- After you set **Bandwidth Metric** to **Uplink Bandwidth** (or **Downlink Bandwidth**), the system prompts you to configure the uplink bandwidth or downlink bandwidth for the interface.
- When traffic on the interface reaches the specified load threshold, the interface does not participate in load balancing. For example, if the uplink bandwidth is 100 Mbps and the load threshold is 80%, when the occupied uplink bandwidth of the interface reaches 80 Mbps, the interface does not participate in load balancing.

< Back
Edit Interface

Basic Info

Interface Name Ge0/7

Interface Bandwidth

① Uplink Bandwidth

Mbps
▼
Enter the uplink bandwidth.

① Downlink Bandwidth

Mbps
▼

Threshold

* ① Uplink Load Threshold

%

* ① Downlink Load Threshold

%

Save

- b After verifying the configuration, click **Save**.

7.4.4 Viewing Load Balancing Session Information

Procedure

- (1) Choose **Network > Routing > Egress Load Balancing > Session Info**.
- (2) On the tab page, information about the sessions involved in load balancing is displayed.

Global Config
Session Info

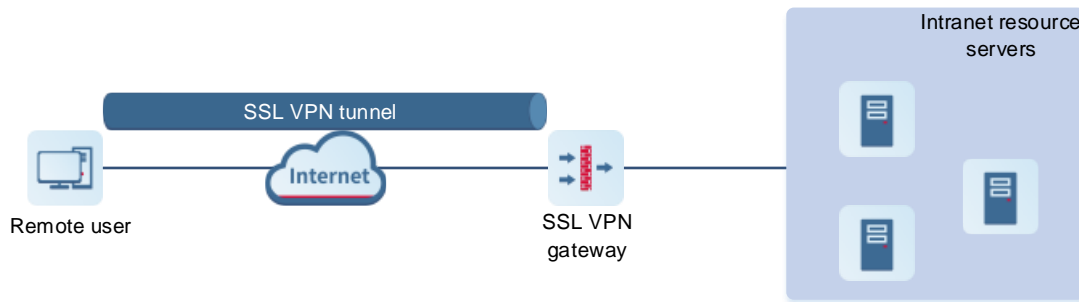
Clear Hit Record
Refresh

<input type="checkbox"/>	ID	Associated Route	Interface Name	Hit Sessions	Operation
No Data					

7.5 SSL VPN

7.5.1 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
RG-WALL 1600-Z5100-S	20

7.5.2 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.

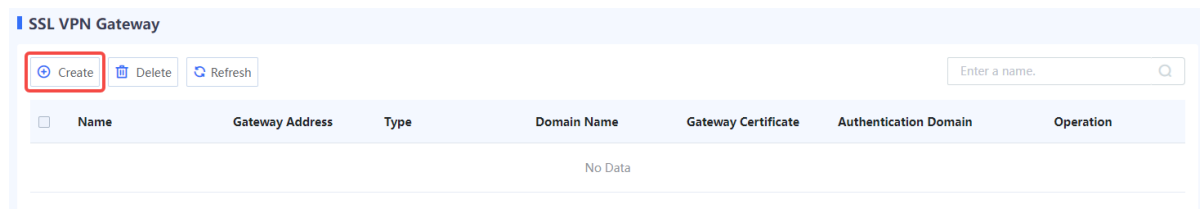
Precautions

- 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.

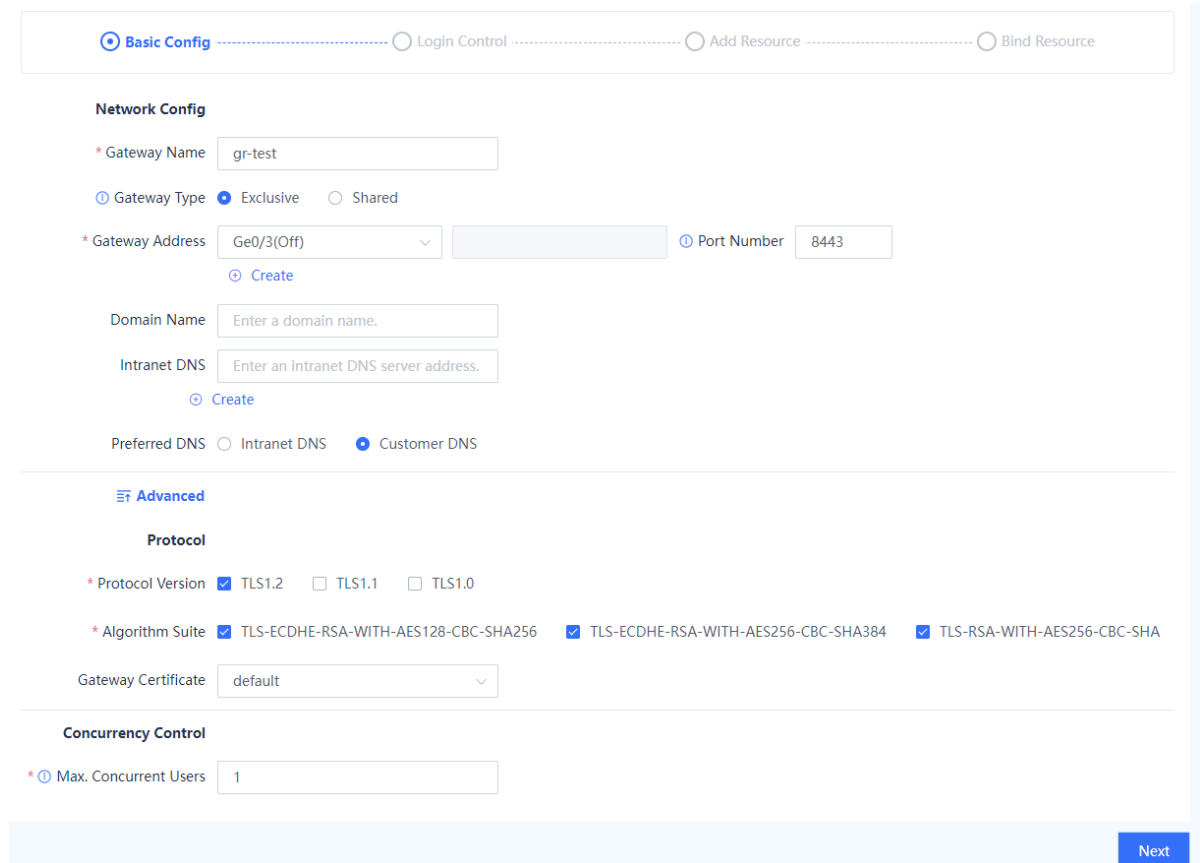
Procedure

- (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.



Item	Description	Remarks
Network Config		
Gateway Name	Name of the SSL VPN gateway.	[Example] gateway1
Gateway Type	<ul style="list-style-type: none"> ● Exclusive: The system allocates a unique IP address and domain name to the virtual gateway, and users can log in to the SSL VPN gateway by using the IP address (or domain name) and port number. ● Shared: The system allocates a shared IP address and domain name to the virtual gateway, and users can log in to the SSL VPN gateway by using the domain name and port number. 	[Example] Shared

Item	Description	Remarks
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 addresses, each of which can be used for login.	[Example] 1.1.1.1
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. Note: The domain name must be resolvable by public network DNS.	[Example] www.abc.com
Intranet DNS	IP address of the DNS server used to resolve internal domain names. You must configure this parameter when internal domain resources exist.	[Example] 192.168.0.1
Preferred DNS	Preferred DNS server used when internal network resources are accessed. You can specify the DNS server to be preferentially used for domain name resolution. If a domain name cannot be resolved, the DNS server of the client is used.	[Example] Intranet DNS
Advanced		
Protocol Version	Version of the SSL protocol used when an SSL connection is established between the SSL VPN gateway and client. The protocol version used by both ends must be the same.	[Example] 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 6.8.2 Local Certificate .	N/A
Concurrency Control		
Max. Concurrent Users	Maximum number of users that can concurrently log in to the SSL VPN gateway. When the maximum number of concurrent users is reached, new users cannot log in to the SSL VPN gateway.	[Example] 20

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

The screenshot shows the 'Add SSL VPN Gateway' configuration interface. At the top, there are four tabs: 'Basic Config' (checked), 'Login Control' (active), 'Add Resource', and 'Bind Resource'. Below the tabs, the configuration is organized into several sections:

- Authentication:** Includes a field for 'User Authentication Domain' set to 'default'.
- Prevent Brute-Force Attack:** Contains two sub-sections. The first, 'User Lockout', has a toggle set to 'On', 'Max. User Attempts' set to '5', and 'Lockout Period' set to '300' seconds. The second, 'Single IP Lockout', also has a toggle set to 'On', 'Max. Single IP Attempts' set to '5', and 'Lockout Period' set to '300' seconds.
- Login Verification:** Includes several options: 'Graphic Verification' (off), 'Enable upon' (0 Consecutive Input Errors), 'Hardware Signature Verification' (off), 'Maximum Signatures Bound to Each User' (3), 'Auto Hardware Signature Approval' (off), 'Auto User Unbinding' (off), and 'Auto Approval of Trusted Public Terminals' (off).
- Client Version Control:** Shows 'Available Client Versions' with 'Any Version' selected, and other options for 'Latest Version on Secure Cloud' and 'Custom Config'.

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

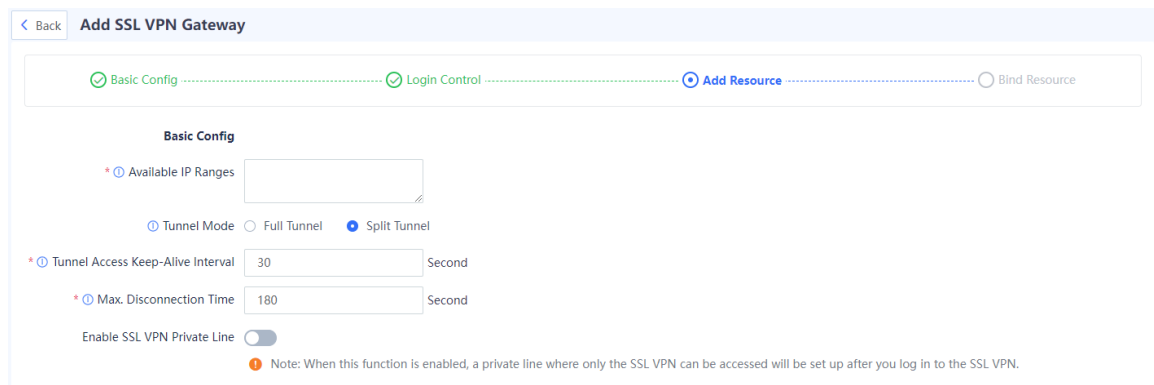
Item	Description	Remarks
Authentication		
User Authentication Domain	Authentication domain for which the login control policies configured on this page will be applied. An SSL VPN gateway can be bound to only one authentication domain.	[Example] default
Prevent Brute-Force Attack		
User Lockout	Specifies whether to enable user lockout after a certain number of consecutive failed login attempts. During the lockout period, the user cannot log in to the gateway.	[Example] Enable
Max. User Attempts	Maximum number of consecutive login failures that a user is allowed before being locked out.	[Example] 5
Lockout Period	Lockout period during which the user cannot log in to the gateway.	[Example] 300 seconds

Item	Description	Remarks
Single IP Lockout	Specifies whether to enable locking out of a specific IP address on which a certain number of consecutive login failures are detected. During the lockout period, the user cannot log in to the gateway from this IP address.	[Example] Enable
Max. Single IP Attempts	Maximum number of consecutive login failures that are allowed from a specific IP address before it is locked out.	[Example] 5
Lockout Period	Lockout period during which the user cannot log in to the gateway from the locked IP address.	[Example] 300 seconds
Login Verification		
Graphic Verification	Specifies whether to display a graphic verification code on the gateway login page after a certain number of consecutive login failures. This function can prevent 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 Approval	Specifies whether to enable automatic approval of hardware signatures for devices attempting to log in to the gateway.	[Example] Disable
Auto Unbinding	Specifies whether to allow users to unbind the hardware signatures from their accounts. If unbinding is performed when hardware signature verification is enabled, the hardware signature of the device needs to be approved again before the user logs in. For more information about how to manage hardware signatures, see 7.5.3 Hardware Signature Management .	[Example] Disable
Auto Approval of Trusted Public Terminals	Specifies whether to enable automatic approval of the trusted device whose hardware signature is imported to the firewall. Users associated with this hardware signature can log in to the gateway without manual approval.	N/A
Idle Timeout		

Item	Description	Remarks
The idle status will time out after	Maximum duration during which an SSL VPN session remains idle before it is forcibly terminated.	[Example] 30 minutes
Client Version Control		
Available Client Versions	<p>Version of the SSL VPN client that connects to the SSL VPN gateway. Currently, only Ruijie SSL VPN client is supported.</p> <ul style="list-style-type: none"> ● Any Version: no limit on the version of the SSL VPN client ● Latest Version on Secure Cloud: the latest version released on Ruijie Secure Cloud Platform ● Custom Config (The earliest version for clients on each platform can be specified.): custom client versions for each type of system 	[Example] Any Version

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

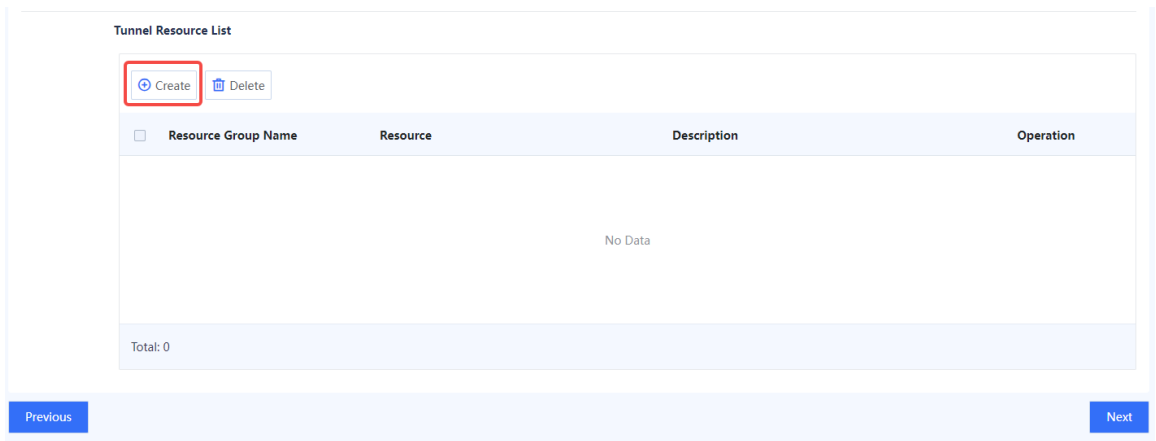
a Configure basic information:



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	<p>Supports two modes:</p> <ul style="list-style-type: none"> ● Split Tunnel: Only the traffic to authorized resources is sent through the SSL VPN tunnel. ● Full Tunnel: All user traffic, including traffic for Internet access and local communications, is sent through the SSL VPN tunnel. 	[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

Item	Description	Remarks
Max. Disconnection Time	Maximum disconnection time. If the SSL VPN client fails to send a keep-alive message to the SSL VPN gateway within the maximum disconnection time, the SSL VPN gateway closes the tunnel, and the user is forced to go offline. The maximum disconnection time should be at least three times the tunnel access keep-alive interval.	[Example] 180 seconds
SSL VPN Private Line	If this function is enabled, users can only access the addresses in the tunnel resource group list after logging in to the SSL VPN gateway. Other resources cannot be accessed.	[Example] Disable

- b If you set **Tunnel Mode** to **Split Tunnel**, you need to create a tunnel resource group. Click **Create** to configure the information of resources that can be accessed through this tunnel.



Add Tunnel Resource Group



* Tunnel Resource Group Name

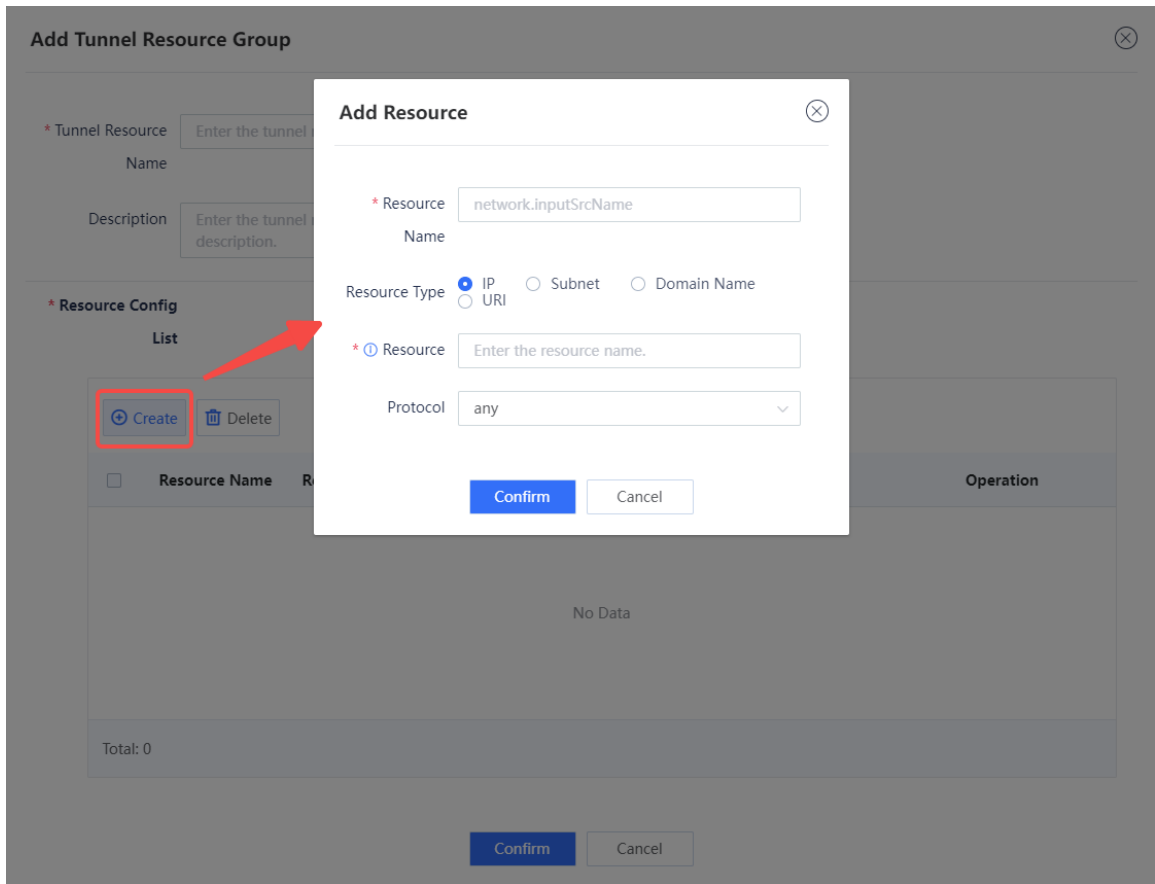
Description

* 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

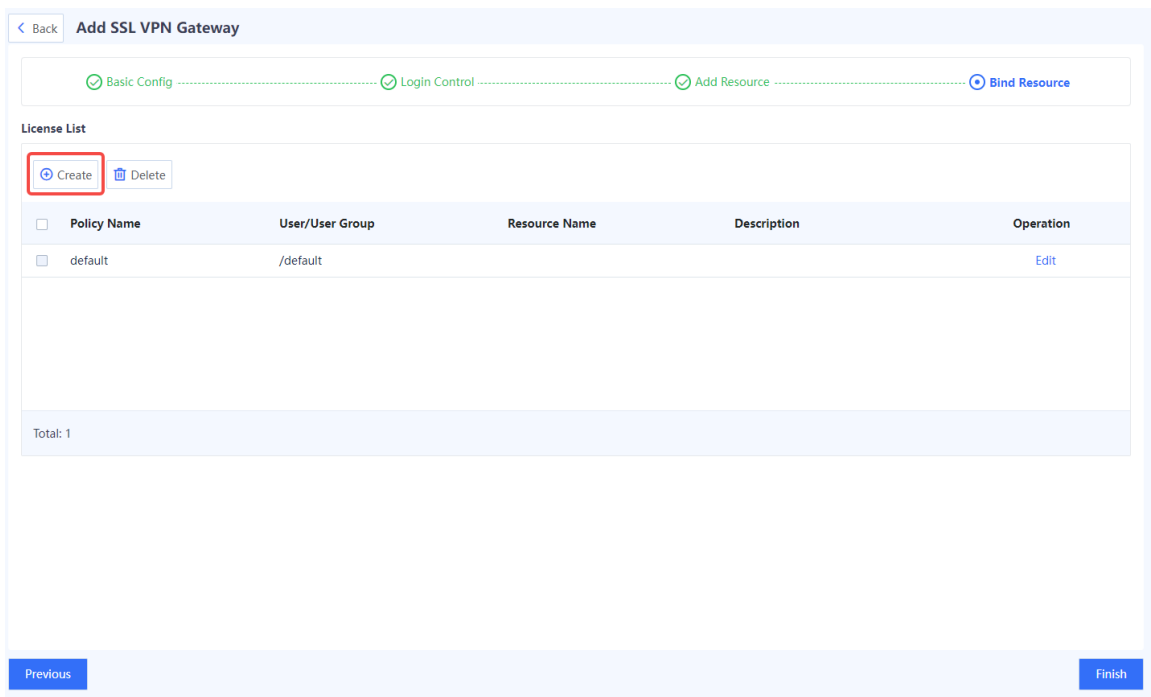
- c In the **Tunnel Resource List** area, click **Create** to configure the information of the resources in the resource group.



Item	Description	Remarks
Resource Name	Name of the resource that can be access through this tunnel.	[Example] IP
Resource Type	Supported resource types are as follows: <ul style="list-style-type: none"> ● IP: Only a single IP address is supported. Example: 192.168. 1.1. ● Subnet: IP/Mask length. Example: 192.168.1.0/24. ● Domain Name: Domain name. Example: www.abc.com. ● URI: URI. Example: <proto://ip[:port]>. 	N/A
Resource	Resource to be entered based on the selected resource type. For example, enter an IP address if Resource Type is set to IP .	N/A

Item	Description	Remarks
Protocol	Network protocol that specified resources use for authorized users to access. For example, if Resource Type is set to IP and this parameter is set to any , the user can access all external services provided at the IP address. If this parameter is set to TCP , the user can only access TCP-based external services provided at the IP address.	[Example] TCP

- d Verify the configuration and click **Confirm** to return to the **Add Tunnel Resource Group** page.
- (6) Verify the configured resource information, and click **Next** to configure the authorization policy for the resources that the user can access.
 - a Click **Create** to add an authorization policy, or click **Edit** in the **Operation** column to modify the existing policy.



- 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 (with the name of **sslvpn_c2s_SSL VPN gateway name**) 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.
- After the SSL VPN gateway is successfully added, a defense policy with the service type of SSL VPN is

automatically generated on the **Policy > Security Defense > Local Defense** page to permit SSL VPN traffic.

- 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.

7.5.3 Hardware Signature Management

Application Scenario

You can enable the hardware signature verification function, and bind hardware signatures with users. This limits the number of devices that can access the SSL VPN gateway and helps prevent unauthorized access and misuse of accounts.

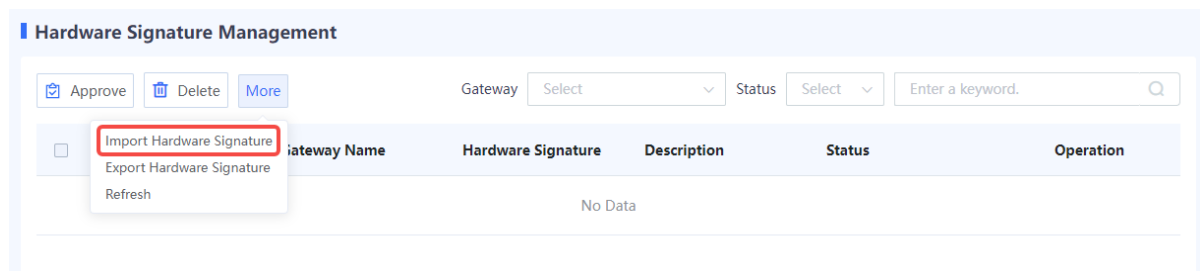
Administrators can manually or automatically approve the hardware signatures of user devices that request access to the gateway. Only approved devices are allowed to access internal resources through the gateway.

Precautions

- If the hardware signature verification and automatic approval functions are enabled when you create an SSL VPN gateway, devices with unapproved hardware signatures on this page can still log in to the gateway. After login, the device signature information will be imported and displayed on the **Hardware Signature Management** page and marked as approved.
- If you enable the hardware signature verification function but disable the automatic approval function when you create an SSL VPN gateway, the administrator needs to manually approve the devices on this page. Otherwise, the users associated with these hardware signatures cannot log in to the gateway.

Procedure

- (1) Choose **Network > SSL VPN > Hardware Signature Management**.
- (2) Click **More** and select **Import Hardware Signature**.



- (3) Select the gateway to which the hardware signature is imported. Click **Browse** to select the hardware signature file and upload it.

Note

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

Import Hardware Signature ✕

* Gateway ▼

Name

Signature

File

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

Hardware Signature Management

Approve
 Delete

Gateway ▼
Status ▼
 Q

<input type="checkbox"/>	Username	Gateway Name	Hardware Signature	Description	Status	Operation
No Data						

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

Hardware Signature Management

Approve
 Delete

Gateway ▼
Status ▼
 Q

<input type="checkbox"/>	Username	Gateway Name	Hardware Signature	Description	Status	Operation
No Data						

7.5.4 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.

Online User Info | Lock User Info | Lock IP Info

Refresh Offline Gateway Select Enter a username. Q

<input type="checkbox"/>	Gateway Name	Username	Login Time	Login IP	Virtual Addresses	Online Duration	Uplink Traffic	Downlink Traffic	Operation
No Data									

(3) To force a user to go offline, click **Offline** in the **Operation** column.

2. Viewing Locked User Information

(1) Choose **Network > SSL VPN > Operation Monitoring**.

(2) 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.

Online User Info | Lock User Info | Lock IP Info

Refresh Unlock Gateway Select Enter a username. Q

<input type="checkbox"/>	Locked Username	Lockout Duration	Login IP	Remaining Lockout Duration	Operation
No Data					

(3) To unlock a user, click **Unlock** in the **Operation** column.

3. Viewing Locked IP Information

(1) Choose **Network > SSL VPN > Operation Monitoring**.

(2) 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.

Online User Info | Lock User Info | Lock IP Info

Refresh Unlock Gateway Select Enter an IP address. Q

<input type="checkbox"/>	Locked IP	Lockout Duration	Remaining Lockout Duration	Operation
No Data				

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

7.6 IPsec VPN

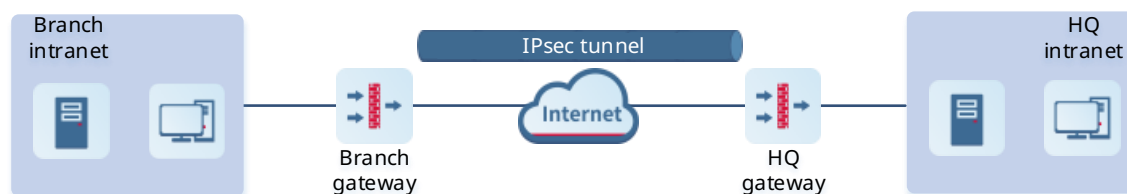
7.6.1 Overview

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 7-1 Typical Application Scenario of IPsec VPN



7.6.2 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.

7.6.3 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.

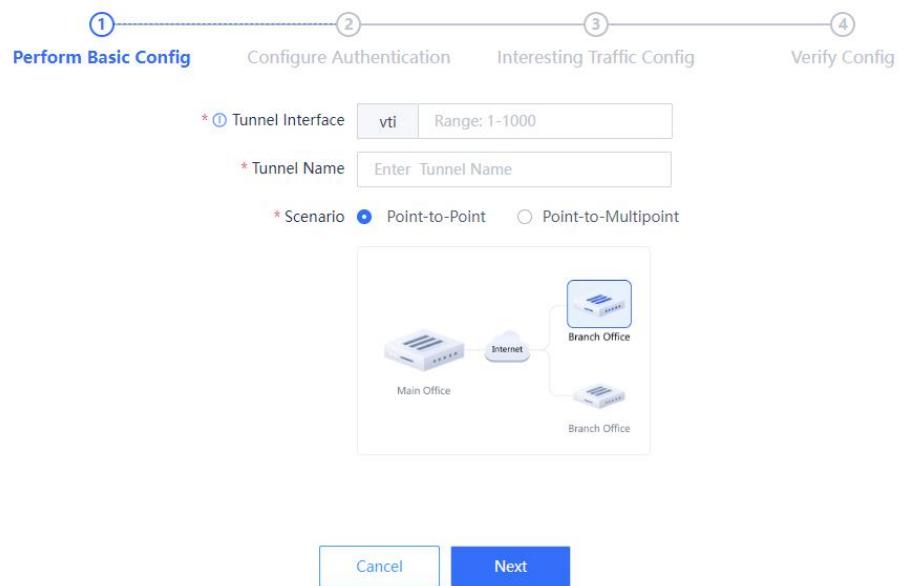
Caution

- 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



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 vti+Interface number. After completing IPsec VPN configuration on the wizard, you can view the automatically created tunnel interface information on the Tunnel Interface page.</p>	<p>Enter the interface number. Range: 1–1000.</p> <p>[Example]</p> <p>vti2</p>

Item	Description	Remarks
Tunnel Name	IPsec tunnel name.	Characters such as ~!#%^&*+ {};:"'</>? are not allowed. [Example] ipsec_1
Scenario	<p>Select the IPsec tunnel type based on the deployment scenario:</p> <ul style="list-style-type: none"> ● Point-to-Point: applies to scenarios where the peer end has a fixed IP address, such as IPsec VPN deployment at an enterprise branch. ● Point-to-Multipoint: 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. 	<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 Network > IPsec VPN > Custom Tunnel.</p> <p>[Example] Point-to-Point</p>

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

Perform Basic Config
 Configure Authentication
 Interesting Traffic Config
 Verify Config

* 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"> This parameter is mandatory in a point-to-point scenario. After entering the IP address or domain name, click Ping to verify that the devices at both ends are reachable to each other. The value must be the same as that of Local Address configured for the peer device. [Example] 40.0.0.50
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> [Example] Ge0/2
Authentication Mode	<p>Identity authentication mode of both ends of the tunnel.</p> <p>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.</p>	[Example] Pre-shared Key
Key	Key string for identity authentication in pre-shared key authentication mode.	<ul style="list-style-type: none"> Length range: 6 to 16 characters. Configure the same identity authentication mode (pre-shared key) and key for both ends. [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.

✔ ✔ 3 4
Perform Basic Config Configure Authentication Interesting Traffic Config Verify Config

Enter the keyword.

<input type="checkbox"/>	Proxy Mode	Local Network	Peer Network	Operation
No Data				

/ Page Total:0

Go to

- 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

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"> ● Auto: 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. ● Subnet-to-Subnet: Data flows between two specific subnets are protected. ● Host-to-Host: Data flows between two specific hosts are protected. 	<p>Point-to-point IPsec VPN does not support the Auto proxy mode.</p> <p>[Example]</p> <p>Subnet-to-Subnet</p>

Item	Description	Remarks
Local Network	Source address of interesting traffic. Typically, a network segment or specific host address to be protected on the local intranet is set.	The address format varies with the proxy mode: <ul style="list-style-type: none"> ● Subnet-to-Subnet: Enter an IP range. Example: 192.168.1.0/255.255.255.0 or 192.168.1.0/24. ● Host-to-Host: Enter an IP address. Example: 192.168.1.1.
Peer Network	Destination address of interesting traffic. Typically, a network segment or specific host address to be protected on the peer intranet is set.	The address format varies with the proxy mode: <ul style="list-style-type: none"> ● Subnet-to-Subnet: Enter an IP range. Example: 192.168.1.0/255.255.255.0 or 192.168.1.0/24. ● Host-to-Host: Enter an IP address. Example: 192.168.1.1.

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

Perform Basic Config Configure Authentication **Interesting Traffic Config** Verify Config

<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	Edit Delete

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.

✓ Perform Basic Config
 ✓ Configure Authentication
 ✓ Interesting Traffic Config
 4 Verify Config

ⓘ 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
Identity Authentication Parameters		
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. [Example] Enable

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

Item	Description	Remarks
Peer ID	String that identifies the peer device for identity authentication.	<ul style="list-style-type: none"> ● This parameter is mandatory when Peer Identity Authentication is enabled. ● The value must be the same as that of Local ID configured for the peer device. Obtain the value from the administrator of the peer device. ● The string format varies with the peer ID type: <ul style="list-style-type: none"> ○ IPV4_ADDRESS: IP address of the peer end. Example: 10.1.1.1. ○ FQDN: Domain name of the peer end. Example: bbb.com. ○ USER_FQDN: User domain name of the peer end in the format of <i>Username@Domain name</i>. Example: susan@bbb.com.
<p>DPD</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	<p>Two DPD modes are supported:</p> <ul style="list-style-type: none"> ● Idle Mode: 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. ● Regular Mode: The local end sends DPD messages periodically based on the configured DPD detection interval. 	<p>This parameter is supported in a point-to-point scenario.</p> <p>[Example]</p> <p>Idle Mode</p>
DPD Detection Interval	In regular mode, set the interval between two DPD detections, in seconds.	<p>The default value is 30 seconds.</p> <p>[Example]</p> <p>30</p>
DPD Retry Interval	<p>Interval for retransmitting DPD messages.</p> <p>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.</p>	<p>The default value is 5 seconds.</p> <p>[Example]</p> <p>3</p>

Item	Description	Remarks
<p>Reverse Route Injection</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 Injection	Whether to enable reverse route injection.	[Example] Enable
Next-Hop Address	Next-hop address of the route.	<ul style="list-style-type: none"> ● Optional. ● The default outbound interface of the route is the virtual tunnel interface associated with the IPsec tunnel. [Example] 192.168.1.1
Priority	Route priority.	Range: 1–255. Default: 5. [Example] 5
<p>IKE Parameters</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 SA Lifetime must have the same values in the IPsec VPN configuration of the peer device.</p>		
Negotiation Mode	IKE negotiation mode in phase 1. The following modes are supported: <ul style="list-style-type: none"> ● IKEv1 Main Mode: In this mode, identity information is encrypted and protected for higher security. ● IKEv1 Aggressive Mode: In this mode, the negotiation speed is faster, but identity information is not encrypted or protected. 	[Example] IKEv1 Main Mode

Item	Description	Remarks
Encryption Algorithm	<p>Encryption algorithm used in IKE negotiation for establishing IPsec SAs.</p> <p>The following values are supported:</p> <ul style="list-style-type: none"> ● DES: DES algorithm using 56-bit keys ● 3DES: 3DES algorithm using 168-bit keys ● AES-128: AES algorithm using 128-bit keys ● AES-192: AES algorithm using 192-bit keys ● AES-256: AES algorithm using 256-bit keys <p>In order of security from high to low: AES-256 > AES-192 > AES-128 > 3DES > DES.</p>	<ul style="list-style-type: none"> ● Select one or more options from the drop-down list. ● The default encryption algorithm is AES-128. <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"> ● MD5: MD5 algorithm that produces a 128-bit message digest ● SHA: SHA1 algorithm that produces a 160-bit message digest ● SHA-256: SHA2-256 algorithm that produces a 256-bit message digest ● SHA-384: SHA2-384 algorithm that produces a 384-bit message digest ● SHA-512: SHA2-512 algorithm that produces a 512-bit message digest <p>A longer message digest indicates higher security and slower calculation.</p>	<ul style="list-style-type: none"> ● Select one or more options from the drop-down list. ● The default authentication algorithm is SHA. <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"> ● GROUP1: 768-bit DH group ● GROUP2: 1024-bit DH group ● GROUP5: 1536-bit DH group ● GROUP14: 2048-bit DH group ● GROUP15: 3072-bit DH group ● GROUP16: 4096-bit DH group <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"> ● Select one or more options from the drop-down list. ● The default value is GROUP5. <p>[Example] GROUP14</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"> ● Range: 120–604800, in seconds. ● The default value is 86400 seconds (one day). <p>[Example] 86400</p>
<p>IPsec Parameters</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 SA Lifetime must have the same values in the IPsec VPN configuration of the peer device.</p>		
Protocol	<p>Security protocol used by IPsec.</p> <p>Currently, only Encapsulating Security Payload (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"> ● DES: DES algorithm using 56-bit keys ● 3DES: 3DES algorithm using 168-bit keys ● AES-128: AES algorithm using 128-bit keys ● AES-192: AES algorithm using 192-bit keys ● AES-256: AES algorithm using 256-bit keys ● NULL: no encryption <p>In order of security from high to low: AES-256 > AES-192 > AES-128 > 3DES > DES.</p>	<ul style="list-style-type: none"> ● Select one or more options from the drop-down list. ● The default encryption algorithm is AES-128. <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"> ● MD5: MD5 algorithm that produces a 128-bit message digest ● SHA: SHA1 algorithm that produces a 160-bit message digest ● SHA-256: SHA2-256 algorithm that produces a 256-bit message digest ● SHA-384: SHA2-384 algorithm that produces a 384-bit message digest ● SHA-512: SHA2-512 algorithm that produces a 512-bit message digest <p>A longer message digest indicates higher security and slower calculation.</p>	<ul style="list-style-type: none"> ● Select one or more options from the drop-down list. ● The default authentication algorithm is SHA. <p>[Example] MD5</p>
Perfect Forward Secrecy	<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] Enable</p>

Item	Description	Remarks
DH Group	<p>DH group used by PFS. The following values are supported:</p> <ul style="list-style-type: none"> ● GROUP1: 768-bit DH group ● GROUP2: 1024-bit DH group ● GROUP5: 1536-bit DH group ● GROUP14: 2048-bit DH group ● GROUP15: 3072-bit DH group ● GROUP16: 4096-bit DH group <p>A larger group number indicates higher security and slower key calculation.</p>	<ul style="list-style-type: none"> ● Select one or more options from the drop-down list. ● When PFS is enabled, GROUP5 is set by default. <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"> ● Range: 60–604800, in seconds. ● The default value is 3600 seconds (1 hour). <p>[Example] 3000</p>
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"> ● The default value is 1400 bytes. ● The tunnel MTU must be smaller than the outbound interface MTU. <p>[Example] 1480</p>


(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"> ● Name: The value is the same as that of Tunnel Name set for the IPsec tunnel. ● Interface List: The IPsec tunnel interface is added to the list.

Item	Description
Tunnel Interface	<p>The IPsec tunnel interface is added:</p> <ul style="list-style-type: none"> ● Security Zone: The value is the same as that of Tunnel Name set for the IPsec tunnel. ● Tunnel Local Address: IP address of the outbound interface. ● Tunnel Remote Address: IP address used by the peer end to establish the IPsec tunnel. The value is the same as that of Peer Address set in Configure Authentication.
Static Routing	<p>The static route to the peer intranet is added:</p> <ul style="list-style-type: none"> ● Dest. IP Range/Mask: Peer network address set in interesting traffic configuration. ● Interface: IPsec tunnel interface. ● Priority: 5
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"> ● Security policy in the inbound direction: <ul style="list-style-type: none"> ○ Src. Security Zone: The value is the same as that of Tunnel Name set for the IPsec tunnel. (The tunnel interface is added to the zone.) ○ Src. Address: Peer network address set in interesting traffic configuration. ○ Dest. Security Zone: any ○ Dest. Address: Local network address set in interesting traffic configuration. ○ Action: permit ● Security policy in the outbound direction: <ul style="list-style-type: none"> ○ Src. Security Zone: any ○ Src. Address: Local network address set in interesting traffic configuration. ○ Src. Security Zone: The value is the same as that of Tunnel Name set for the IPsec tunnel. (The tunnel interface is added to the zone.) ○ Dest. Address: Peer network address set in interesting traffic configuration. ○ Action: permit
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"> ● Src. Security Zone: any ● Src. Address: any ● Dest. Address: any ● Service: IKE, ESP ● Action: permit

- 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.

7.6.4 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:

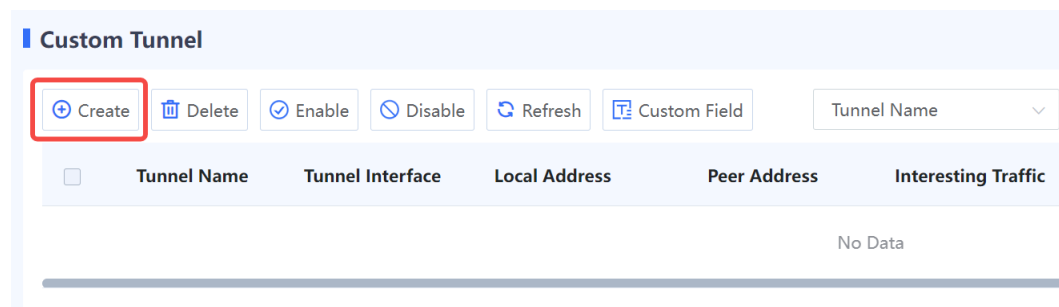
- Create tunnel interfaces to be bound to IPsec tunnel policies based on actual networking requirements. For details on how to create a tunnel interface, see [7.1.5 Configuring a Tunnel interface](#).
- In a point-to-point IPsec VPN scenario, obtain the IP address or domain name of the peer end, as well 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 ① Point-to-Multipoint ①

* Tunnel Name Enter Tunnel Name

Description

* Enabled State Enable Disable

* Tunnel Interface ⊕ Add Tunnel Interface

* Authentication Mode

* Password

* Confirm Key

* Local Address Interface ① IP ①

* Peer Address

Enable Peer Identity Authentication

* Local ID Type

DPD Type

DPD Retry Interval Second

Item	Description	Remarks
Scenario	Select the IPsec tunnel type based on the deployment scenario: <ul style="list-style-type: none"> ● Point-to-Point: applies to scenarios where the peer end has a fixed IP address, such as IPsec VPN deployment at an enterprise branch. ● Point-to-Multipoint: 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. 	On the firewall, one point-to-multipoint IPsec VPN tunnel and multiple point-to-point IPsec VPN tunnels can be configured. [Example] Point-to-Point

Item	Description	Remarks
Tunnel Name	IPsec tunnel name.	<p>Characters such as ~!#%^&*+ {};:"/<>? are not allowed.</p> <p>[Example] ipsec_1</p>
Description	Tunnel description. Provide brief description to help the administrator understand the function of the tunnel.	<p>[Example] 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] Enable</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"> ● Select a configured tunnel interface from the drop-down list. ● To add a tunnel interface, click Add Tunnel Interface. <p>[Example] vti2</p>
Authentication Mode	Identity authentication mode of both ends of the tunnel. Currently, only pre-shared key authentication is supported.	<p>[Example] Pre-shared Key</p>
Key	Key string for identity authentication in pre-shared key authentication mode.	<ul style="list-style-type: none"> ● Length range: 6 to 16 characters. ● Configure the same identity authentication mode (pre-shared key) and key for both ends. <p>[Example] Ruijie123</p>
Local Address	Select the local interface or IP address for establishing a tunnel with the peer end.	<ul style="list-style-type: none"> ● If Interface 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. ● If IP is selected, specify a local IP address as the local address of the IPsec tunnel. ● The value must be the same as that of Peer Address configured for the peer device.

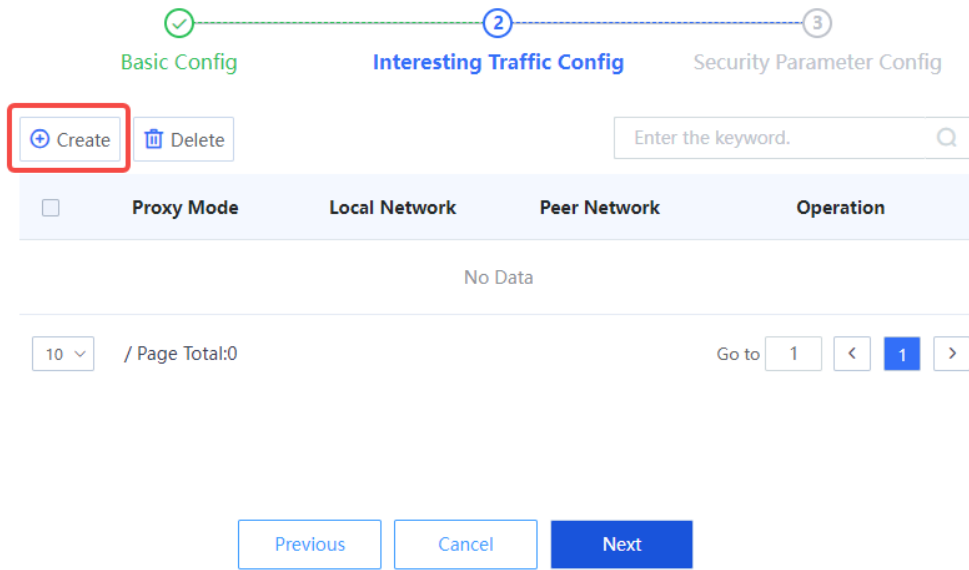
Item	Description	Remarks
Peer Address	IP address or domain name used by the peer device to establish the tunnel.	<ul style="list-style-type: none"> ● This parameter is mandatory in a point-to-point scenario. ● After entering the IP address or domain name, click Ping to verify that the devices at both ends are reachable to each other. ● The value must be the same as that of Local Address configured for the peer device. [Example] 40.0.0.5
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. [Example] Enable
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"> ● IPV4_ADDRESS: An IPv4 address is used as the local ID for IKE negotiation. ● FQDN: A Fully Qualified Domain Name (FQDN) string is used as the local ID for IKE negotiation. ● USER_FQDN: A user FQDN string is used as the local ID for IKE negotiation. 	If IPV4_ADDRESS is selected, the device uses the local 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"> ● The value must be the same as that of Peer ID configured for the peer device. ● The string format varies with the local ID type: <ul style="list-style-type: none"> ○ FQDN: Domain name of the local end. Example: aaa.com. ○ USER_FQDN: User domain name of the local end in the format of <i>Username@Domain name</i>. Example: julia@aaa.com.

Item	Description	Remarks
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"> ● IPV4_ADDRESS: The peer end uses an IPv4 address as the peer ID for identity authentication. ● FQDN: The peer end uses an FQDN string as the peer ID for identity authentication. ● USER_FQDN: The peer end uses a user FQDN string as the peer ID for identity negotiation. 	<ul style="list-style-type: none"> ● This parameter is mandatory when Peer Identity Authentication is enabled. ● The value must be the same as that of Local ID Type configured for the peer device. Obtain the value from the administrator of the peer device. <p>[Example]</p> <p>IPV4_ADDRESS</p>
Peer ID	<p>String that identifies the peer device for identity authentication.</p>	<ul style="list-style-type: none"> ● This parameter is mandatory when Peer Identity Authentication is enabled. ● The value must be the same as that of Local ID configured for the peer device. Obtain the value from the administrator of the peer device. ● The string format varies with the peer ID type: <ul style="list-style-type: none"> ○ IPV4_ADDRESS: IP address of the peer end. Example: 10.1.1.1. ○ FQDN: Domain name of the peer end. Example: bbb.com. ○ USER_FQDN: User domain name of the peer end in the format of <i>Username@Domain name</i>. Example: susan@bbb.com.
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"> ● Idle Mode: 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. ● Regular Mode: The local end sends DPD messages periodically based on the configured DPD detection interval. 	<p>This parameter is supported in a point-to-point scenario.</p> <p>[Example]</p> <p>Idle Mode</p>
DPD Detection Interval	<p>In regular mode, set the interval between two DPD detections, in seconds.</p>	<p>The default value is 30 seconds.</p> <p>[Example]</p> <p>30</p>

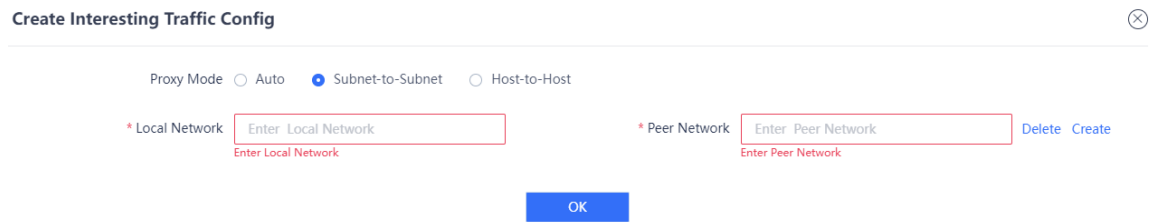
Item	Description	Remarks
DPD Retry Interval	Interval for retransmitting DPD messages. After sending a DPD request message, if the local end does not receive a response message within the retry interval, it retransmits the DPD request message. If the local end does not receive a response message after 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"> This parameter takes effect only when reverse route injection is enabled. The default outbound interface of the route is the IPsec tunnel interface. [Example] 192.168.1.1
Priority	Route priority.	<ul style="list-style-type: none"> This parameter takes effect only when reverse route injection is enabled. Range: 1–255. Default: 5. [Example] 5

(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	<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"> ● Auto: 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. ● Subnet-to-Subnet: Data flows between two specific subnets are protected. ● Host-to-Host: Data flows between two specific hosts are protected. 	<p>[Example] Subnet-to-Subnet</p>

Item	Description	Remarks
Local Network	Source address of interesting traffic. Typically, a network segment or specific host address to be protected on the local intranet is set.	The address format varies with the proxy mode: <ul style="list-style-type: none"> ● Subnet-to-Subnet: Enter an IP range. Example: 192.168.1.0/255.255.255.0 or 192.168.1.0/24. ● Host-to-Host: Enter an IP address. Example: 192.168.1.1.
Peer Network	Destination address of interesting traffic. Typically, a network segment or specific host address to be protected on the peer intranet is set.	The address format varies with the proxy mode: <ul style="list-style-type: none"> ● Subnet-to-Subnet: Enter an IP range. Example: 192.168.1.0/255.255.255.0 or 192.168.1.0/24. ● Host-to-Host: Enter an IP address. Example: 192.168.1.1.

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

Basic Config Interesting Traffic Config Security Parameter Config

<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	Edit Delete

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

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

✓
✓
3

Basic Config
Interesting Traffic Config
Security Parameter Config

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

Tunnel MTU Second

Previous
Cancel
Finish

Item	Description	Remarks
<p>IKE Parameters</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 SA Lifetime must have the same values in the IPsec VPN configuration of the peer device.</p>		
Negotiation Mode	IKE negotiation mode in phase 1. The following modes are supported: <ul style="list-style-type: none"> ● IKEv1 Main Mode: In this mode, identity information is encrypted and protected for higher security. ● IKEv1 Aggressive Mode: In this mode, the negotiation speed is faster, but identity information is not encrypted or protected. 	[Example] IKEv1 Main Mode

Item	Description	Remarks
Encryption Algorithm	<p>Encryption algorithm used in IKE negotiation for establishing IPsec SAs.</p> <p>The following values are supported:</p> <ul style="list-style-type: none"> ● DES: DES algorithm using 56-bit keys ● 3DES: 3DES algorithm using 168-bit keys ● AES-128: AES algorithm using 128-bit keys ● AES-192: AES algorithm using 192-bit keys ● AES-256: AES algorithm using 256-bit keys <p>In order of security from high to low: AES-256 > AES-192 > AES-128 > 3DES > DES.</p>	<ul style="list-style-type: none"> ● Select one or more options from the drop-down list. ● The default encryption algorithm is AES-128. <p>[Example]</p> <p>AES-192</p>
Authentication Algorithm	<p>Authentication algorithm used in IKE negotiation. The following values are supported:</p> <ul style="list-style-type: none"> ● MD5: MD5 algorithm that produces a 128-bit message digest ● SHA: SHA1 algorithm that produces a 160-bit message digest ● SHA-256: SHA2-256 algorithm that produces a 256-bit message digest ● SHA-384: SHA2-384 algorithm that produces a 384-bit message digest ● SHA-512: SHA2-512 algorithm that produces a 512-bit message digest <p>A longer message digest indicates higher security and slower calculation.</p>	<ul style="list-style-type: none"> ● Select one or more options from the drop-down list. ● The default authentication algorithm is SHA. <p>[Example]</p> <p>MD5</p>
DH Group	<p>DH group used in IKE negotiation. The following values are supported:</p> <ul style="list-style-type: none"> ● GROUP1: 768-bit DH group ● GROUP2: 1024-bit DH group ● GROUP5: 1536-bit DH group ● GROUP14: 2048-bit DH group ● GROUP15: 3072-bit DH group ● GROUP16: 4096-bit DH group <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"> ● Select one or more options from the drop-down list. ● The default value is GROUP5. <p>[Example]</p> <p>GROUP14</p>

Item	Description	Remarks
SA Lifetime	IKE SA lifetime. The actual IKE SA lifetime depends on the negotiation result of the two ends.	<ul style="list-style-type: none"> ● Range: 120–604800, in seconds. ● The default value is 86400 seconds (one day). [Example] 86400
<p>IPsec Parameters</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 SA Lifetime must have the same values in the IPsec VPN configuration of the peer device.</p>		
Protocol	Security protocol used by IPsec. Currently, only ESP is supported. The ESP protocol supports packet encryption and authentication.	[Example] ESP
Encapsulation Mode	Encapsulation mode of IPsec. Currently, only the tunnel mode is supported.	[Example] Tunnel
Encryption Algorithm	Encryption algorithm used by the IPsec tunnel. The following values are supported: <ul style="list-style-type: none"> ● DES: DES algorithm using 56-bit keys ● 3DES: 3DES algorithm using 168-bit keys ● AES-128: AES algorithm using 128-bit keys ● AES-192: AES algorithm using 192-bit keys ● AES-256: AES algorithm using 256-bit keys ● NULL: no encryption In order of security from high to low: AES-256 > AES-192 > AES-128 > 3DES > DES.	<ul style="list-style-type: none"> ● Select one or more options from the drop-down list. ● The default encryption algorithm is AES-128. [Example] AES-192
Authentication Algorithm	Authentication algorithm used by the IPsec tunnel. The following values are supported: <ul style="list-style-type: none"> ● MD5: MD5 algorithm that produces a 128-bit message digest ● SHA: SHA1 algorithm that produces a 160-bit message digest ● SHA-256: SHA2-256 algorithm 	<ul style="list-style-type: none"> ● Select one or more options from the drop-down list. ● The default authentication algorithm is SHA. [Example] MD5

Item	Description	Remarks
	<p>that produces a 256-bit message digest</p> <ul style="list-style-type: none"> ● SHA-384: SHA2-384 algorithm that produces a 384-bit message digest ● SHA-512: SHA2-512 algorithm that produces a 512-bit message digest <p>A longer message digest indicates higher security and slower calculation.</p>	
Perfect Forward Secrecy	<p>Whether to enable the 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>Enable</p>
DH Group	<p>DH group used by PFS. The following values are supported:</p> <ul style="list-style-type: none"> ● GROUP1: 768-bit DH group ● GROUP2: 1024-bit DH group ● GROUP5: 1536-bit DH group ● GROUP14: 2048-bit DH group ● GROUP15: 3072-bit DH group ● GROUP16: 4096-bit DH group <p>A larger group number indicates higher security and slower key calculation.</p>	<ul style="list-style-type: none"> ● Select one or more options from the drop-down list. ● When PFS is enabled, GROUP5 is set by default. <p>[Example]</p> <p>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"> ● Range: 60–604800, in seconds. ● The default value is 3600 seconds (1 hour). <p>[Example]</p> <p>3000</p>
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"> ● The default value is 1400 bytes. ● The tunnel MTU must be smaller than the outbound interface MTU. <p>[Example]</p> <p>1480</p>

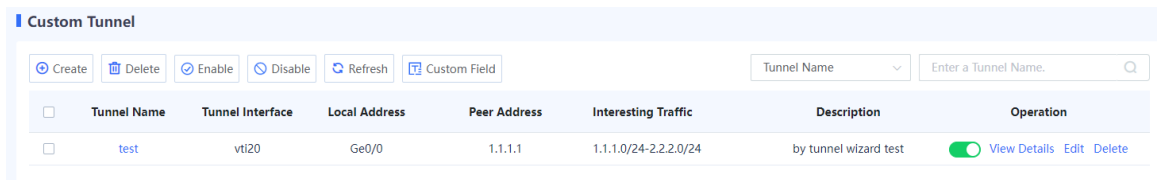
- (5) After verifying the configurations, click **Finish** to save the configurations. To modify the configurations, click **Previous**.


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"> ● Dest. IP Range/Mask: Peer network address set in interesting traffic configuration. ● Interface: Tunnel interface associated with the IPsec tunnel. ● Priority: 5
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"> ● Security policy in the inbound direction: <ul style="list-style-type: none"> ○ Src. Security Zone: untrust ○ Src. Address: Peer network address set in interesting traffic configuration. ○ Dest. Security Zone: trust ○ Dest. Address: Local network address set in interesting traffic configuration. ○ Action: permit ● Security policy in the outbound direction: <ul style="list-style-type: none"> ○ Src. Security Zone: any ○ Src. Address: Local network address set in interesting traffic configuration. ○ Dest. Security Zone: untrust ○ Dest. Address: Peer network address set in interesting traffic configuration. ○ Action: permit

- 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.

7.6.5 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.

Advanced Settings Details

NAT traversal

* ⓘ NAT Keep-Alive Interval Second

ⓘ Anti-Replay Attack

Anti-Replay Window

Action Specified by DF Bit

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 an IPsec-encapsulated packet so that the packet can traverse the NAT device.	Enabled by default. [Example] Enable
NAT Keep-Alive Interval	Sending interval of NAT keepalive packets. 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.	<ul style="list-style-type: none"> ● This parameter takes effect only when NAT Traversal is enabled. ● The default NAT keep-alive interval is 20 seconds. [Example] 20 seconds

Item	Description	Remarks
Anti-Replay Attack	<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]</p> <p>20 seconds</p>
Anti-Replay Window	<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"> ● This parameter takes effect only when the anti-replay attack function is enabled. ● The default value is 64 bits. ● 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. ● 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. <p>[Example]</p> <p>64</p>

Item	Description	Remarks
Action Specified by DF Bit	<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"> ● clear: The DF flag bit is set to 0, which indicates that IPsec-encapsulated packets can be fragmented. ● set: The DF flag bit is set to 1, which indicates that IPsec-encapsulated packets cannot be fragmented. ● copy: The DF flag bit of the outer IP header is set to the same as the DF flag bit of the original packet. 	<ul style="list-style-type: none"> ● 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. ● 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 clear). ● The default action is clear, which allows IPsec packet fragmentation. <p>[Example]</p> <p>clear</p>

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

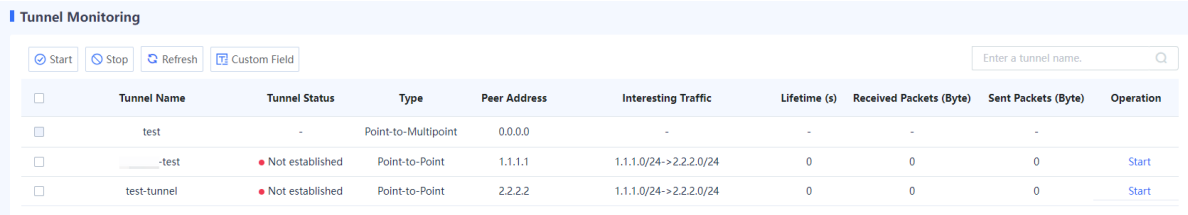
7.6.6 Tunnel Monitoring

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

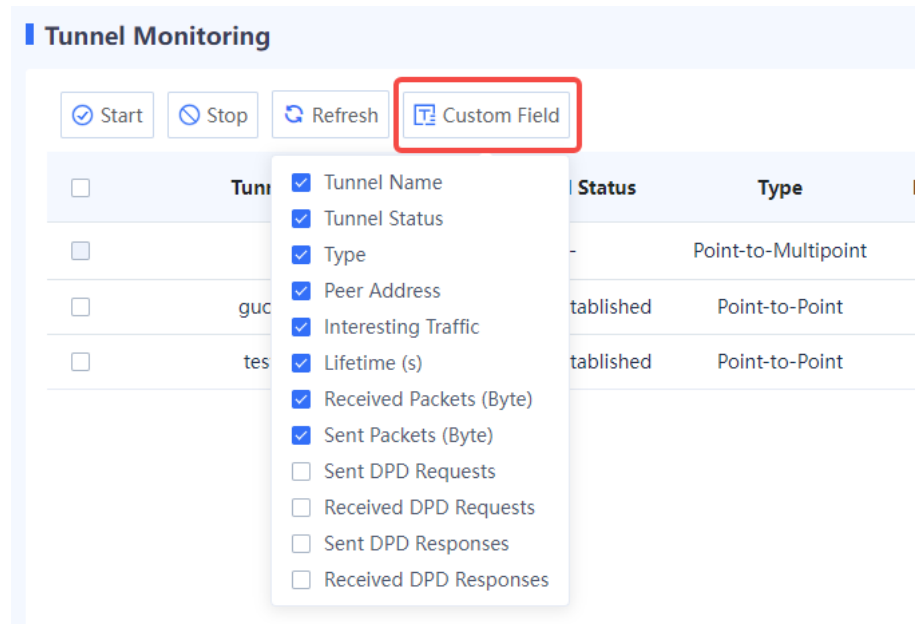
(1) Choose **Network > IPsec VPN > Tunnel Monitoring**.



The screenshot shows the 'Tunnel Monitoring' page with a search bar and a table of tunnels. The table has columns for Tunnel Name, Tunnel Status, Type, Peer Address, Interesting Traffic, Lifetime (s), Received Packets (Byte), Sent Packets (Byte), and Operation.

Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Received Packets (Byte)	Sent Packets (Byte)	Operation
test	-	Point-to-Multipoint	0.0.0.0	-	-	-	-	
-test	Not established	Point-to-Point	1.1.1.1	1.1.1.0/24->2.2.2.0/24	0	0	0	Start
test-tunnel	Not established	Point-to-Point	2.2.2.2	1.1.1.0/24->2.2.2.0/24	0	0	0	Start

(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.

Item	Description
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**.

7.6.7 Viewing IPsec VPN Logs

IPsec VPN logs record important events and abnormal information during the working process of IPsec tunnels. The logs help administrators locate and rectify faults when IPsec VPN functions are abnormal. For details on how to view IPsec VPN logs, see [9.2.2 6. Querying IPsec VPN Logs](#).

7.7 DNS Server

7.7.1 Overview

TCP/IP enables device communications using IP addresses. However, complex IP addresses can be difficult to remember for users. To address this issue, host names (in the form of strings) that correspond to IP addresses were designed. Domain Name System (DNS) is introduced to provide and resolve the mapping between domain names and IP addresses.

DNS is a distributed database on the Internet that provides mapping between domain names and IP addresses, making it easier for users to access the Internet without memorizing IP addresses 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.

A firewall can act as a DNS client and dynamically obtains IP addresses of domain names from the DNS server to enable communications.



In the following scenarios, a firewall can act as a DNS client and send request packets to the DNS server.

- Perform ping or tracert operations using domain names.
- Access Ruijie Secure Cloud Platform using domain names to upgrade a signature library.

7.7.2 Creating a DNS Server

Configure the IP address of the DNS server on the web UI so that the firewall can act as a DNS client and send domain name resolution requests to the DNS server.

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 **Add DNS** page is displayed.

The screenshot shows the 'Add DNS' configuration page. At the top left, there is a '< Back' button. The page title is 'Add DNS'. Below the title, there is a required input field labeled '* DNS Server Address1' with an empty text box. At the bottom right of the page, there is a blue 'Save' button.

- 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.

7.8 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

Save

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

Item	Description	Remarks
IP Assignment Range	Range of IP addresses allocated by the DHCP server.	<ul style="list-style-type: none"> ● Enter an IP address range per line. ● Connect the start IP address and end IP address with a hyphen (-). [Example] 192.168.1.1-192.168.1.10
Subnet	Subnet where the IP addresses are located.	Enter the subnet address/ mask bits. [Example] 192.168.1.0/24
Default Gateway	Default gateway that provides network access service to the terminals, which obtain IP addresses.	[Example] 255.255.255.0
Primary DNS Server	Preferred DNS server used by the DHCP service.	Click Use System DNS Settings . Then the system automatically fills in the system DNS server. You can also configure a public DNS server. [Example] 192.168.10.1
Secondary DNS Server	Alternative DNS server used by the DHCP service.	[Example] 192.168.30.1
Advanced		
Lease Time	Address lease period. In general, terminal devices automatically renews the lease in connected state to keep the IP address unchanged. If the lease is not renewed due to disconnection or network instability, the IP addresses are reclaimed after the lease expires. When the terminal devices recover connectivity, they will request the addresses again.	<ul style="list-style-type: none"> ● The lease period ranges from 3 minutes to 365 days. ● The default lease period is 1 hour. [Example] 1 hour
Reserved IP Address/Range	Reserved IP addresses in the IP Assignment Range .	[Example] 192.168.1.2

Item	Description	Remarks
Binding Host MAC	<p>Static bindings between the pre-assigned IP addresses specified by IP Assignment Range and the MAC addresses of the clients.</p> <p>When receiving a request for an IP address from a client with a matching MAC address, the DHCP server allocates the pre-assigned IP address that is bound to the MAC address only to this client.</p>	<ul style="list-style-type: none"> ● The value is in the format of IP address/MAC address, where the IP address should be a pre-assigned address in the IP Assignment Range. ● Enter one binding entry per line. <p>[Example]</p> <p>192.168.10.1/d8:9e:f3:3f:d5:64</p>

c Click **Save**.

3. Configuring a DHCPv6 Server

(1) Choose **Network > DHCP > DHCP Server**.

(2) Configure the DHCP server information.

a Click **Create**.

The **Create DHCP Service** page is displayed. Set **IPv6**.

< Back
Create DHCP Service

Protocol Type Ipv4 Ipv6

Basic Info

* Interface Select an interface.

* Primary DNS Server Enter the DNS server address.

Secondary DNS Server

* Lease Time Day Hour Minute

Address Pool

+ Create
Delete

	Type	Prefix	Available Prefix Length	Operation
No Data				

Save

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**.

Address Pool

<input type="checkbox"/>	Type	Prefix	Available Prefix Length	Operation
No Data				

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

Create Address Pool ⊗

* Type Network Address Prefix

* Prefix

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.

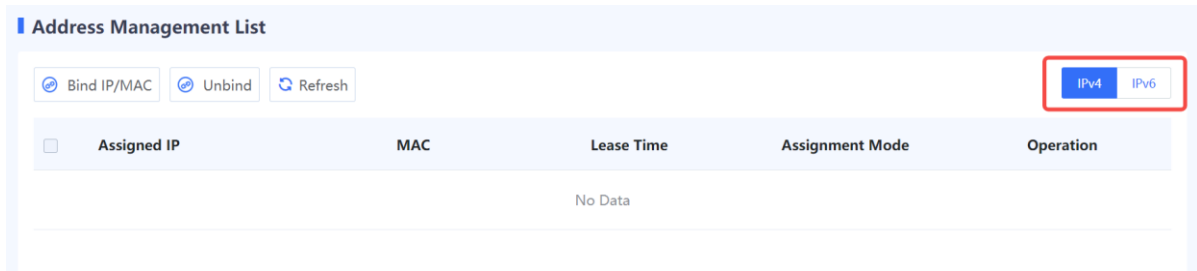
7.8.3 Address Management List

Application Scenario

You can view the IP addresses allocated by the DHCP server on the **Address Management List** page.

Procedure

- (1) Choose **Network > DHCP > Address Management List**.
- (2) Click **IPv4** or **IPv6** in the upper-right corner to view assigned IPv4 or IPv6 addresses.



- (3) 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 Link Detection

7.9.1 Link Detection

Application Scenario

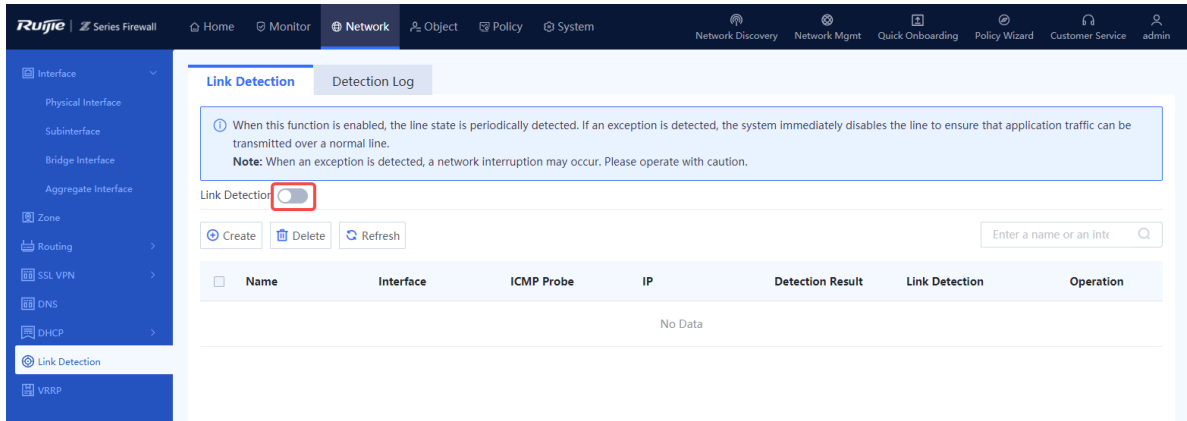
Link detection checks the connectivity of network links. When it is associated with static routing and intelligent routing, automatic route switching can be implemented. If link detection is not associated with intelligent routing or static routing, the static routes and default routes on the interface will not be invalid even if the detection result is abnormal.

Procedure

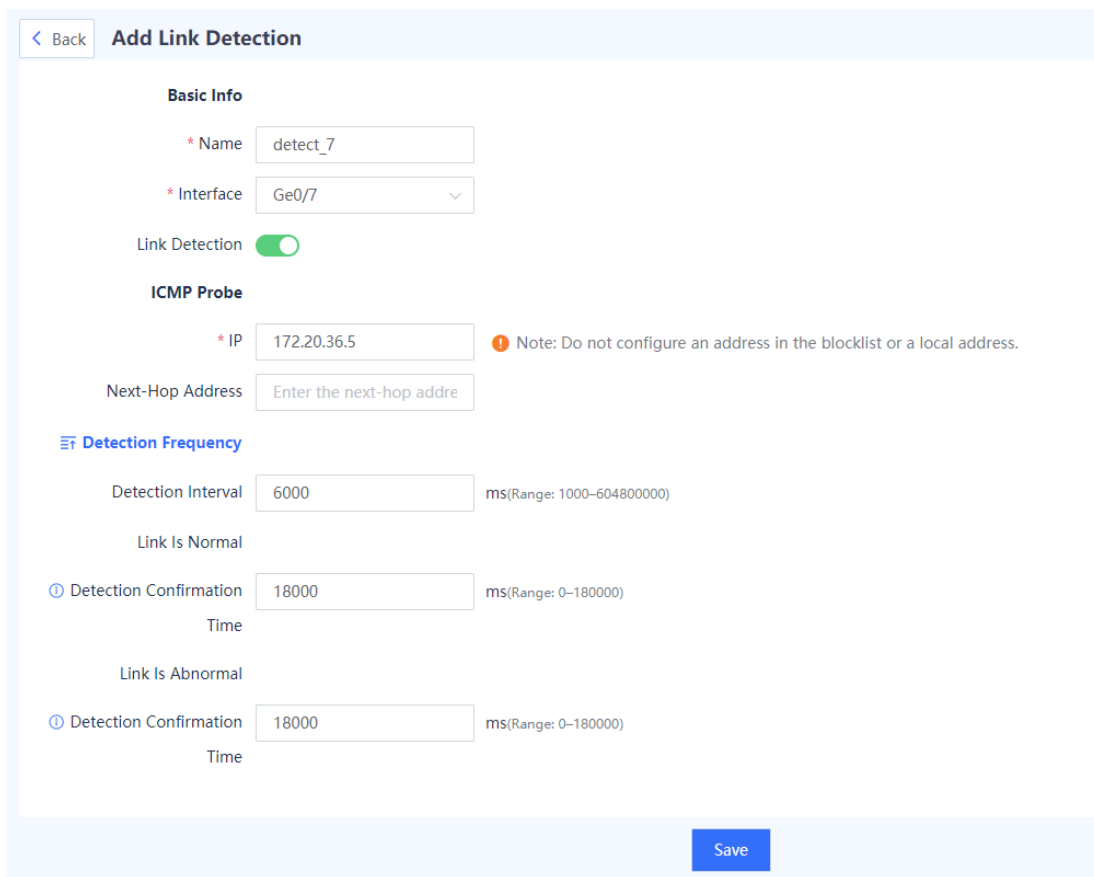
- (1) Choose **Network > Link Detection > Link Detection**.
- (2) Click  to enable link detection.

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.

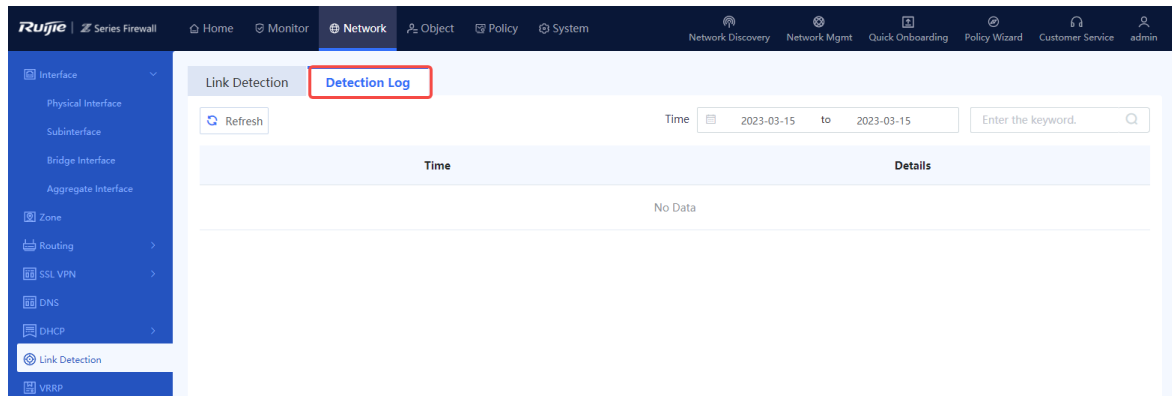


(3) Click **Create** to access the **Add Link Detection** page. Set the detection parameters.



(4) Click **Save**.

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



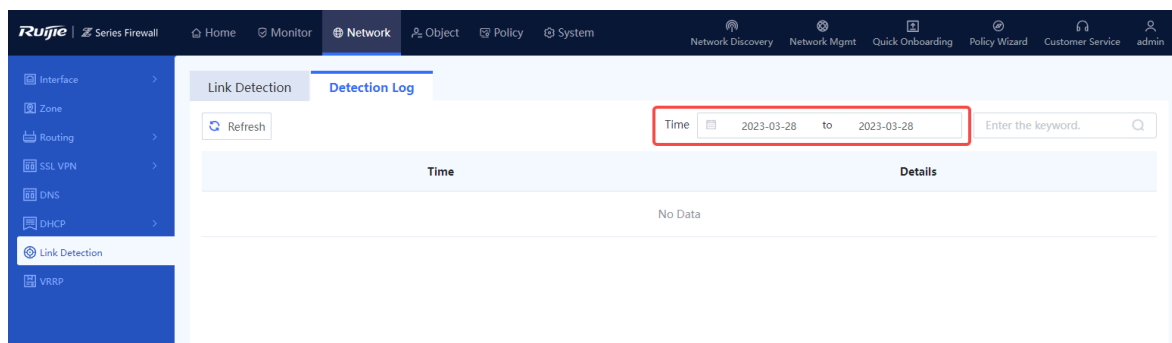
7.9.2 Detection Log

Application Scenario

View historical detection logs on the **Detection Log** tab page.

Procedure

- (1) Choose **Network > Link Detection > Detection Log**.
- (2) Select the query period and view the detection logs generated within the specified period.



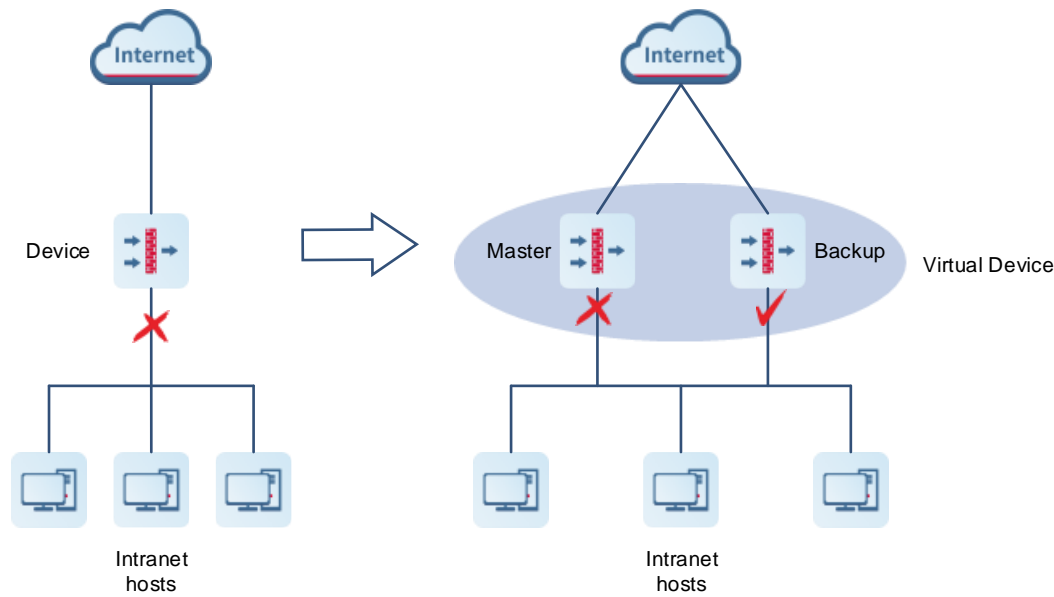
7.10 VRRP

7.10.1 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.

7.10.2 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.

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 finds that its priority is higher than that of the master device, it preempts to become the new master device after the specific period (3 x Advertisement interval + Preemption delay) elapses. (If its priority is the same as that of the master device, the device with a larger primary IP address of the deployment interface is elected as the master device.)

- (4) 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.

7.10.3 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
Basic Info		
VRRP Group Name	Number of the VRRP group. A group of devices with the same VRRP group name forms a virtual device.	[Example] 1
Priority	The priority of the VRRP group. A larger value indicates a higher priority. In a VRRP group, the device with the highest priority is elected as the master device.	[Example] 254
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

Item	Description	Remarks
Virtual IP	IP address of the virtual device, which is different from the IP address of the deployment interface but must be on the same network segment as the deployment interface.	[Example] 192.168.1.1
Monitoring Interface	Interface used to monitor uplink interface status changes of the device. This parameter can only be configured on the master device.	[Example] Ge0/2
Association Priority	When the status of the monitoring interface changes, this parameter determines how the VRRP priority of the local device is modified. If the monitoring interface goes Down, the priority of the device is reduced by the specified value. At this point, another device with the highest priority in the VRRP group can be elected as the new master device.	[Example] 10
Advanced		
Preemption Delay	If the backup device finds that its priority is higher than that of the master device, it advertises its master role after the specific period (3 x Advertisement interval + Preemption delay) elapses. The unit of preemption delay is second.	[Example] 1
Advertisement Interval	Interval in seconds at which the master device sends VRRP messages. All devices within the same VRRP group must be configured with the same advertisement interval.	[Example] 1
Authentication		
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.
- Configure a VRRP group with the same group name on another device on the network. Otherwise, the VRRP group cannot be set up successfully.

7.10.4 Viewing VRRP Logs

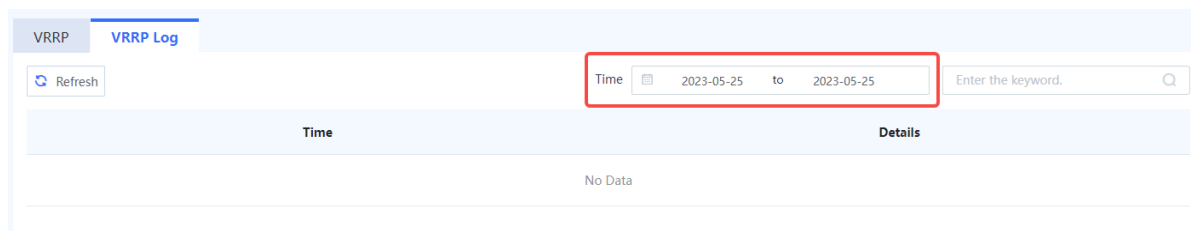
Application Scenario

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.



8 System Management

8.1 Administrators

8.1.1 Overview

The Z-S series firewall devices support administrators in multiple roles to separate permissions and implement independent permission control.

Administrator Permission Control

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 8-1](#).

Table 8-1 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	<ul style="list-style-type: none"> No permission on Admin menus under System Read-write permissions on other menus 	securityadmin
Auditor	<ul style="list-style-type: none"> Read permission on Home menus Read permission on Monitor menus No permissions on other menus 	auditadmin
User Admin	<ul style="list-style-type: none"> Read permission on Home menus Read-write permissions on Admin menus under System No permissions on other menus 	useradmin

8.1.2 Enabling Default Accounts

Application Scenario

The system default administrator accounts **securityadmin**, **auditadmin**, and **useradmin** take effect after you enable and set passwords for them.

Note

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

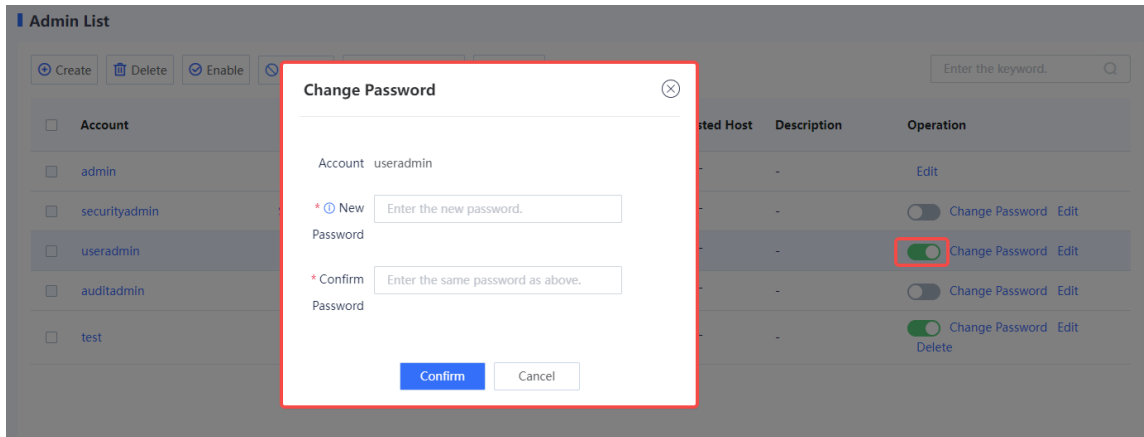
Procedure

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

The system displays the default accounts.

- (2) Select a default account to be enabled and toggle on the switch in the **Operation** column.

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



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

A valid password should meet the following format requirements:

- o A password must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.
- o Chinese characters, spaces, and full-width characters are not allowed.
- o The value is a string of 8 to 15 characters.
- o 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 so that the account can be easily identified.

< Back

Edit Admin Account

Basic Info

* Account

* Enabled State Enable Disable

* Role

Description

Configure Trusted Host

Restrict Trusted Host Login

- The default administrator account cannot be deleted.

8.1.3 Creating an Administrator Account

When management personnel change, you can create an administrator account and assign a role to it, or delete an administrator account that is no longer in use to avoid security risks caused by account leakage.

Table 8-2 Procedure for Creating an Administrator Account

Step	Description
Create an administrator role.	The system can assign operation permissions on different menu items to different roles, and then assign the roles to different accounts to control their permissions. The system has a default administrator role Super Admin . This role has all operation permissions, which cannot be modified.
Create an administrator account.	With the increase of device administrators, you can create more administrator accounts and assign roles for them to obtain corresponding permissions. The system has a default super administrator account admin . This account has all operation permissions and cannot be disabled. The role of this account cannot be modified.

1. (Optional) Creating an Administrator Role

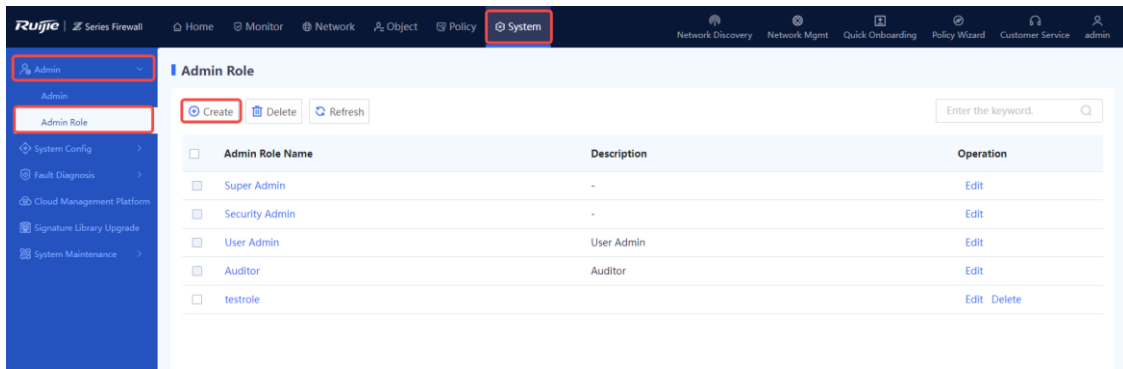
Application Scenario

You can create an administrator role on the web UI to manage menu item operating permissions of administrators.

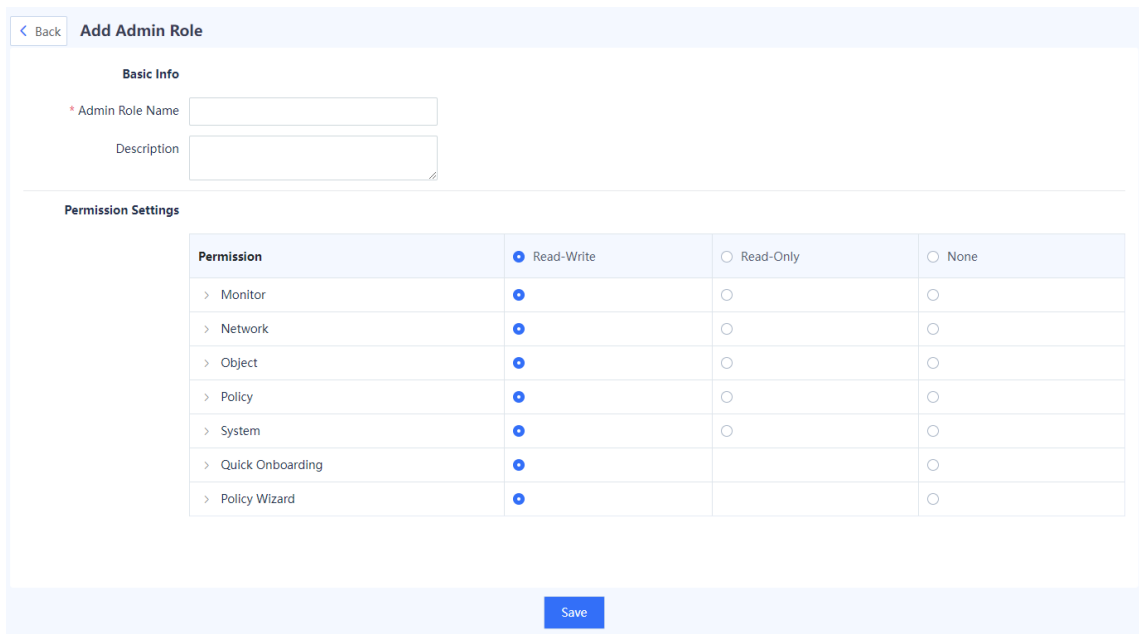
When creating an administrator, you can assign the default role to the administrator. You can also create new roles as required.

Procedure

- (1) Access the **Add Admin Role** page.
 - a Choose **System > Admin Role**.
 - b In the operation area, click **Create**.



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



Item	Description	Remarks
Admin Role Name	Name of the new administrator role.	[Example] Admin Role 1
Description	Description of the new administrator role.	[Example] New
Permission Settings		
Permission	Web UI functions that can be operated by the new administrator role.	[Example] Monitor
Permission Type	Permission types of the new administrator role, including: <ul style="list-style-type: none"> ● Read-Write: View, add, delete, and edit permissions ● Read-Only: View permission only ● None: No permission 	[Example] Read-Write

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

Follow-up Procedure

The created administrator roles are displayed in the administrator role list. You can edit or delete these administrator roles.

- **Edit:** If the permissions of a role need to be changed, **admin** can edit the role description and permissions.
- **Delete:** If a role is not required, **admin** can delete roles that are not associated with an administrator account. If a role to be deleted is associated with an administrator account, **admin** can click **Edit** to change the role associated with the administrator account.

Note

The default administrator roles **Super Admin**, **Security Admin**, **Auditor**, and **User Admin** cannot be deleted.

2. Creating an Administrator Account

Application Scenario

With the increase of device administrators, you can create more administrator accounts and assign corresponding permissions.

A new administrator can access the web platform using the account and password to configure and manage devices.

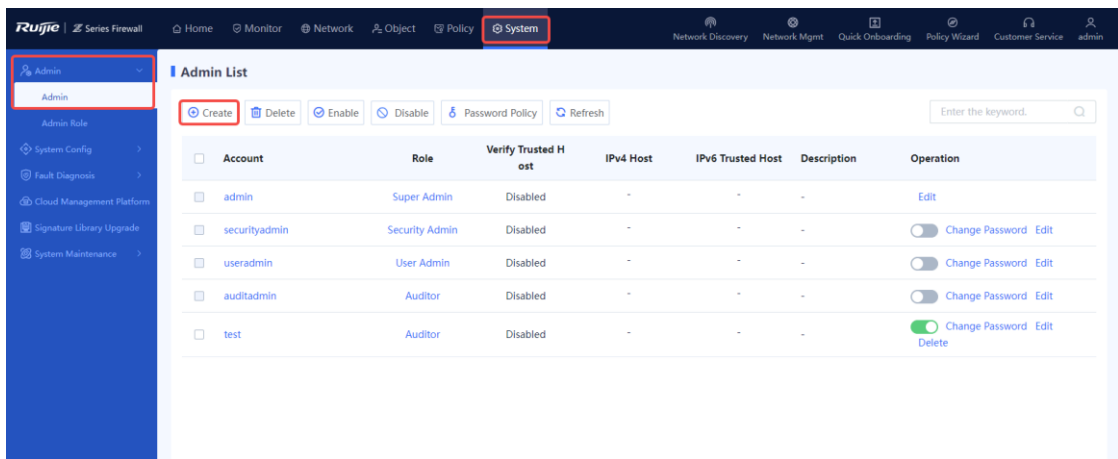
Both the super administrator and user administrator have the permission to create an administrator account.

Procedure

(1) Access the **Add Admin Account** page.

- a Choose **System > Admin**.

b In the operation area, click **Create**.



(2) Set parameters for the new administrator.

[Back](#) **Add Admin Account**

Basic Info

* Account

* Enabled State Enable Disable

* Role ▼

Description

Advanced

* Password

* Confirm Password

Configure Trusted Host

Restrict Trusted Host Login

IPv4 Trusted Host 1 [Delete](#)

IPv6 Trusted Host 1 [Delete](#)

Item	Description	Remarks
Basic Info		
Account	Username of the created administrator.	<ul style="list-style-type: none"> The username can contain letters, digits, and underscores (_), and must start with a letter. The value cannot be the same as an existing administrator username. [Example] Admin_security
Enabled State	Whether to enable the new administrator account.	[Example] Enable
Role	Role of the new administrator, which specifies the operation permissions of the administrator.	[Example] Security Admin
Description	Description of the new administrator.	Characters such as `~!#%^&*+ ;:'"/<>? are not allowed. [Example] With the security monitor permission
Advanced		
Password	Password used by the new administrator to log in to the web UI.	<ul style="list-style-type: none"> A password must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Chinese characters, spaces, and full-width characters are not allowed. The password is a string of 8 to 15 characters. The password cannot be the same as the username or the username in reverse order. [Example] admin@123
Confirm Password	Enter the login password again.	The value of Confirm Password must be the same as that of Password . [Example] admin@123
Configure Trusted Host		
Restrict Trusted Host Login	If this function is enabled, the account can only log in to the firewall using a specified IP address (trusted host).	[Example] Enable
IPv4 Trusted Host 1	Enter the IPv4 address of a trusted host.	[Example] 192.168.1.1

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

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

Follow-up Procedure

The created administrator accounts are displayed in the administrator list. You can edit, disable, or delete these administrator accounts.

Note

The username of a created administrator account cannot be modified, but other parameters such as description and password can be modified.

8.1.4 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 In 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

Submit

Cancel

- (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.

8.1.5 Modifying the Administrator Password

Application Scenario

You can modify the login password of an administrator account when the password is weak or at risk of password leakage.

- The **admin** account can be used to modify the login passwords of other administrators.
- The **useradmin** account can be used to modify the login passwords of other administrators except for the **admin** account.

Procedure

- (1) Access the **Change Password** page.
 - a Choose **System > Admin**.
 - b Select the administrator whose password needs to be changed and click **Change Password** in the **Operation** column.

Admin List

Create Delete Enable Disable Password Policy Refresh Q

Account	Role	Verify Trusted Host	IPv4 Host	IPv6 Trusted Host	Description	Operation
<input type="checkbox"/> admin	Super Admin	Disabled	-	-	-	Edit
<input type="checkbox"/> securityadmin	Security Admin	Disabled	-	-	-	<input type="checkbox"/> Change Password Edit
<input type="checkbox"/> useradmin	User Admin	Disabled	-	-	-	<input type="checkbox"/> Change Password Edit
<input type="checkbox"/> auditadmin	Auditor	Disabled	-	-	-	<input type="checkbox"/> Change Password Edit
<input type="checkbox"/> test	Auditor	Disabled	-	-	-	<input checked="" type="checkbox"/> Change Password Edit Delete

(2) Set a new password for the administrator.

Change Password ⊗

Account securityadmin

* New
Password

* Confirm
Password

- A valid password should meet the following format requirements:
 - A password must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.
 - Chinese characters, spaces, and full-width characters are not allowed.
 - The value is a string of 8 to 15 characters.
 - Cannot be the same as the username or the username in reverse order.

(3) Click **Confirm**.

8.2 System Configuration

You can modify the system time and service parameters, as well as import licenses in system configuration.

8.2.1 Setting System Time

Application Scenario

The system time is the current time of the device and is a key parameter during device running. Administrators can accurately track the occurrence time of system events by checking the time information in device logs or alarms. In addition, when multiple devices in a network collaborate, accurate system time ensures the precision and consistency of their collaborative work, and facilitates management.

Background

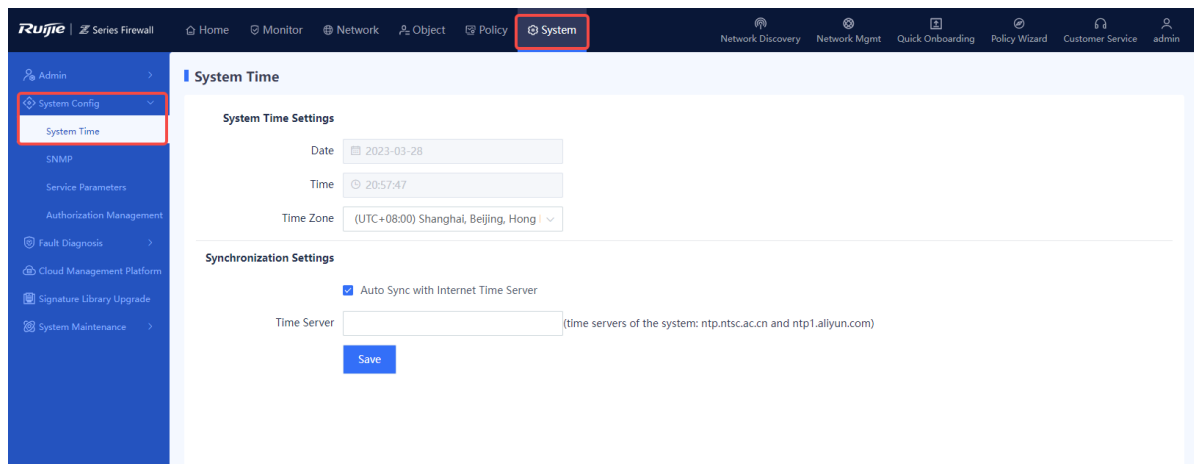
The system time setting consists of manual setting and automatic synchronization:

- Manual time synchronization: Administrators need to manually set the date, time, and time zone. This method may have some time deviation.
- Automatic time synchronization: The system can automatically synchronize its time using the Network Time Protocol (NTP) time servers. NTP is an application layer protocol used for clock synchronization on the Internet. It facilitates time synchronization between distributed time servers and clients. A local system running NTP can both receive synchronization information from other time sources and act as a time source to synchronize other clocks. This is achieved through the exchange of NTP packets.

Procedure

(1) Access the **System Time** page.

Choose **System > System Config > System Time**.



(2) Select different setting methods as required.

- Manual time synchronization

In the **System Time Settings** area, set the date, time, and time zone.

System Time Settings

* Date	<input type="text" value="2023-03-28"/>
* Time	<input type="text" value="20:57:47"/>
* Time Zone	<input type="text" value="(UTC+08:00) Shanghai, Beijing, Hong Kong"/>

- Automatic time synchronization

In the **Synchronization Settings** area, check **Auto Sync with Internet Time Server** and enter the IP address or domain name of the time server.

 Note

If a time server is set for synchronization, you need to make sure that the DNS service is normal.

Synchronization Settings

Auto Sync with Internet Time Server

Time Server (time servers of the system: ntp.ntsc.ac.cn and ntp1.aliyun.com)

(3) Click **Save**.

After you complete the configuration of automatic time synchronization, the system synchronizes the time within a few minutes.

8.2.2 Configuring SNMP

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

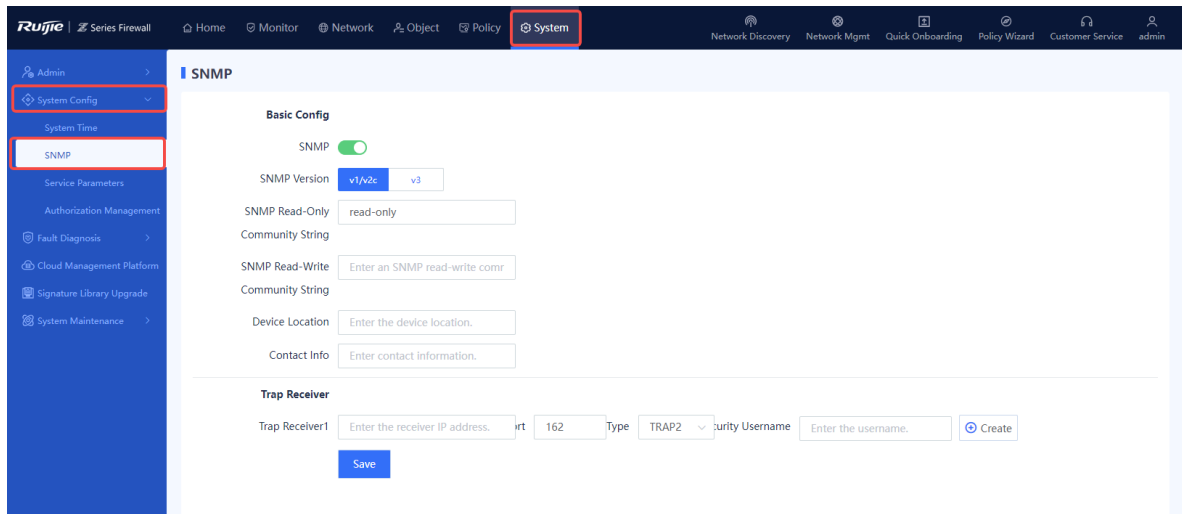
SNMPv3 defines extended security capabilities and provides the following security features through data identification and encryption:

- 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.

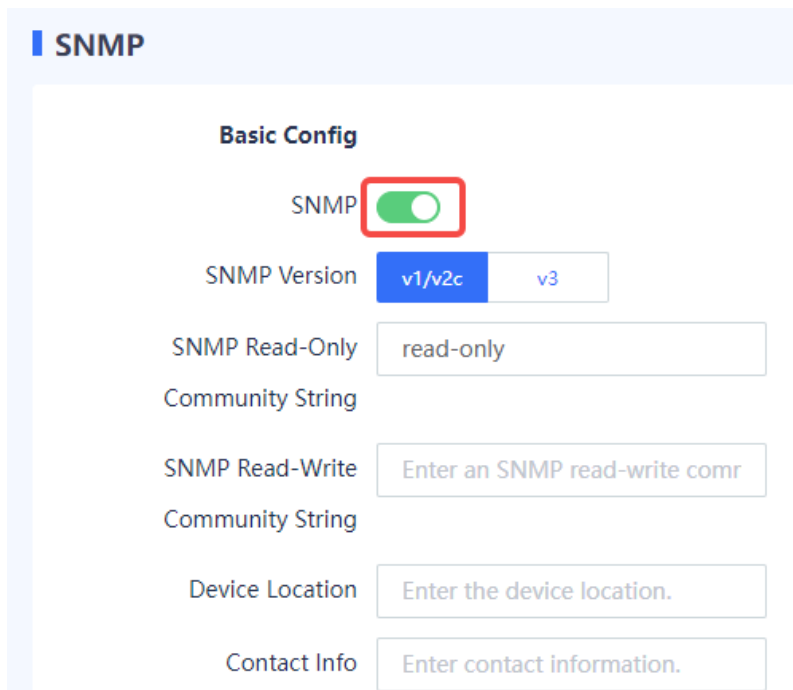
2. Procedure

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

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



(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 v1/v2c and v3 .	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 String	Community name used for authentication between the managed device and NMS server. If the NMS user uses a read-write community name for authentication, the user possesses the read-write permission on device configuration.	The value must be the same as the read-write community name on the NMS. Otherwise, access from the NMS to the device may fail. Characters such as `~!#%^&*+ \{};:'"/<>?` and spaces are not allowed. [Example] private
SNMP version: v3		
Security Username	Username used by the NMS user to access the managed device.	The value must be the same as that on the NMS. Characters such as `~!#%^&*+ \{};:'"/<>?` and spaces are not allowed. [Example] user1
Authentication Algorithm	Authentication algorithm used to verify the user identity. MD5 and SHA algorithms are supported.	The value must be the same as that on the NMS. [Example] MD5

Item	Description	Remarks
Authentication Key	Password used to verify whether the NMS user is valid.	The value must be the same as the authentication password configured on the NMS. [Example] authkey
Encryption Algorithm	Encryption algorithm used to encrypt the transmitted data. AES and DES algorithms are supported.	The value must be the same as that on the NMS. [Example] AES
Encryption Key	Password used to encrypt the transmitted data.	The value must be the same as the encryption password configured on the NMS. [Example] prikey
Device Location	Physical location of the managed device. This information allows the administrator to quickly locate a faulty device.	N/A
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.	N/A
Trap Receiver Click Create to add a trap receiver.		
Trap Receiver	Destination host address that receives the Trap message.	[Example] 1.1.1.2
Port	Number of the port used by the managed device to send a Trap message to the destination host. The default value is 162 .	[Example] 162
Type	Trap type. The options are TRAP , TRAP2 , and INFORM .	The type is TRAP2 in most cases. [Example] TRAP2

Item	Description	Remarks
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**.

8.2.3 Configuring Service Parameters

1. Modifying the Web Login Configuration

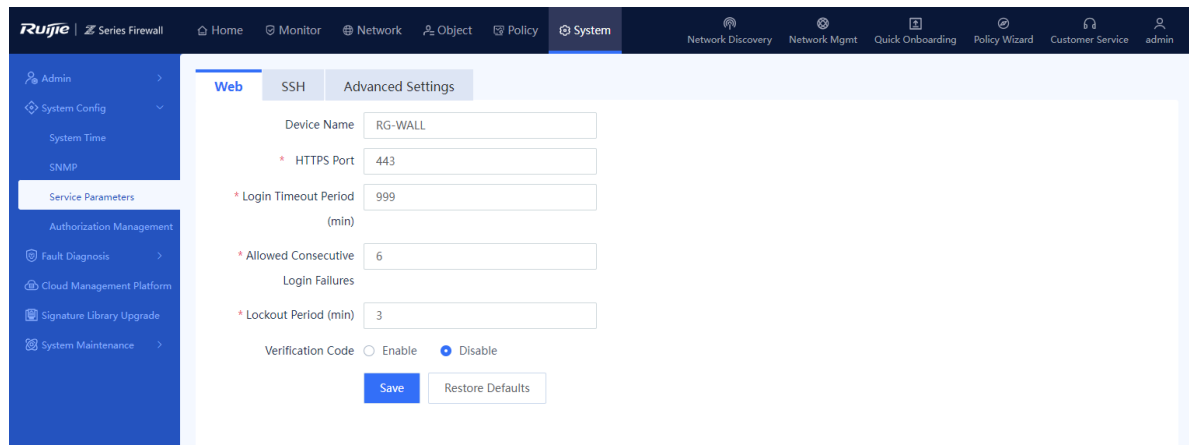
Application Scenario

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. This configuration can improve the login security and reduce the data leakage risks caused by password leakage.

Procedure

(1) Access the **Web** tab page to configure parameters.

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



(2) Customize the web service configuration.

Item	Description	Remarks
Device Name	Name of the device. In integrated deployment on Ruijie Cloud, you can view the modified device name on Ruijie Cloud and the master device. For details about integrated deployment on Ruijie Cloud, see 4 Integrated Deployment on Ruijie Cloud .	[Example] Z3200-S

Item	Description	Remarks
HTTPS Port	Port number used by the web service.	The default value is 443 . [Example] 443
Login Timeout Period (min)	Period of time within which if no operation is performed after login to the web UI. The system displays a prompt of login timeout when the administrator tries to log in to the web UI again.	<ul style="list-style-type: none"> ● Enter an integer in the range of 0 to 1440, in minutes. ● The default value is 30 minutes. [Example] 30
Allowed Consecutive Login Failures	Number of consecutive incorrect password attempts. If a user enters an incorrect password for a number of times exceeding the value specified by this parameter, the system automatically locks the user.	<ul style="list-style-type: none"> ● Enter an integer in the range of 1 to 10. ● The default value is 6. [Example] 3
Lockout Period (min)	Period of time within which the automatically locked user is not allowed to log in to the web UI.	<ul style="list-style-type: none"> ● Enter an integer in the range of 1 to 30, in minutes. ● The default value is 3 minutes. [Example] 30
Verification Code	Whether a verification code is required for login to the web UI.	By default, the value is Enable . [Example] Enable

(3) Click **Save**.

2. Modifying SSH Service Configuration

Application Scenario

You can modify the SSH service configuration to ensure secure device login using SSH.

Procedure

(1) Access the **SSH** tab page to configure service parameters.

Choose **System > System Config > Service Parameters** and click the **SSH** tab.

Web
SSH
Advanced Settings

* SSH Status

* SSH Port

* Allowed Consecutive Login Failures

* Lockout Period (min)

(2) Set parameters of the SSH service.

Item	Description	Remarks
SSH State	Whether to enable the SSH service. When the SSH service is disabled, users cannot access the firewall through SSH.	By default, the value is Enable .
SSH Port	Port number used by the SSH service. To enhance security and prevent potential attacks targeting the default port (port 22) to collect server information, you are advised to modify the SSH port.	The default value is 22 . [Example] 20
Allowed Consecutive Login Failures	Number of consecutive incorrect password attempts when accessing the firewall using SSH. If a user enters an incorrect password for a number of times exceeding the value specified by this parameter, the system automatically locks the user.	Enter an integer ranging from 1 to 5. The default value is 3 . [Example] 3
Lockout Period (min)	Period of time within which the automatically locked user is not allowed to log in to the web UI.	Enter an integer in the range of 1 to 30, in minutes. The default value is 1 minute. [Example] 1

(3) Click **Save**.

3. Configuring Other Parameters

Application Scenario

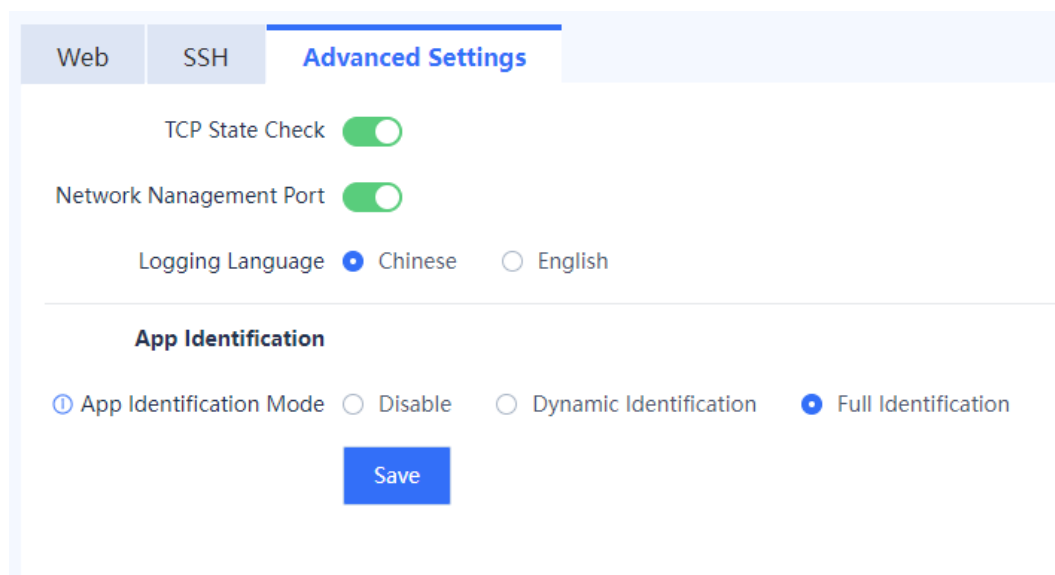
A firewall can perform validity checks on the link status of packets using the state check function. When TCP state check is enabled, the firewall checks whether a TCP packet is the first packet before processing it. The device can establish a session entry only after the first packet passes the check and subsequent packets are forwarded based on the session entry.

The state check function is suitable for network environments where the forward and reverse paths of packets are consistent. However, in cases where the forward and reverse paths are inconsistent, the device may only receive subsequent packets of the communication process without receiving the first packet. In such scenarios, you need to disable the state check function to ensure normal service running. Administrators can enable or disable the state check function for the TCP protocol based on specific requirements.

Procedure

(1) Access the **Advanced Settings** tab page to configure the TCP state check function.

Choose **System > System Config > Service Parameters** and click the **Advanced Settings** tab.



(2) Toggle on or off **TCP State Check** to enable or disable the TCP state check function.

(3) Toggle on or off **Network Management Port** to enable or disable the network management port function.

The network management port switch controls the enabling state of ports 43561, 43562, and 20099. By default, the network management port function is enabled on the device. If you disable this function, the firewall cannot be discovered and managed in integrated deployment on Ruijie Cloud. For details about integrated deployment on Ruijie Cloud, see [4 Integrated Deployment on Ruijie Cloud](#).

(4) Select the logging language, which supports both Chinese and English.

(5) Select an application identification mode:

- No identification: The application identification function is disabled on all traffic.
- Dynamic identification: The device identifies traffic only when specific services require the application identification results.
- Full identification: The device performs application identification on all traffic.

(6) Click **Save**.

8.3 Activating the License

Application Scenario

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

- Online activation: requires the device to be connected to the Internet.
- Manual activation: does not require an Internet connection. A license file (in .zip or .lic format) needs to be uploaded for activation.

 **Caution**

The TI function supports online activation only.

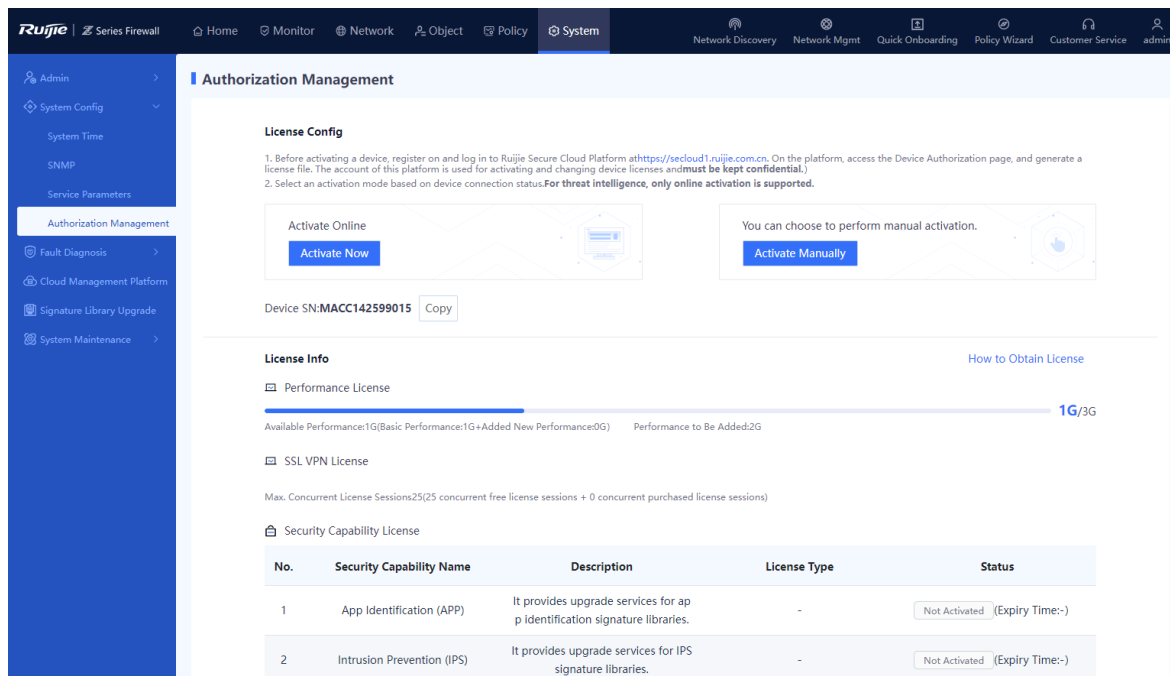
Prerequisites

You have performed the following operations: Log in to the Ruijie Secure Cloud Platform (<https://secloud-en.ruijienetworks.com/>), and choose **Device Authorization** from the main menu. On the page that is displayed, click **Activate License**, and generate a license file.

Procedure

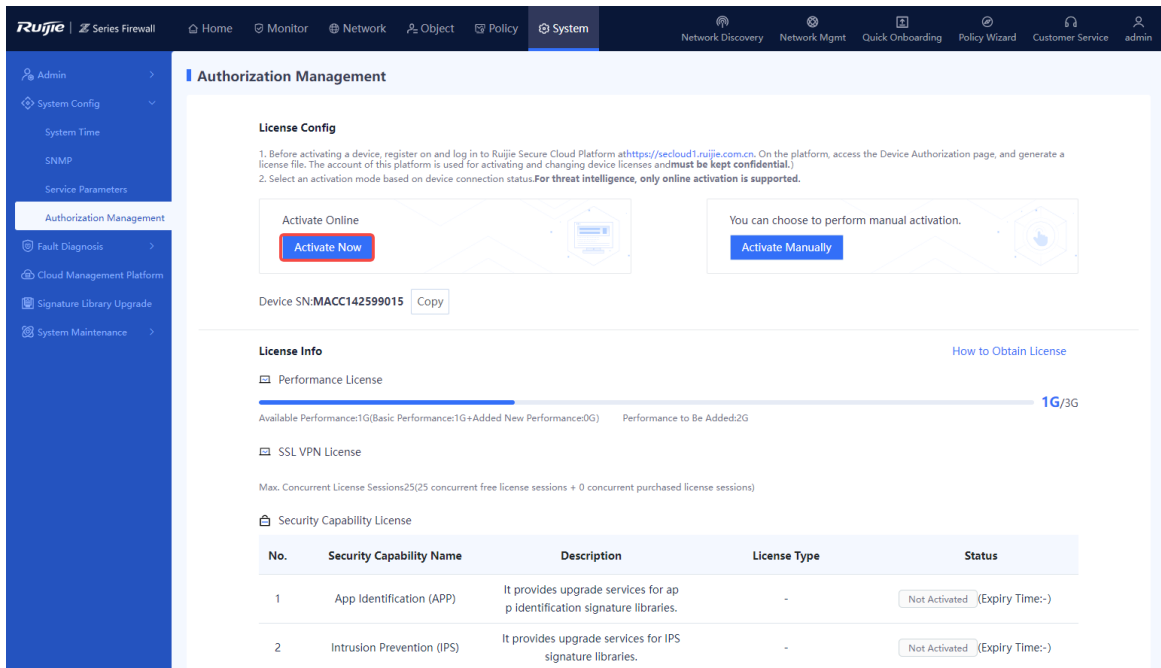
(1) Access the **Authorization Management** page.

Choose **System > System Config > Authorization Management**.



(2) Select an activation mode.

- To perform online activation, click **Active Now**.



- To perform manual activation, click **Activate Manually**, upload the license file (in .zip or .lic format), and click **Activate**.

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:MACC142599015

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

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

Figure 8-1 Successful License Activation

Activation Info ⊗

No.	License File	Status	Cause
 <p>Activation failed.</p> <p>Activation information is unavailable. Log in to Ruijie Secure Cloud Platform at https://secloud1.ruijie.com.cn On the platform, access the Device Authorization page, and click Activate License to active the device license.</p>			

8.4 Fault Diagnosis

When a device fails to communicate with a specific IP address or domain name, or device hardware or software fails, the fault diagnosis function allows administrators to troubleshoot the issues and help R&D engineers locate the faults.

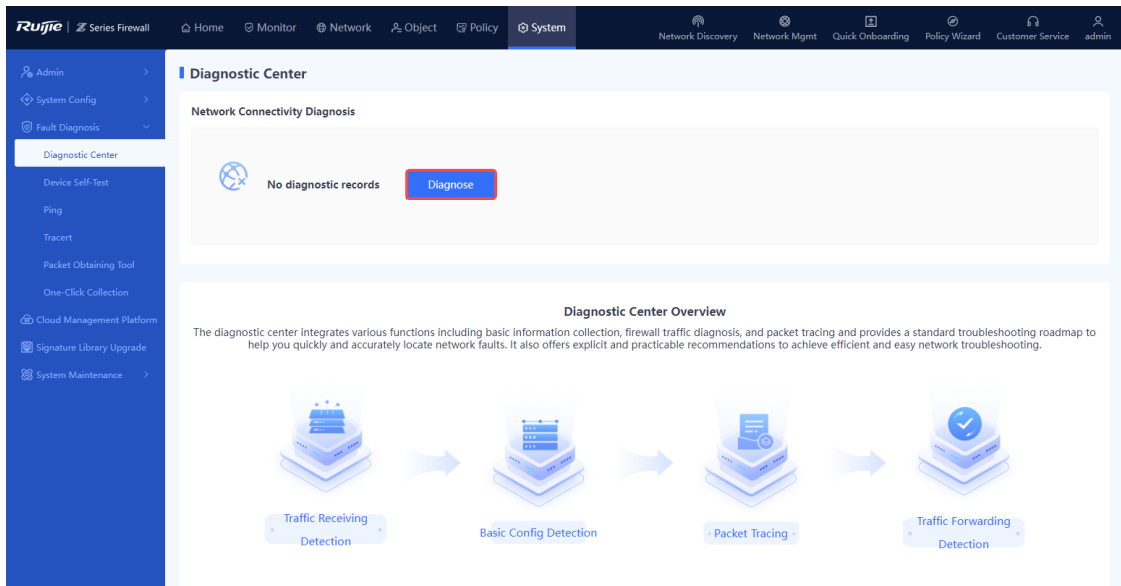
8.4.1 Diagnostic Center

Application Scenario

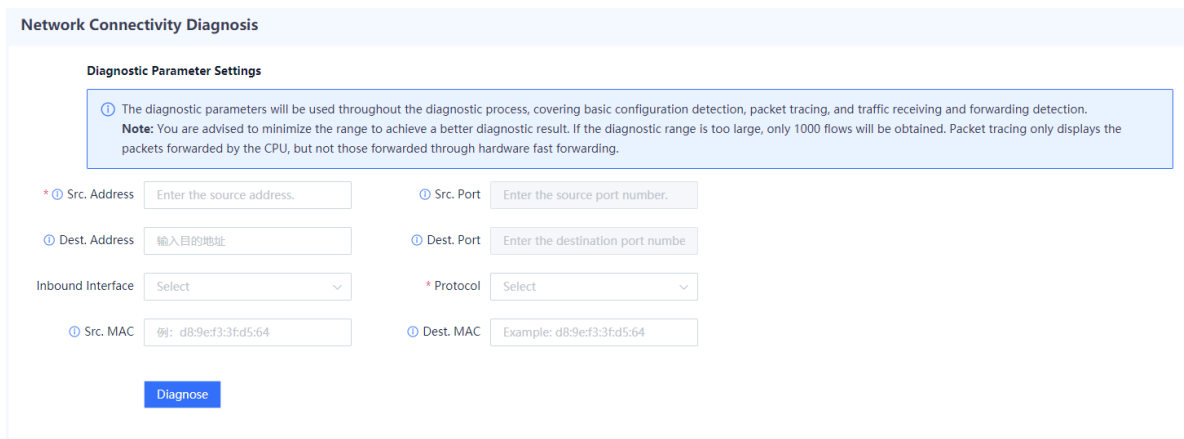
The diagnostic center integrates various functions including traffic receiving detection, basic configuration (security policy and NAT policy) detection, packet tracing, and traffic forwarding detection and provides a standard troubleshooting roadmap to help you locate network faults with one click. It also offers explicit and practicable recommendations to achieve efficient and easy network troubleshooting.

Procedure

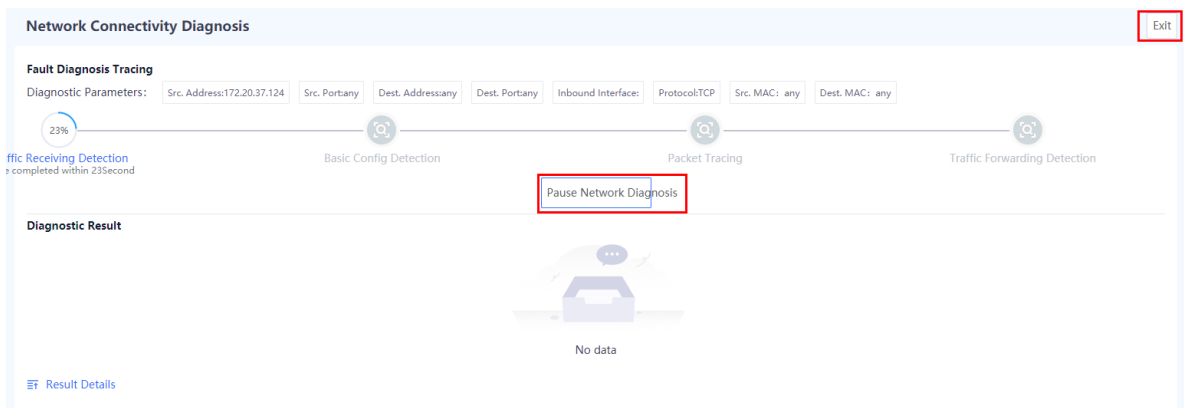
- (1) Choose **System > Fault Diagnosis > Diagnostic Center**.
- (2) Click **Diagnose**.



- (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.



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



- (5) After the diagnosis is complete, the diagnostic result and diagnostic details are displayed in the lower part of the page. After you troubleshoot the fault based on the diagnostic details, click **I have handled the problem**.

Network Connectivity Diagnosis Exit

Fault Diagnosis Tracing

Diagnostic Parameters: Src. Address:192.168.1.44 Src. Port:any Dest. Address:114.114.114.114 Dest. Port:any Inbound Interface:Ge0/0 Protocol:ip Src. MAC: any Dest. MAC: any

Traffic Receiving Detection ! Basic Config Detection I have handled the problem 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.	Troubleshooting Operation Ignore
interfacemodule: The WAN interface is not added to an untrust zone...	The interface is not added to the corresponding security zone. Check whether a LAN interface is added to the trust zone, and whether a 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. ✔		
The security policy module passes the check. ✔		
The DNS module passes the check. ✔		
The DHCP module passes the check. ✔		

- (6) In the dialog box that is displayed, select **Network connectivity is normal**. The firewall continues to check the next item.

i Note

If the fault is not rectified, click **Continue** and the device starts diagnosis again.

Tip ✕

Check the network status.

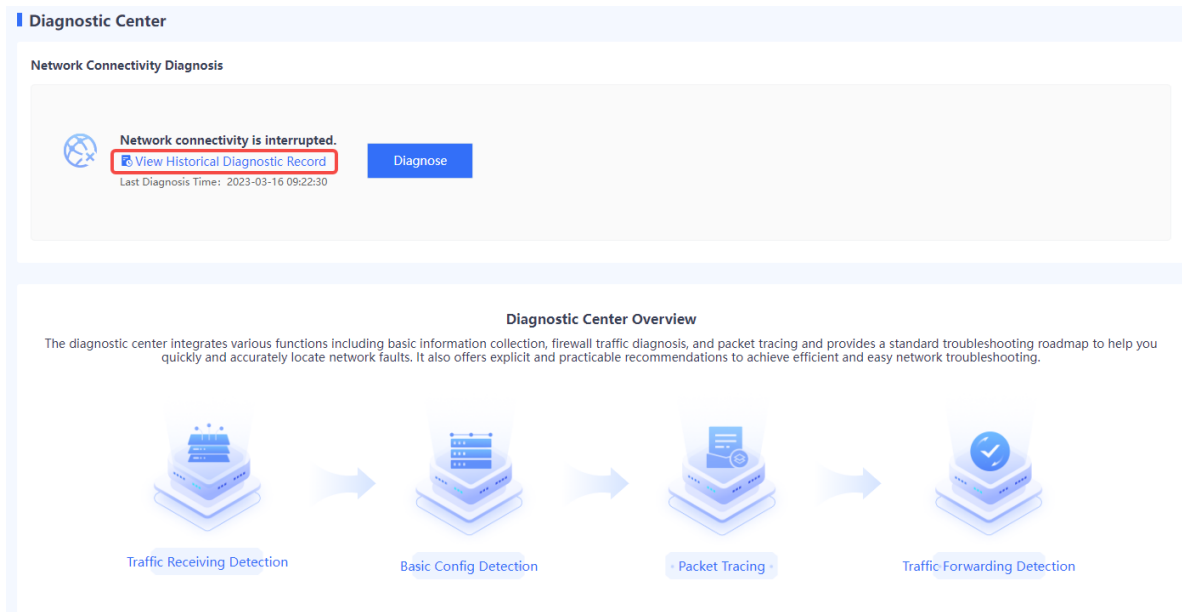
On a client, ping the intranet interface IP address, extranet interface IP address, and destination IP address of the firewall in sequence to determine whether network connectivity is normal.

Network connectivity is normal. The issue is resolved. End the diagnosis. Continue
 Network connectivity is not normal. The issue is not resolved. Continue

- (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.



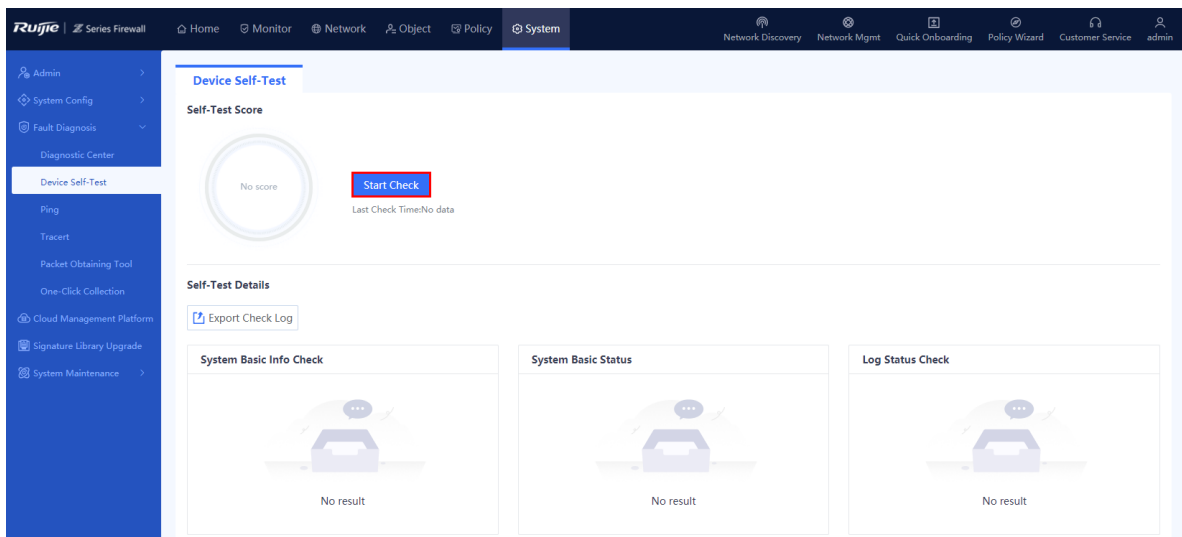
8.4.2 Device Self-Test

Application Scenario

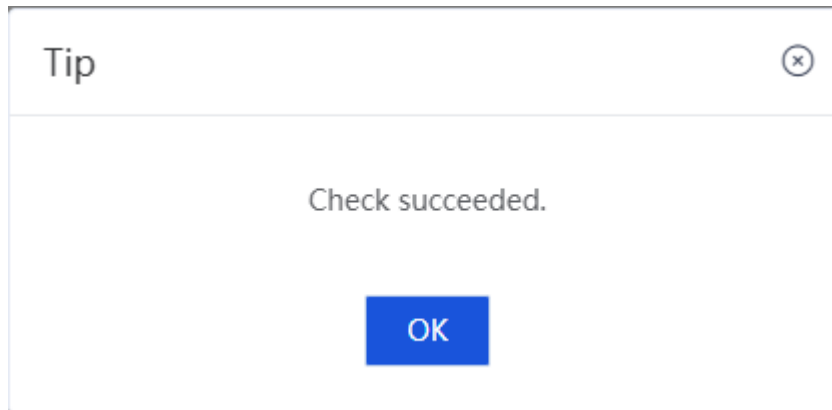
The device self-test function can detect the device version, CPU usage, memory usage, and whether risky configuration exists.

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 message that is displayed, click **OK**.



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

The screenshot displays the 'Device Self-Test' interface. At the top, it shows a 'Self-Test Score' of 83 with a 'Start Check' button and the last check time: 2023-03-14 23:30:13. Below this is the 'Self-Test Details' section, which includes an 'Export Check Log' button and several check panels:

- System Basic Info Check:** Lists device details such as Device Model (Z3200-S), Device Hardware SN (MACC932672666), Device Software SN (M20540903132023), and Device Software Version (NGFW_NTOS 1.0R5). A warning icon indicates that the version is not recommended by the cloud server.
- System Basic Status:** Shows two circular progress indicators: CPU Usage at 35.4% and Memory Usage at 41.5%.
- Log Status Check (-2 points):** Contains two items: 'Whether Hard Disk Is Available: Yes' (green checkmark) and 'Whether Syslog Server Is Set: No syslog server is set. The log storage time requirement may not be met.' (red warning icon). A 'Fix' button is present.
- Management Mode Check (-10 points):** Contains two items: 'SSH Login Failure Limit' (green checkmark) and 'Admin Timeout Period: The login timeout period is long, and security risks exist.' (red warning icon). A 'Fix' button is present.
- Authorization Status Check (-5 points):** Contains one item: 'Threat Intelligence (TI): The license file has expired.' (red warning icon).
- Policy Check:** Contains one item: 'High-risk policy: The interface configuration of the policy is any.' (red warning icon).

8.4.3 Ping

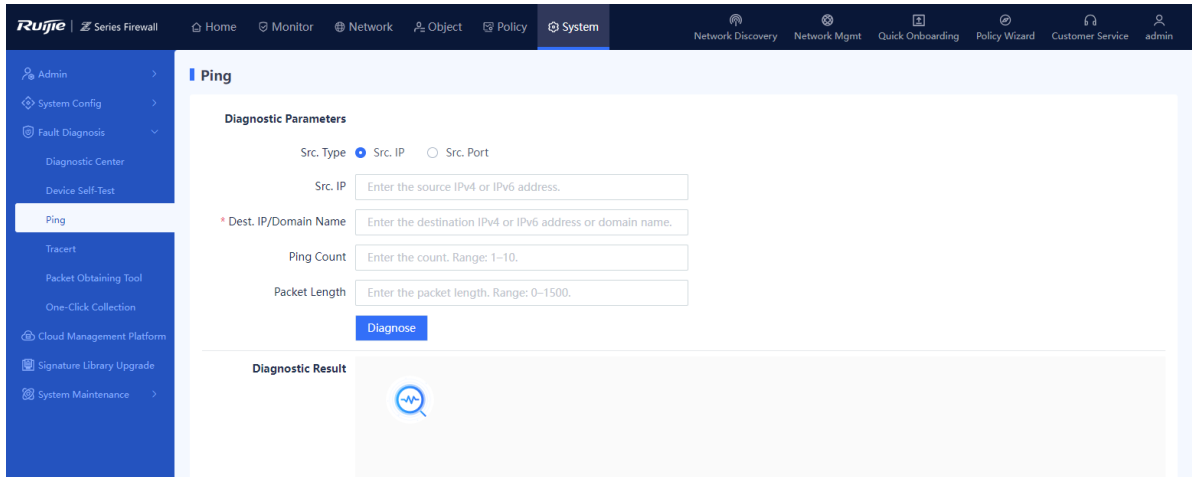
Application Scenario

You can check whether the device can communicate with another device with a specific IP address or domain name using ping.

Procedure

(1) Access the **Ping** page.

Choose **System > Fault Diagnosis > Ping**.

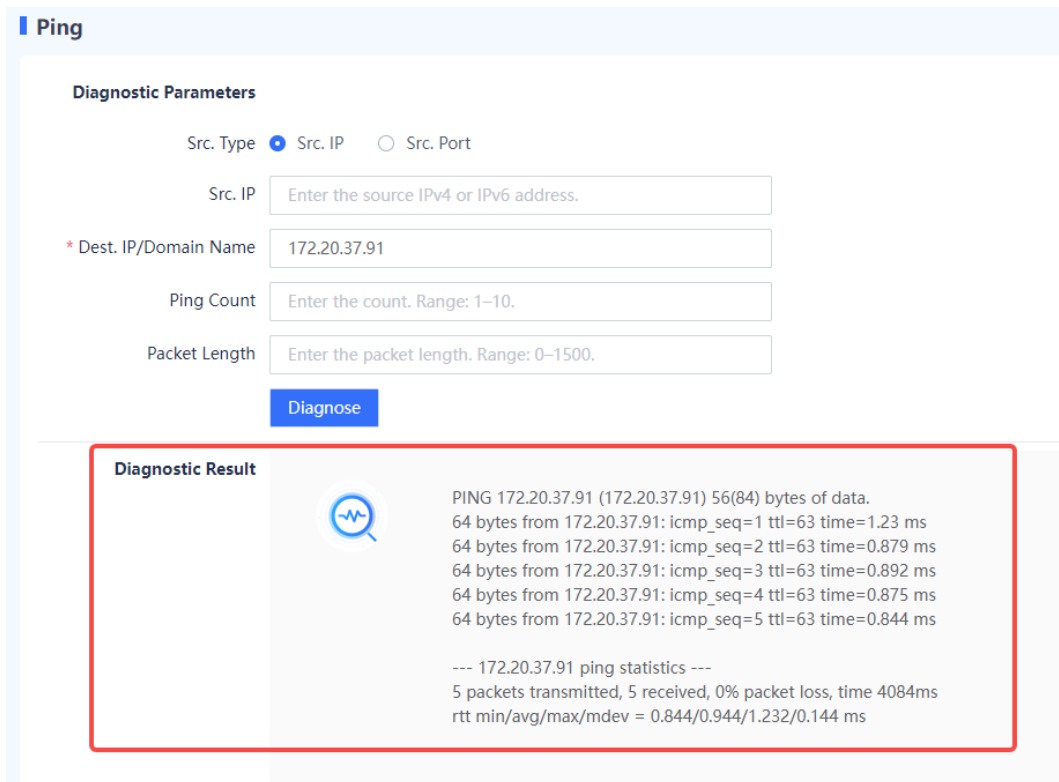


(2) Configure the diagnosis parameters, such as the source IP address, destination IP address, and domain name.

(3) Click **Diagnose**.

Follow-up Procedure

The diagnostic result is displayed in the lower part of the page.



8.4.4 Tracert

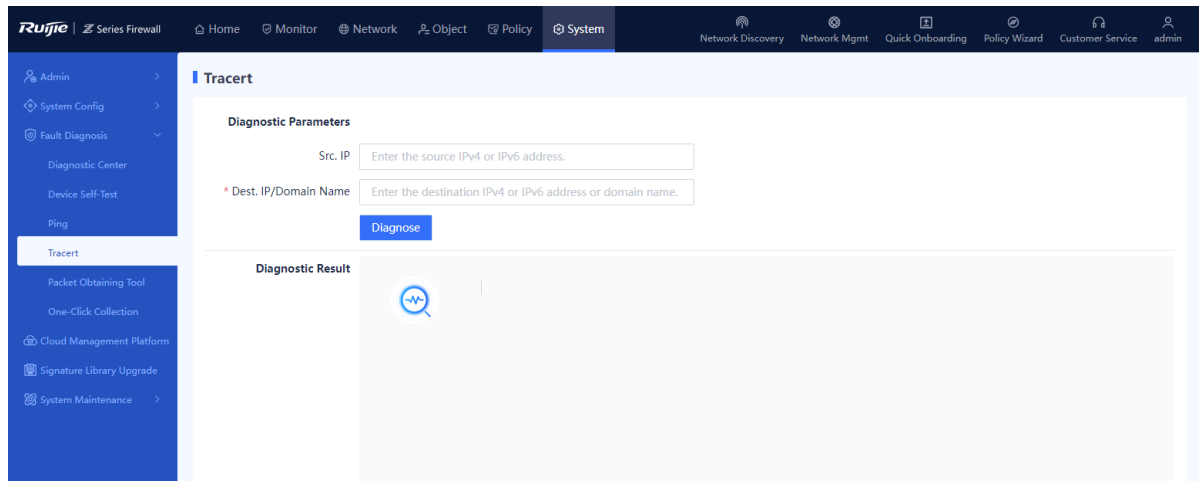
Application Scenario

You can locate a network fault using tracert.

Procedure

- (1) Access the **Tracert** page.

Choose **System > Fault Diagnosis > Tracert**.

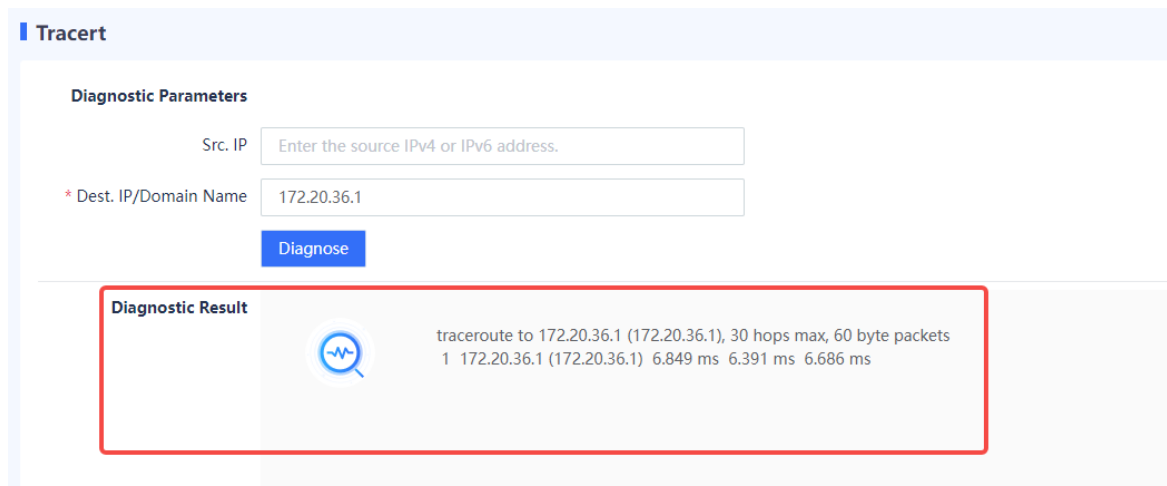


- (2) Configure the diagnosis parameters, such as the source IP address, destination IP address, and domain name.

- (3) Click Diagnose.

Follow-up Procedure

The diagnostic result is displayed in the lower part of the page.



8.4.5 Packet Obtaining Tool

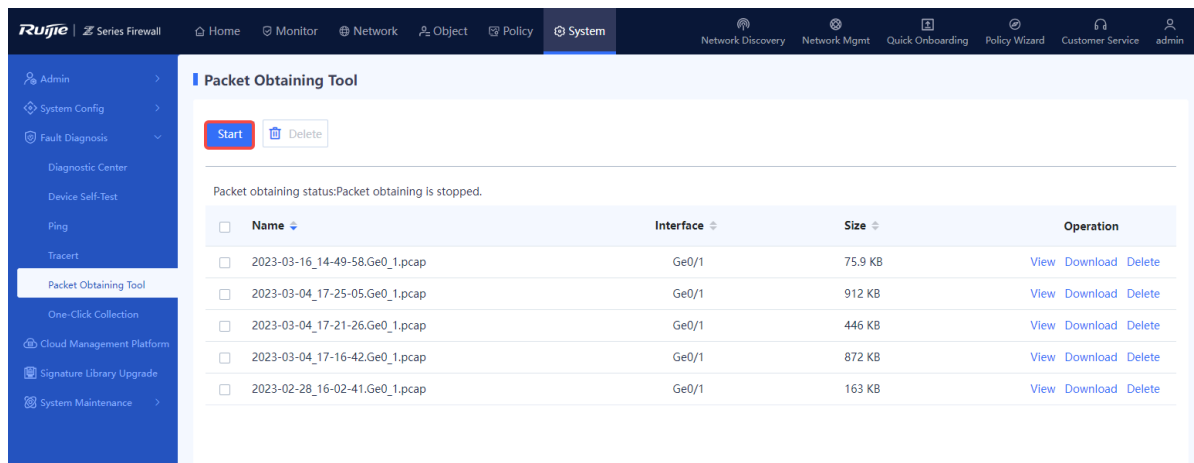
Application Scenario

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) Access the **Packet Obtaining Tool** page.

Choose **System > Fault Diagnosis > Packet Obtaining Tool**.



(2) Click **Start**, select the interface where packets need to be obtained, and then set the packet obtaining rule.

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

i Src. MAC

i Dest. MAC

(3) Click **Start**. The system obtains packets based on the specified protocol type, IP address, port number, and MAC address.

Follow-up Procedure

- After the packet obtaining file is generated, you can click **View** to view and analyze the file online.
- After the packet obtaining file is generated, you can click **Download** to download the file to your PC and use tools to analyze the file.
- If the packet obtaining file is no longer in use, you can click **Delete** as an administrator to release storage

space on the device. Batch deletion is also supported.

8.4.6 One-Click Fault Information Collection

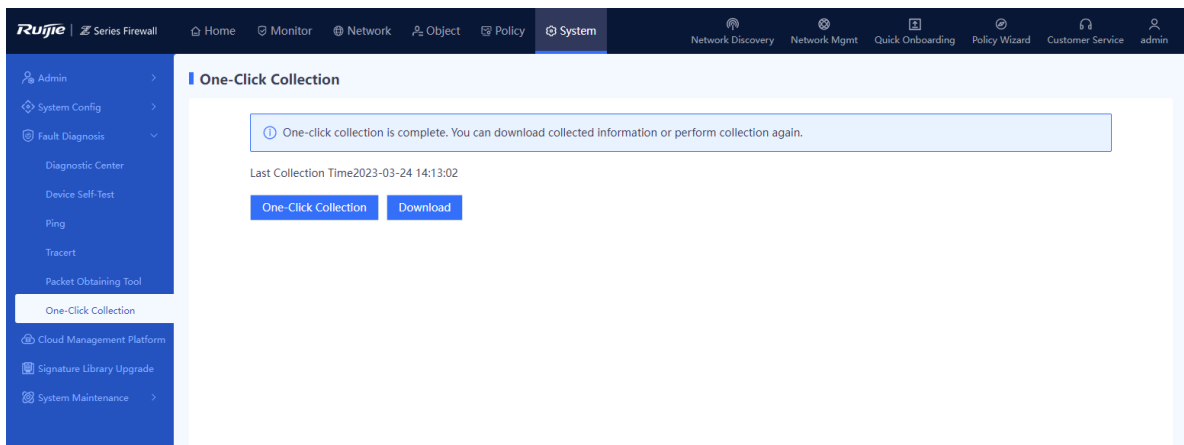
Application Scenario

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**.



- (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.

8.5 Signature Library Upgrade

Application Scenario

By regularly upgrading the signature libraries, the firewall can stay up-to-date with the latest application and threat features, which enables the firewall to protect the network against emerging attacks. 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. Online and local signature library upgrades are both supported.

Prerequisites

- Online signature library upgrades rely on device information, including the software version, device SN, device model, and signature library version. You can obtain the updated signature library version on the cloud platform based on the device information.
- 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 record device SNs.

Procedure

- (1) Access the **Signature Library Upgrade** page.

Choose **System > Signature Library Upgrade**.

Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time: Daily Hour Minute

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

Signature Library Type

(Upgrade all signature libraries online simultaneously)

<div style="border: 1px solid #ccc; padding: 5px;"> <h5>App Identification Signature Library</h5> <p>Current Version: 20230525.1111 Last Upgrade Time:- Latest Version: Unable to obtain the latest version. Version State:- Activation State: Not Activated</p> <p><input type="button" value="Online Upgrade"/> <input type="button" value="Local Upgrade"/> <input type="button" value="Rolling back"/></p> </div>	<div style="border: 1px solid #ccc; padding: 5px;"> <h5>Virus Protection Signature Library (Deep Scan)</h5> <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 Activation State: Not Activated</p> <p><input type="button" value="Online Upgrade"/> <input type="button" value="Local Upgrade"/></p> </div>	<div style="border: 1px solid #ccc; padding: 5px;"> <h5>Virus Protection Signature Library (Quick Scan)</h5> <p>Current Version:- Last Upgrade Time:- Latest Version: Unable to obtain the latest version. Version State:- Activation State: Not Activated</p> <p><input type="button" value="Online Upgrade"/> <input type="button" value="Local Upgrade"/></p> </div>
--	---	--

The system displays information about the current signature libraries:

- (2) **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. Select a proper upgrade method:

- o Scheduled automatic upgrade

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

Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time: Daily Hour Minute

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

- a Set the time for automatic upgrade. You are advised to configure an off-peak period.
 - b Select the type of signature library to be upgraded.
 - c Click **Save**.
- o Local upgrade
 - a In the area of a signature library to be upgraded, click **Local Upgrade**.

Signature Library Type

Upgrade All (Upgrade all signature libraries online simultaneously)

App Identification Signature Library

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

Virus Protection Signature Library (Deep Scan)

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

Intrusion Prevention Signature Library

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

ISP Address Library

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

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

Local Upgrade ⊗

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

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

Import

- c Click **Browse** to import the upgrade file.
- d Click Upgrade Now.
- o Online upgrade

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.

Note

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

8.6 System Maintenance

8.6.1 Checking Device Information

Application Scenario

You can view basic information about the firewall, including the device model and other device information.

Procedure

- (1) Choose **System > System Maintenance > Device Info**.
- (2) View device details.

Device Info		
Device Model RG-WALL 1600-Z3200-S v1.00	Device Time 2023-07-28 11:43:04	MAC EC:B9:70:B6:8D:D9
SN MACC142599015	Version Info V5.2-NGFW_NTOS 1.0R6, Release(03191804)	Running Time Running 1 Week, 3 Day, 1 Hour, 6 Minute
License Expiration 0 items activated View Details		

8.6.2 Managing Configuration Backup

1. Backing Up Configuration Files

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**.

Config Backup

Back Up Config

Restore

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

Mode 2: Restore from a local backup file.

- (2) You can back up configuration files in one of the following ways:

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

Config Backup

Back Up Config

📁 Manually Back Up

📄 Export Current Config

Restore

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

▼
Restore

Mode 2: Restore from a local backup file.

Browse
Restore

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

Config Backup

Back Up Config

📁 Manually Back Up

📄 Export Current Config

Restore

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

▼
Restore

Mode 2: Restore from a local backup file.

Browse
Restore

2. Restoring Configurations

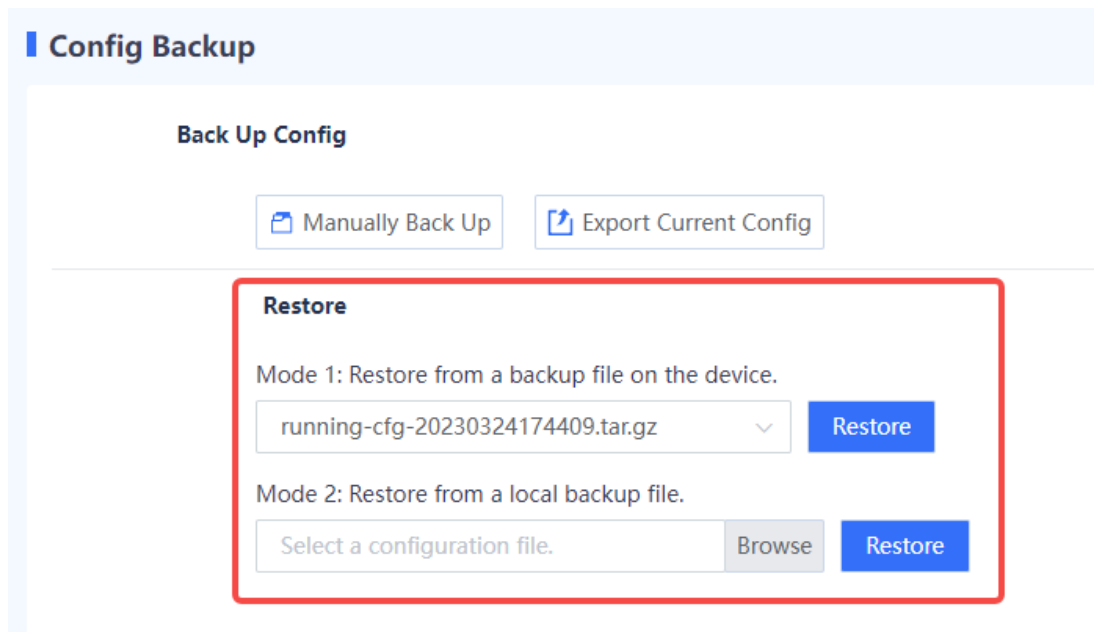
Application Scenario

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.

8.6.3 Upgrading the System

You can upgrade the software of the device to obtain the latest device functions.

The system supports both online and local upgrade modes.

1. Online Upgrade

Application Scenario

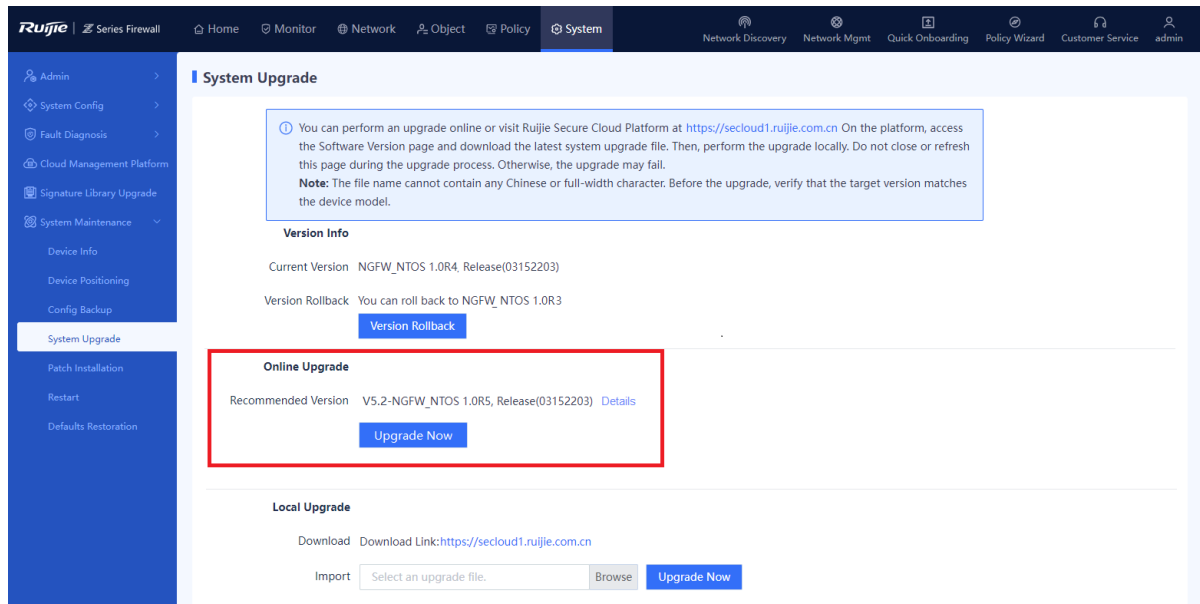
When the network communication between the device and Ruijie Secure Cloud Platform is normal, and the system displays a recommended version, you can upgrade the software version in online mode.

Prerequisites

You have confirmed the upgrade version before upgrading your device.

Procedure

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



- (2) In the Online Upgrade area, click Upgrade Now.
- (3) Read the prompt information and click **Confirm**.

Follow-up Procedure

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

2. Offline Upgrade

Application Scenario

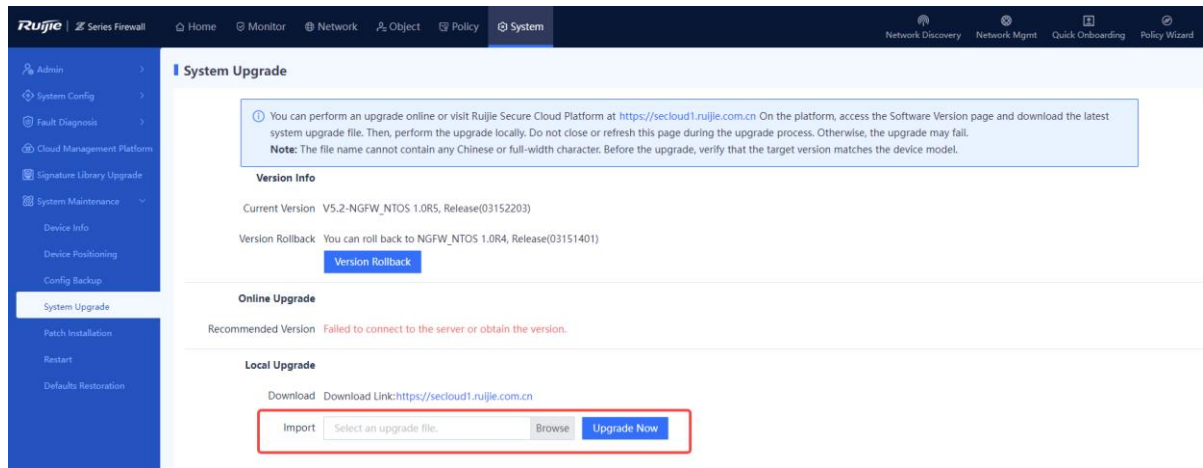
When a network exception occurs between the device and Ruijie Secure Cloud Platform, the system cannot automatically obtain the latest software version. You can upgrade or roll back the software version in offline mode.

Prerequisites

You have obtained the upgrade file in advance. To obtain the upgrade file, log in to the Ruijie Secure Cloud Platform (<https://secloud-en.ruijienetworks.com/>), choose **Version Upgrade** > **Version Info**, and then download the latest file to the local device.

Procedure

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



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

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

(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 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

Version Rollback Dialog:

Version Rollback

Do you want to perform version rollback now?

OK Cancel

8.6.4 Installing Patches

Patches can be installed to fix faults that occur during device running. 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.

Patches can be installed in both online and local modes.

1. Online Upgrade

Application Scenario

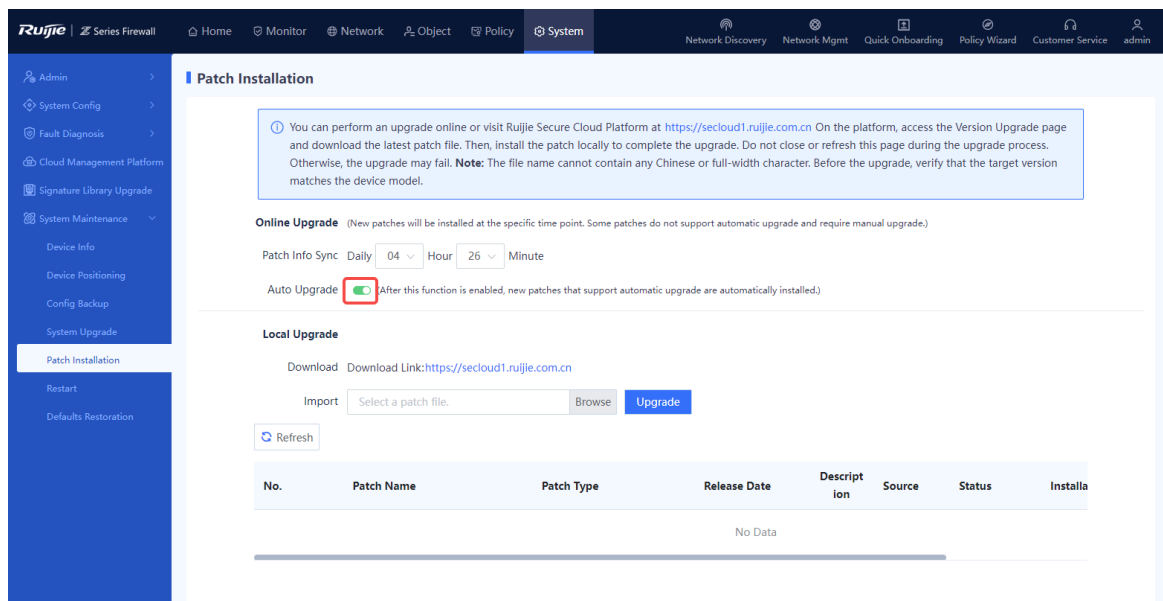
You can perform online upgrade when the device can properly communicate with the Ruijie Secure Cloud Platform.

Prerequisites

You have confirmed the upgrade version before upgrading your device.

Procedure

(1) Choose **System > System Maintenance > Patch Installation**.



(2) In the **Online Upgrade** area, toggle on **Auto Upgrade** and set the patch synchronization time. Then, the device will synchronize and install the patch at the specified time.

(3) After the upgrade is successful, you can view the patch installation history at the bottom of the page.

2. Offline Upgrade

Application Scenario

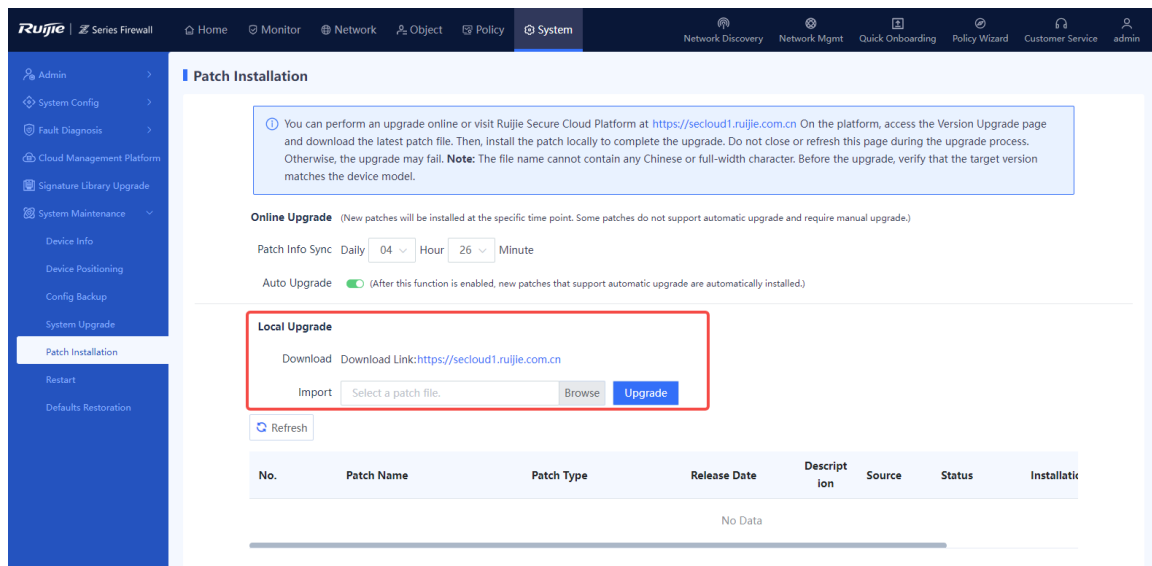
When a network exception occurs between the device and Ruijie Secure Cloud Platform, the system cannot automatically obtain the latest software version. You can install patches in offline mode.

Prerequisites

You have obtained the patch file in advance. To obtain the patch file, log in to the Ruijie Secure Cloud Platform (<https://secloud-en.ruijienetworks.com/>), choose **Version Upgrade > Patch Info**, and then download the latest patch file to the local device.

Procedure

(1) Choose **System > System Maintenance > Patch Installation**.



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

(3) Click **Upgrade** to start system upgrade.

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.

8.6.5 Restarting the Device

Application Scenario

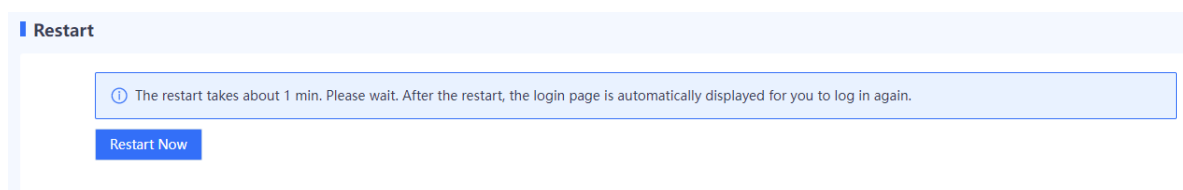
You can restart the device when it fails and cannot be restored.

Prerequisites

- When a firewall is not running properly, troubleshoot the issue first rather than simply restarting the system, which prevents services from being affected.
- However, if you have to restart the system, you are advised to do so during an off-peak period to minimize impact on the services, such as late at night.
- To avoid loss of temporary data due to restart, ensure that you have saved configuration files before restarting.

Procedure

- (1) Choose **System > System Maintenance > Restart**.
- (2) Click **Restart Now**. In the dialog box that is displayed, click **OK** to restart the device immediately.



8.6.6 Restoring to Factory Settings

Application Scenario

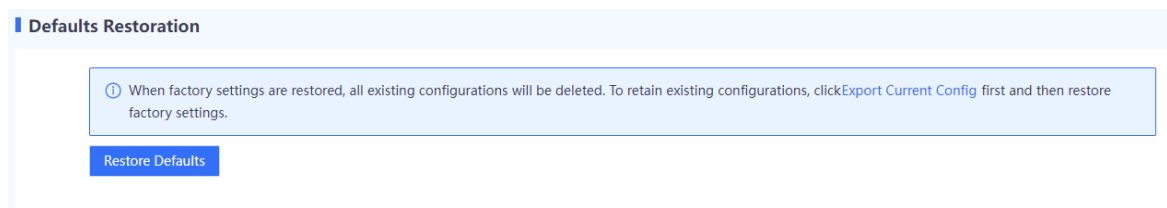
You can perform the defaults restoration operation to delete all configurations from the device or reset the default password for the **admin** account.

 **Caution**

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

Procedure

- (1) Choose **System > System Maintenance > Defaults Restoration**.
- (2) Click **Restore Defaults**.



Follow-up Procedure

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

- The IP address of the management interface is restored to 192.168.1.200.
- The administrator account name and password are restored to **admin/firewall**.

9 Security Monitoring Management

9.1 Security Cockpit

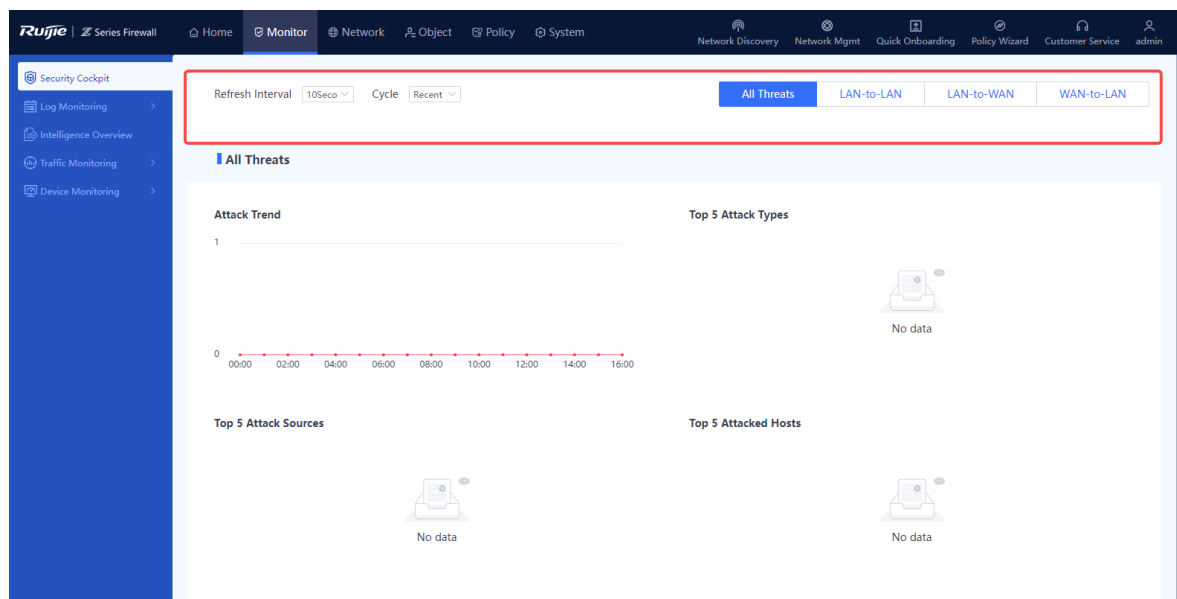
Application Scenario

Security cockpit is the attack statistics collection function of the firewall. It effectively helps administrators identify the most common types of threats, frequent attackers engaged in malicious network activities, and objects that are frequently targeted in attacks. This information allows administrators to take appropriate security measures.

Security cockpit collects data on detected attacks, event types, risk levels, and the actions taken by the system against these attacks. Based on this information, the system generates distribution charts such as attack trends and the top 5 attack types, as well as an attack trend graph.

Procedure

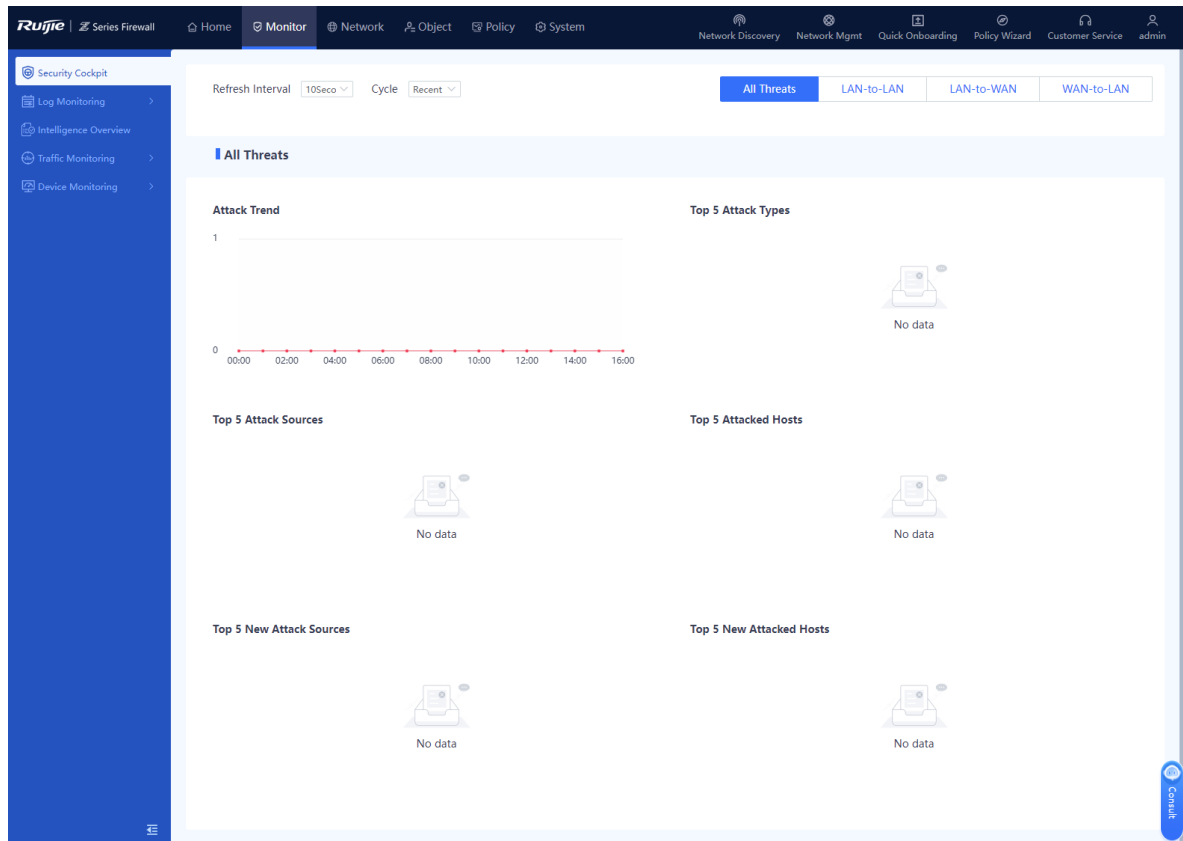
- (1) Choose **Monitor > Security Cockpit**. On the page that is displayed, select **Recent** from the **Cycle** drop-down list.
- (2) Set the refresh interval and display cycle, and select the attack type.



You can select the following attack types:

- All Threats
- LAN-to-LAN
- LAN-to-WAN
- WAN-to-LAN

- (3) The system displays distribution charts of corresponding attacks, including attack trends, top 5 attack types, and top 5 attack sources.



9.2 Log Monitoring Management

9.2.1 Log Overview

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. The device supports the output of various types of logs, including system logs, security logs, operation logs, and session logs. In addition, the Syslog protocol can be used to back up log files to a third-party server.

9.2.2 Querying Logs

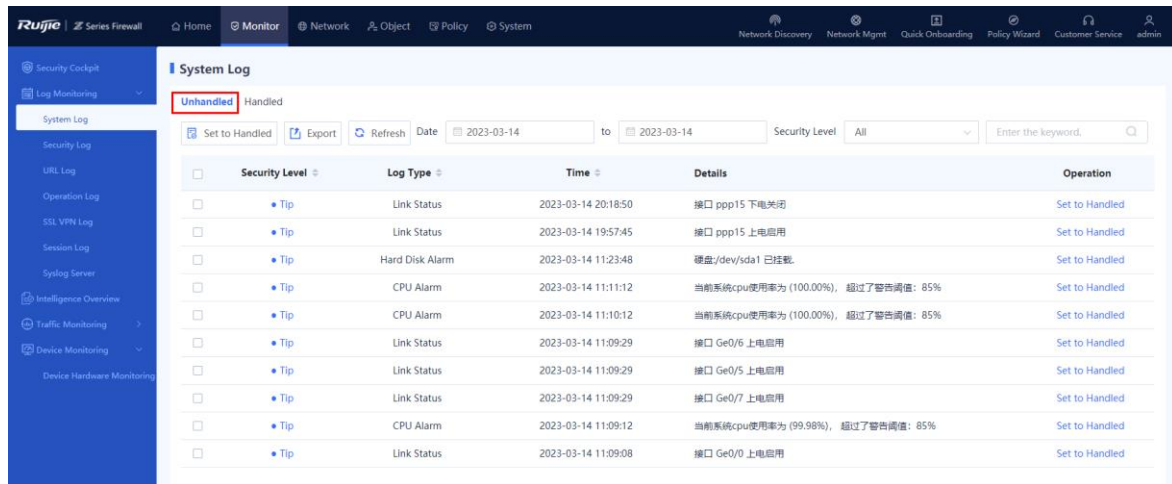
1. Querying System Logs

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.
Log Type	Type of a system log.
Time	Time when a system log is generated.
Details	Detailed information of a system log.
Operation	Click Set to Handled to mark a log as Handled and switch to the Handled tab to view handled logs.

Note

The system supports fuzzy match by the security level, log type, or other keywords. Only system logs matching the search criteria are displayed on the page.

Follow-up Procedure

- Select multiple logs and click **Set to Handled** to modify the status of the selected logs to **Handled** in a batch.
- Click **Export** to export system logs to the local device in the Excel format, facilitating subsequent query.
- Click **Refresh** to obtain the latest system logs.

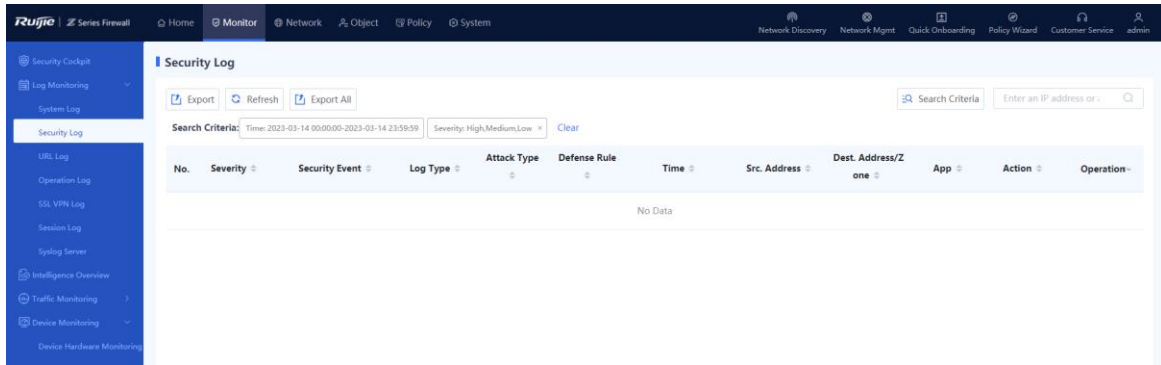
2. Querying Security Logs

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.
Action	Operation result of a security policy on the traffic.
Operation	Click View Details to obtain details about an operation log.

Note

You can click **Search Criteria** to set the keywords for log query. Only 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.

3. Querying URL Logs

Application Scenario

By viewing the logs, administrators can check the hit status of the URL filtering templates.

Precautions

URL logs are stored and displayed only if the device is equipped with a hard disk.

Procedure

- (1) Choose **Monitor > Log Monitoring > URL Log**.
- (2) The URL log-related information is displayed on the web page.



Note

You can click **Search Criteria** to set the keywords for log query. Only URL logs matching the search criteria are displayed on the page.

Follow-up Procedure

- Click **Export** to export URL logs to the local device in the Excel format, facilitating subsequent queries.
- Click **Refresh** to obtain the latest URL logs.

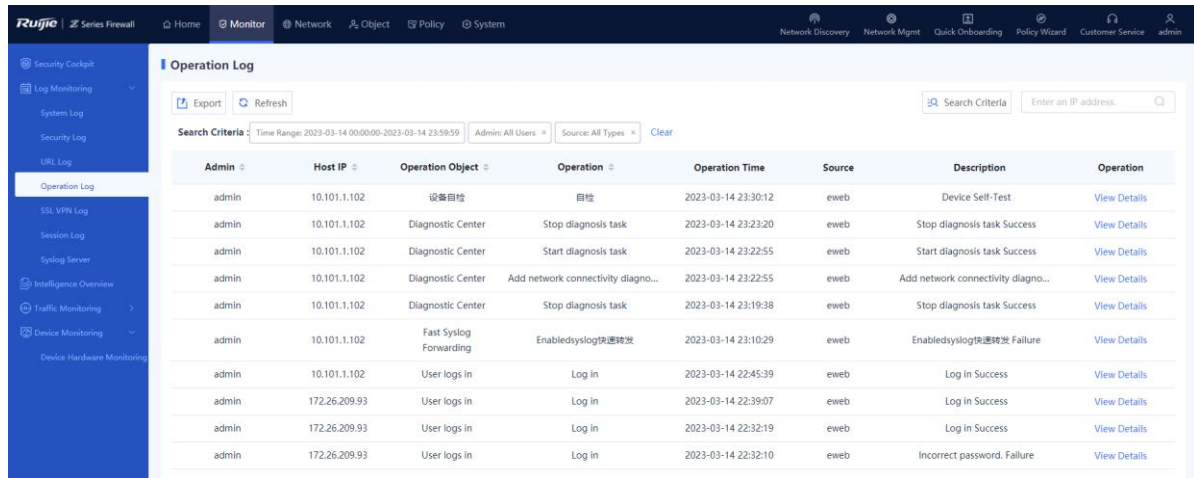
4. Querying Operation Logs

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**.



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

Field	Description
Admin	Name of the administrator who performs the operation.
Host IP	Host IP address used by the administrator to log in to the firewall.
Operation Object	Type of the object managed by the administrator.
Operation	Specific operation performed by the administrator.
Operation Time	Time when the administrator performs the operation.
Description	Description of the operation log.
Operation	Click View Details to obtain details about an operation log.

Note

You can click **Search Criteria** to set the keywords for log query. Only operation logs matching the search criteria are displayed on the page.

Follow-up Procedure

- Click **Export** to export operation logs to the local device in the Excel format, facilitating subsequent query.
- Click **Refresh** to obtain the latest operation logs.

5. Querying SSL VPN Logs

Application Scenario

By viewing the logs, administrators can check details about SSL VPN sessions.

Procedure

- (1) Choose **Monitor > Log Monitoring > SSL VPN Log**.
- (2) The SSL VPN log-related information is displayed on the web page.

Note

You can click **Search Criteria** to set the keywords for log query. Only SSL VPN logs matching the search criteria are displayed on the page.

Follow-up Procedure

- Click **Export** to export logs to the local device in the Excel format, facilitating subsequent queries.
- Click **Refresh** to obtain the latest logs.

6. Querying 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.

IPsec VPN Logs						
Export	Refresh	Custom Field	Date: <input type="text" value="2023-07-28"/>	to: <input type="text" value="2023-07-28"/>	Log Level: <input type="text" value="All"/>	<input type="text" value="Enter the keyword."/>
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: 2c1be916).		
• 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. Querying Session Logs

Application Scenario

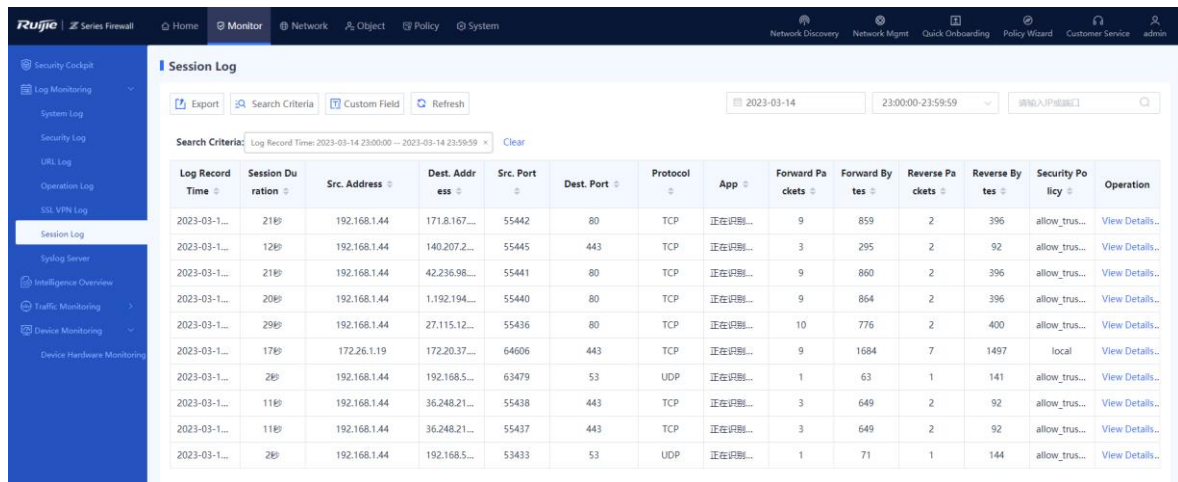
By querying session logs, the administrator can view detailed information of each data flow, including 5-tuple information of the data flow (source IP address, source port, destination IP address, destination port, and protocol) as well as the security policy hit by the data flow and the application carried in the data flow.

Precautions

Session logs are stored and displayed only if the device is equipped with a hard disk.

Procedure

- (1) Choose **Monitor > Log Monitoring > Session Log**.
- (2) The session log-related information is displayed on the web page.



Log Record Time	Session Duration	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Forward Packets	Forward Bytes	Reverse Packets	Reverse Bytes	Security Policy	Operation
2023-03-1...	21秒	192.168.1.44	171.8.167...	55442	80	TCP	正在识别...	9	859	2	396	allow_trus...	View Details...
2023-03-1...	12秒	192.168.1.44	140.207.2...	55445	443	TCP	正在识别...	3	295	2	92	allow_trus...	View Details...
2023-03-1...	21秒	192.168.1.44	42.236.98...	55441	80	TCP	正在识别...	9	860	2	396	allow_trus...	View Details...
2023-03-1...	20秒	192.168.1.44	1.192.194...	55440	80	TCP	正在识别...	9	864	2	396	allow_trus...	View Details...
2023-03-1...	29秒	192.168.1.44	27.115.12...	55436	80	TCP	正在识别...	10	776	2	400	allow_trus...	View Details...
2023-03-1...	17秒	172.26.1.19	172.20.37...	64606	443	TCP	正在识别...	9	1684	7	1497	local	View Details...
2023-03-1...	2秒	192.168.1.44	192.168.5...	63479	53	UDP	正在识别...	1	63	1	141	allow_trus...	View Details...
2023-03-1...	11秒	192.168.1.44	36.248.21...	55438	443	TCP	正在识别...	3	649	2	92	allow_trus...	View Details...
2023-03-1...	11秒	192.168.1.44	36.248.21...	55437	443	TCP	正在识别...	3	649	2	92	allow_trus...	View Details...
2023-03-1...	2秒	192.168.1.44	192.168.5...	53433	53	UDP	正在识别...	1	71	1	144	allow_trus...	View Details...

Note

You can click **Search Criteria** to set the keywords for log query. Only session logs matching the search criteria are displayed on the page.

Follow-up Procedure

- Click **Export** to export session logs to the local device in the Excel format, facilitating subsequent query.
- Click **Custom Field** to set the fields to be displayed on the page.
- Click **Refresh** to obtain the latest session logs.

9.2.3 Configuring the Syslog Server

Application Scenario

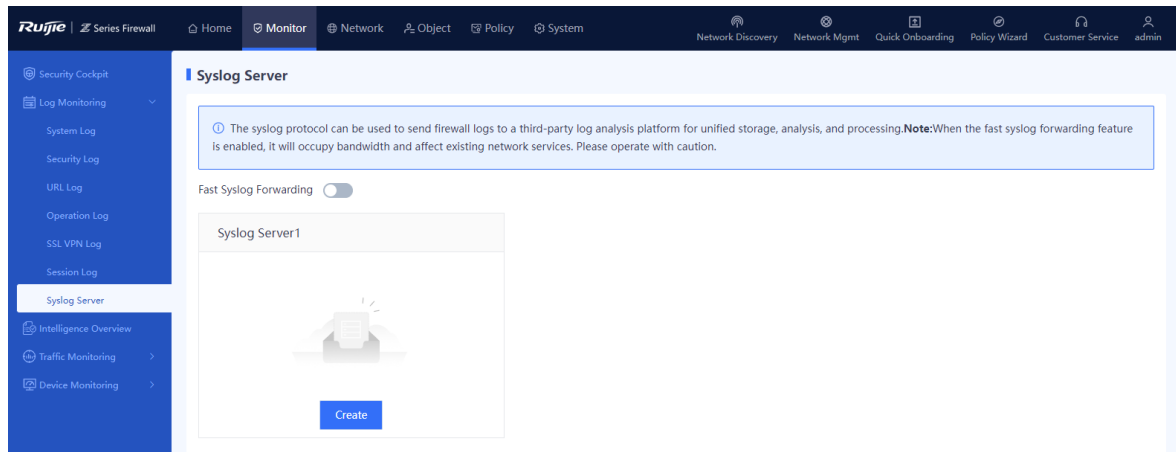
If the firewall is not installed with a hard disk upon factory delivery, logs can only be stored in the memory (for no longer than one day) and all the logs in the memory will be lost after device restart. To ensure that more log information can be obtained, the system logs and security logs of the firewall can be transmitted to a third-party log platform through Syslog for storage and analysis.

Background

The system supports a maximum of three Syslog servers.

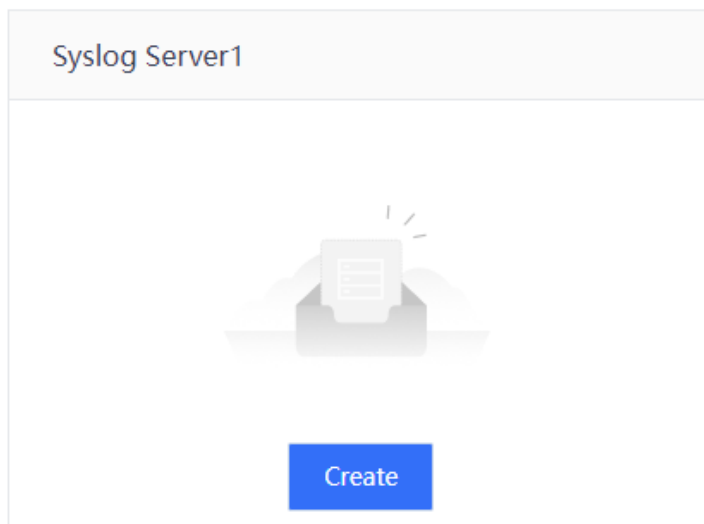
Procedure

- (1) Choose **Monitor > Log Monitoring > SYSLOG Server**.



(2) Configure the Syslog server 1.

- a In the **Syslog Server1** area, click **Create**.



- b Set parameters for the Syslog server 1.

Syslog Server1

* Server IP

* Port

* Standard Protocol Version rfc3164 rfc5424

* Logs to Be Sent to Syslog Server

- Session Log [Edit Template](#)
- Security Log [Edit Template](#)
- URL Log [Edit Template](#)
- System Log [Edit Template](#)
- DHCP Log [Edit Template](#)

Select a syslog log type.


Item	Description	Remarks
Server IP	IP address of the Syslog server.	Set this parameter to the IP address of the Syslog server. [Example] 192.168.10.30
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. [Example] 80
Standard Protocol Version	Protocol used for formatting logs.	Select a protocol version supported by the Syslog server. [Example] RFC5424

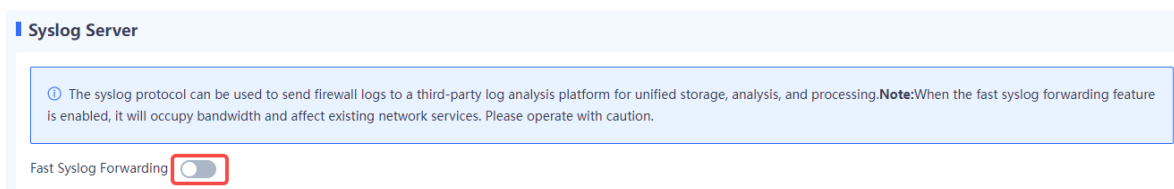
Item	Description	Remarks
Logs to Be Sent to Syslog Server	Types of logs to be sent to the Syslog server.	You can select specific log types that you want to include in the logs forwarded to the server. [Example] System Log

c Click **Save**.

(3) (Optional) If you need to add Syslog server 2, click **Create** in the **Syslog Server2** area.

(4) (Optional) If you need to add Syslog server 3, click **Create** in the **Syslog Server3** area.

(5) (Optional) To forward the Syslog logs in real time, you can toggle on  to enable the fast Syslog forwarding function.



Follow-up Procedure

When the Syslog server is configured, the system sends log information to the specified application server or maintenance terminal.

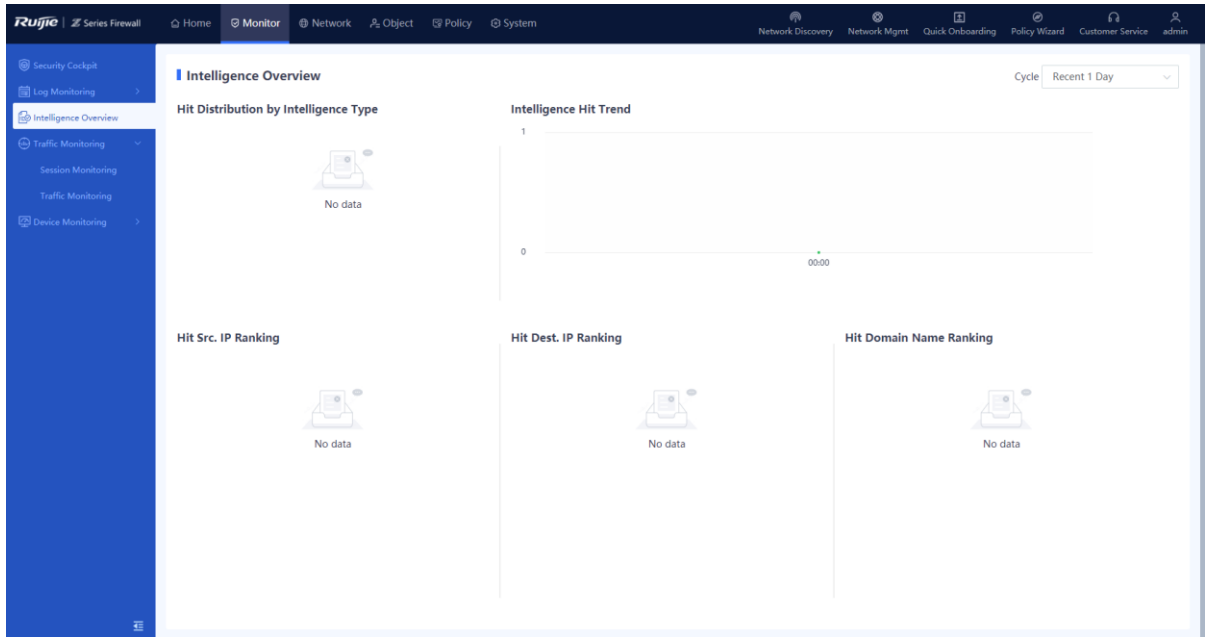
9.3 Intelligence Overview

Application Scenario

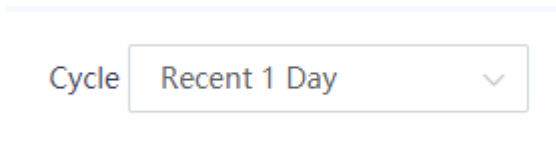
The intelligence overview function is used to display the hit distribution by intelligence type and the intelligence hit trend. This information can help administrators effectively master threats in the current network environment and then develop more refined protection policies to protect LAN hosts.

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 TI 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.

Item	Description
Hit Src. IP Ranking	<p>Displays the ranking of source IP addresses by the number of TI hits. This information helps administrators analyze the threat 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 by the number of TI 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 by the number of TI 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>

9.4 Traffic Monitoring

9.4.1 Interface Traffic

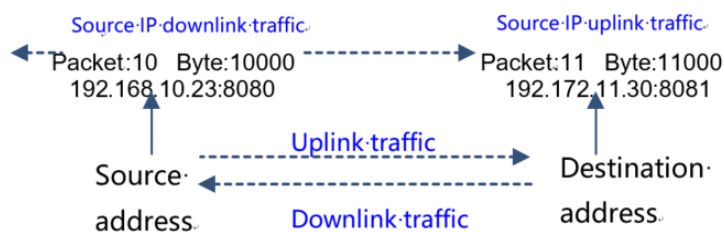
Application Scenario

You can use the interface traffic monitoring function to display the trend of uplink and downlink traffic on a specific interface. This function provides administrators with valuable insights into the current network traffic status, enabling them to take appropriate traffic management measures.

Background

- Uplink traffic: traffic transmitted from the interface.
- Downlink traffic: traffic received by the interface.

The following figure shows the uplink traffic and downlink traffic:



Procedure

- (1) Choose **Monitor > Traffic Monitoring > Traffic Monitoring > Interface Traffic**.

- (2) Click **Interface Traffic Statistics**, select the interface to be queried, and then 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.

The screenshot shows the 'Interface Traffic Statistics' page with the 'Interface Traffic Details' tab selected. The table below lists the details for various interfaces.

Interface	Interface Status	Zone	IP	Uplink	Downlink
Ge0/0	🟢	trust	10.51.212.212/24	9.46Kbps	3.18Kbps
Ge0/1	🟢	zone1	10.10.10.1/24 2000:10:1/64	2.82Mbps	47.89Kbps
Ge0/2	🟢	zone2	20.20.20.1/24 2000:20:1/64	50.44Kbps	2.79Mbps
Ge0/3	🟡			0bps	0bps
Ge0/4	🟡	test3		0bps	0bps
Ge0/5	🟡	zone4	42.194.197.1/24	0bps	0bps
Ge0/6	🟡	trust		0bps	0bps
Ge0/7	🟡	untrust		0bps	0bps
TenGe0/0	🟡	monitor		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.

9.4.2 Real-Time Traffic

Application Scenario

Enable this function to display the distribution of real-time uplink and downlink traffic on interfaces.

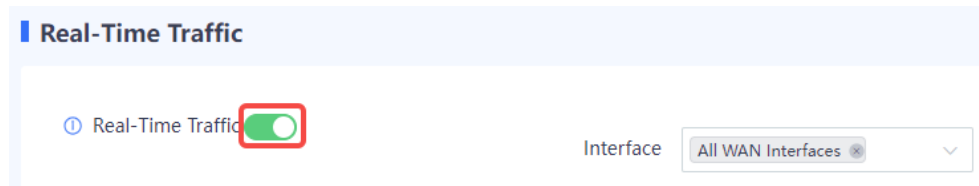
Precautions

Real-time traffic statistics can be collected and displayed only when a hard disk is installed.

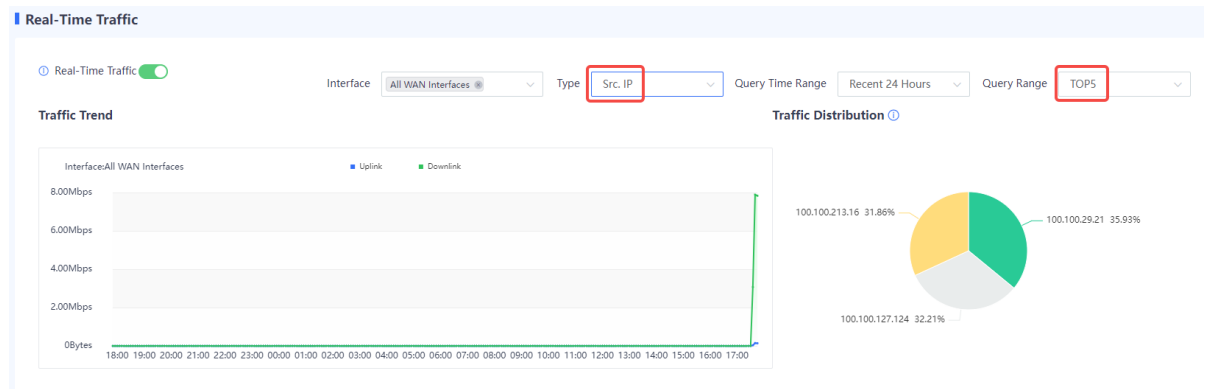
Procedure

- (1) Choose **Monitor > Traffic Monitoring > Real-Time Traffic**.

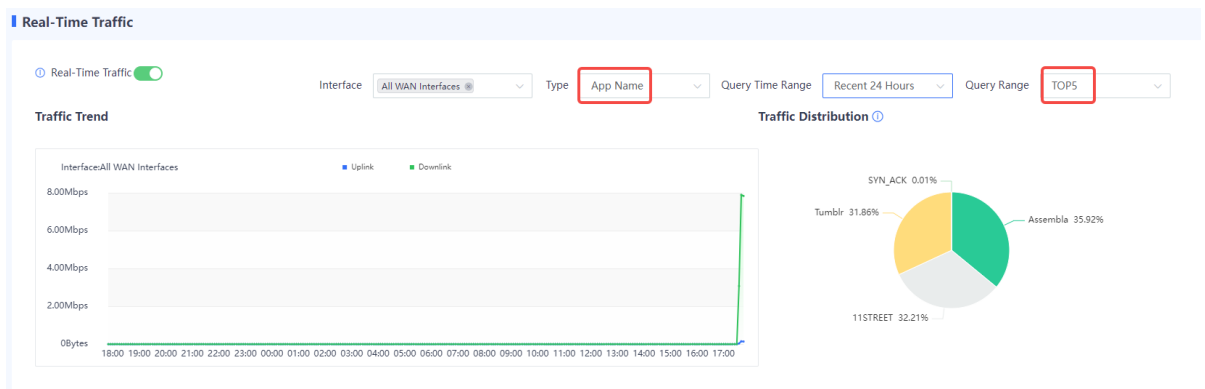
- (2) Toggle on to enable real-time traffic statistics.



- (3) Set **Type** to **Src. IP** to display top 5 source IP addresses with the highest traffic and corresponding traffic information.



- (4) Set **Type** to **App Name** to display top 5 applications with the highest traffic and corresponding traffic information.



9.4.3 Traffic Statistics

Application Scenario

Enable this function to display the distribution of historical uplink and downlink traffic on interfaces.

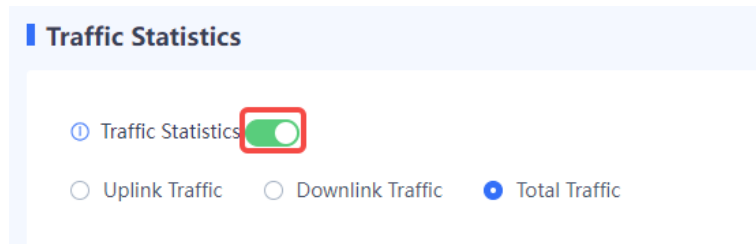
Precautions

Traffic statistics can be collected and displayed only when a hard disk is installed.

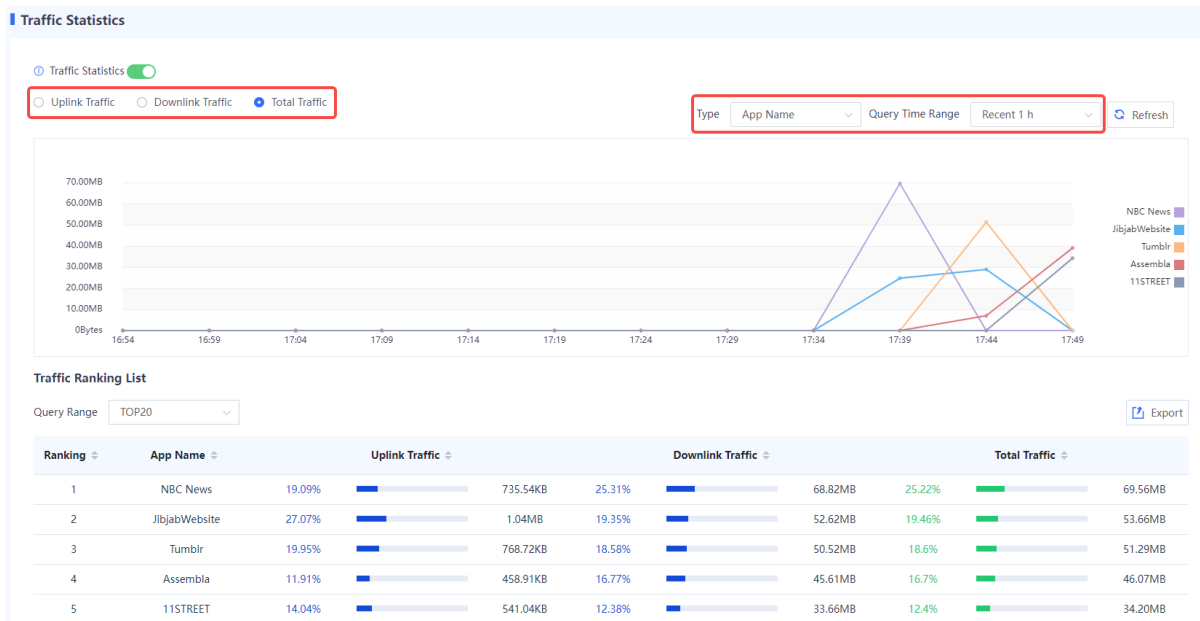
Procedure

- (1) Choose **Monitor > Traffic Monitoring > Real-Time Traffic**.

(2) Toggle on to enable traffic statistics.



(3) Set search criteria to view information about specific traffic.



9.5 Session Monitoring

9.5.1 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.

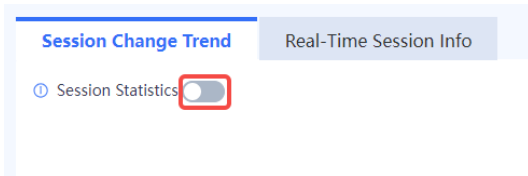
9.5.2 Session Change Trend

Application Scenario

The session change trend function supports real-time monitoring and visualization of the changes in new sessions and concurrent sessions within a specified time period.

Procedure

- (1) Choose **Monitor > Traffic Monitoring > Session Monitoring > Session Change Trend**.
- (2) Toggle on **Session Statistics**.



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

Tip ✕

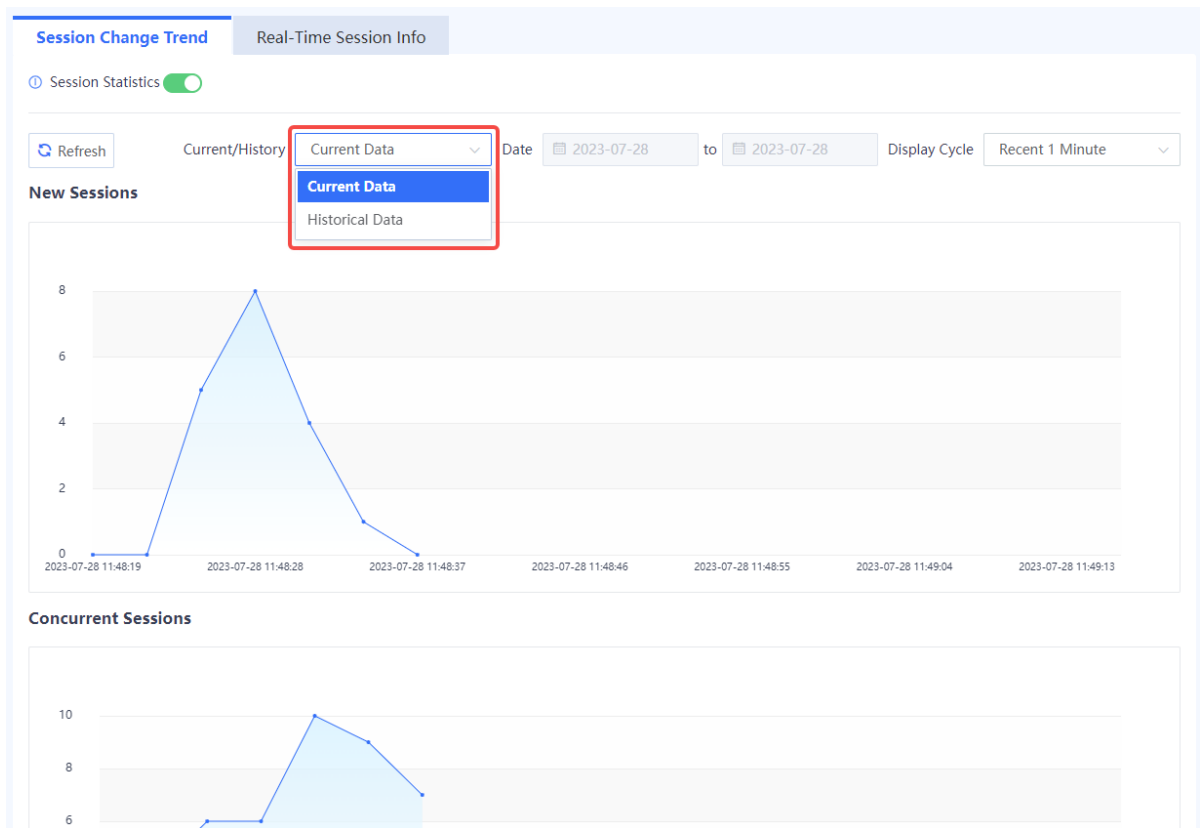
! Are you sure you want to enable real-time session statistics?

When this function is enabled, the device performance is greatly affected.



(3) You can query current or historical data:

- **Current Data:** displays trends in new and concurrent sessions over the last 24 hours.
- **Historical Data:** displays trends in new and concurrent sessions over a specified period of time.



9.5.3 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.

<input type="checkbox"/>	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Security Policy	Operation
<input type="checkbox"/>	2023-07-28 17:42:19	29Minute58Second	172.17.97.28	10.51.212.212	53302	443	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:42:19	29Minute58Second	172.17.97.28	10.51.212.212	53304	443	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:32:42	28Minute14Second	10.52.24.249	10.51.212.212	10863	22	TCP	SSH	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:42:19	29Minute58Second	172.17.97.28	10.51.212.212	53303	443	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:28:56	22Minute19Second	100.100.121.50	200.200.116.196	56419	443	TCP	Global New	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:42:19	29Minute58Second	172.17.97.28	10.51.212.212	53306	443	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:34:45	25Minute57Second	100.100.44.200	200.200.160.243	50197	443	TCP	NBC News	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:30:17	29Minute58Second	10.51.212.212	34.111.156.117	34854	5683	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:32:38	29Minute1Second	10.51.212.212	47.104.206.152	44440	25857	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:41:20	30Minute0Second	100.100.213.16	200.200.107.6	53791	443	TCP	Tumblr	L7	Block View Details

Session Description



Basic Info

Session Creation Time:2023-07-28 17:42:19 Time Before Session Timeout:29Minute58Second

Src. and Dest.

Src. Address:172.17.97.28 Dest. Address:10.51.212.212
 Src. Port:53302 Dest. Port:443
 NAT Src. Address:- NAT Dest. Address:-
 NAT Src. Port:- NAT Dest. Port:-

More

Protocol:TCP App:HTTPSprotocol
 Inbound Interface:Ge0/0 Outbound Interface:lo
 Forward Packets:6 Forward Bytes:1631
 Reverse Packets:4 Reverse Bytes:320
 Security Policy: _visit_local_ Session State:connection established

Disable

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

The screenshot shows the 'Real-Time Session Info' interface. At the top, there are tabs for 'Session Change Trend' and 'Real-Time Session Info'. Below the tabs, there are buttons for 'Block', 'Search Criteria' (highlighted with a red box), 'Custom Field', and 'Refresh'. A 'Refresh Interval' dropdown is set to '30s'. Below these buttons, the 'Search Criteria' section shows 'Session Creation Time: 60Minute' with a 'Clear' button. The main part of the interface is 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. The table contains 12 rows of session data.

<input type="checkbox"/>	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Security Policy	Operation
<input type="checkbox"/>	2023-07-28 17:43:19	2Second	10.52.24.249	10.51.212.212	4894	443	TCP	HTTPSprotocol	_visit_local_	Block View Details
<input type="checkbox"/>	2023-07-28 17:32:42	27Minute16Second	10.52.24.249	10.51.212.212	10863	22	TCP	SSH	_visit_local_	Block View Details
<input type="checkbox"/>	2023-07-28 17:28:56	21Minute21Second	100.100.121.50	200.200.116.196	56419	443	TCP	Global New	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:43:19	2Second	172.17.97.28	10.51.212.212	54171	443	TCP	HTTPSprotocol	_visit_local_	Block View Details
<input type="checkbox"/>	2023-07-28 17:34:45	24Minute59Second	100.100.44.200	200.200.160.243	50197	443	TCP	NBC News	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:30:17	30Minute0Second	10.51.212.212	34.111.156.117	34854	5683	TCP	HTTPSprotocol	_visit_local_	Block View Details
<input type="checkbox"/>	2023-07-28 17:32:38	29Minute27Second	10.51.212.212	47.104.206.152	44440	25857	TCP	HTTPSprotocol	_visit_local_	Block View Details
<input type="checkbox"/>	2023-07-28 17:41:20	30Minute0Second	100.100.213.16	200.200.107.6	53791	443	TCP	Tumblr	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:42:57	8Second	10.51.212.212	114.118.7.163	55213	123	UDP	ApplicationBeing Identified	_visit_local_	Block View Details
<input type="checkbox"/>	2023-07-28 17:43:19	30Minute0Second	10.52.24.249	10.51.212.212	4895	443	TCP	HTTPSprotocol	_visit_local_	Block View Details

(4) (Optional) Select one or more sessions and click **Block** to block the selected sessions.

Session Change Trend **Real-Time Session Info**

Block Search Criteria Custom Field Refresh Refresh Interval 30s

Search Criteria: Session Creation Time: 60Minute Clear

<input type="checkbox"/>	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Security Policy	Operation
<input type="checkbox"/>	2023-07-28 17:42:49	30Minute0Second	172.17.97.28	10.51.212.212	53741	443	TCP	HTTPSProtocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:32:42	27Minute46Second	10.52.24.249	10.51.212.212	10863	22	TCP	SSH	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:28:56	21Minute51Second	100.100.121.50	200.200.116.196	56419	443	TCP	Global New	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:34:45	25Minute29Second	100.100.44.200	200.200.160.243	50197	443	TCP	NBC News	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:30:17	29Minute30Second	10.51.212.212	34.111.156.117	34854	5683	TCP	HTTPSProtocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:32:38	29Minute57Second	10.51.212.212	47.104.206.152	44440	25857	TCP	HTTPSProtocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:41:20	30Minute0Second	100.100.213.16	200.200.107.6	53791	443	TCP	Tumblr	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:42:33	29Minute9Second	10.51.212.210	10.51.212.212	40046	22	TCP	SSH	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:42:38	29Minute49Second	10.51.212.212	10.51.213.10	45144	22	TCP	SSH	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:42:49	2Second	172.17.97.28	10.51.212.212	53740	443	TCP	HTTPSProtocol	__visit_local__	Block View Details

(5) (Optional) Click **Custom Field** to set the session fields to be displayed on the page.

Session Change Trend **Real-Time Session Info**

Block Search Criteria Custom Field Refresh Refresh Interval 30s

Search Criteria: Session Creation Time: 60Minute Clear

<input type="checkbox"/>	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Security Policy	Operation
<input type="checkbox"/>	2023-07-28 17:43:19	2Second	10.52.24.249	10.51.212.212	4894	443	TCP	HTTPSProtocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:32:42	27Minute16Second	10.52.24.249	10.51.212.212	10863	22	TCP	SSH	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:28:56	21Minute21Second	100.100.121.50	200.200.116.196	56419	443	TCP	Global New	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:43:19	2Second	172.17.97.28	10.51.212.212	54171	443	TCP	HTTPSProtocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:34:45	24Minute59Second	100.100.44.200	200.200.160.243	50197	443	TCP	NBC News	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:30:17	30Minute0Second	10.51.212.212	34.111.156.117	34854	5683	TCP	HTTPSProtocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:32:38	29Minute27Second	10.51.212.212	47.104.206.152	44440	25857	TCP	HTTPSProtocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:41:20	30Minute0Second	100.100.213.16	200.200.107.6	53791	443	TCP	Tumblr	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:42:57	8Second	10.51.212.212	114.118.7.163	55213	123	UDP	ApplicationBeing Identified	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:43:19	30Minute0Second	10.52.24.249	10.51.212.212	4895	443	TCP	HTTPSProtocol	__visit_local__	Block View Details

9.6 Device Hardware Monitoring

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

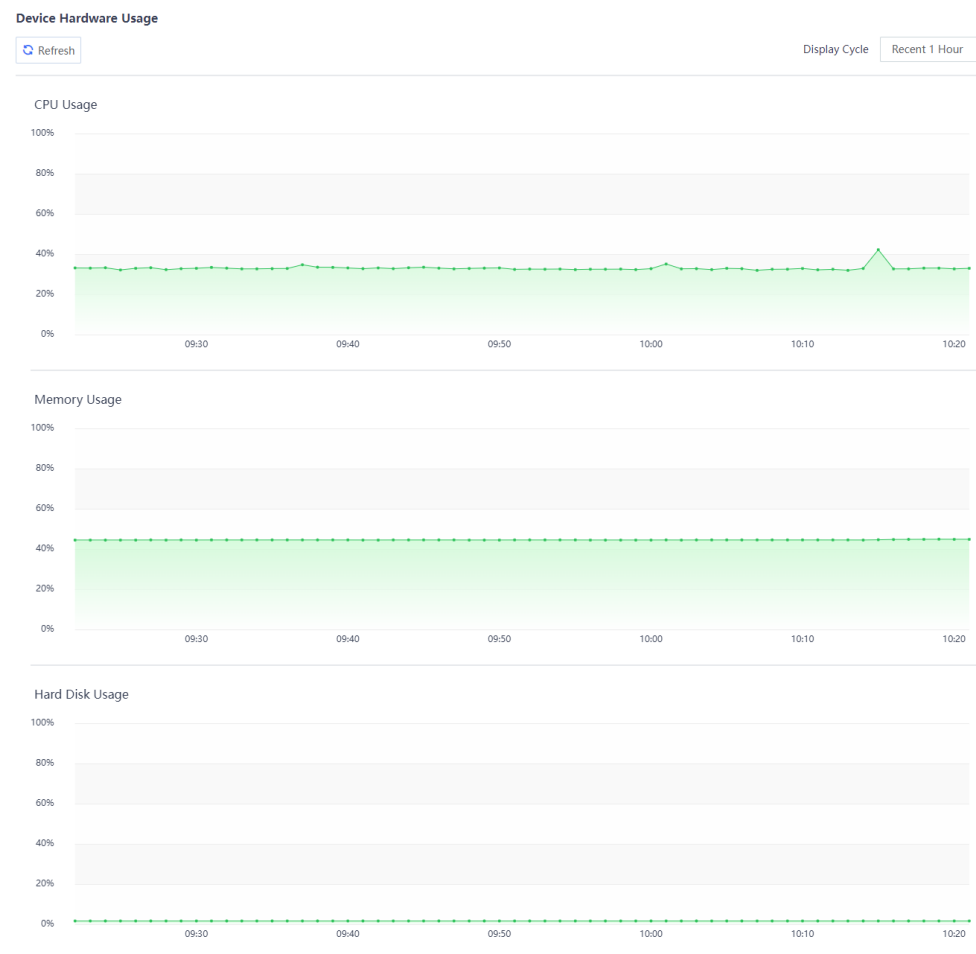
- (1) Choose **Monitor > Device Monitoring > Device Hardware Monitoring**.
- (2) Set **Display Cycle**.



You can select one of the display cycles as needed:

- **Recent 1 Hour:** The system displays the usage over an hour, with a sampling interval of 1 minute.
- **Recent 24 Hours:** The system displays the usage within the last 24 hours with a sampling interval of 5 minutes.
- **Recent 7 Days:** The system displays the usage within the last seven days with a sampling interval of 1 hour.

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



Follow-up Procedure

Item	Description
CPU Usage	<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> <p>App protection or DDoS protection is enabled.</p> <p>Too many connections are created, many of which are initiated by attackers.</p>
Memory Usage	<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 Usage	<p>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.</p>

10 Ruijie Cloud Connection

10.1 Overview

Ruijie Cloud is a remote management platform that manages all links and devices (such as the gateway, switch, AP, and firewall) in SMB scenarios. The administrator can add devices to the Ruijie Cloud, and then manage the devices anytime, anywhere.

10.2 Connecting to Ruijie Cloud

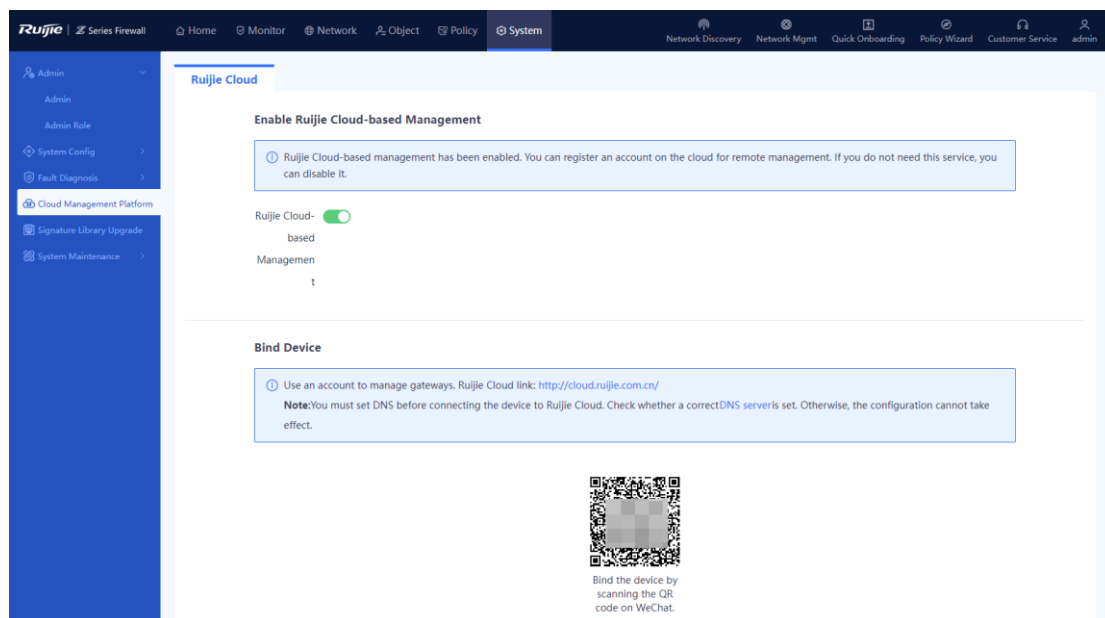
10.2.1 Starting Ruijie Cloud

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) Toggle on **Ruijie Cloud-based Management** (enabled by default). Then you can manage the firewall on Ruijie Cloud.



10.2.2 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 perform maintenance operations on the firewall on Ruijie Cloud.

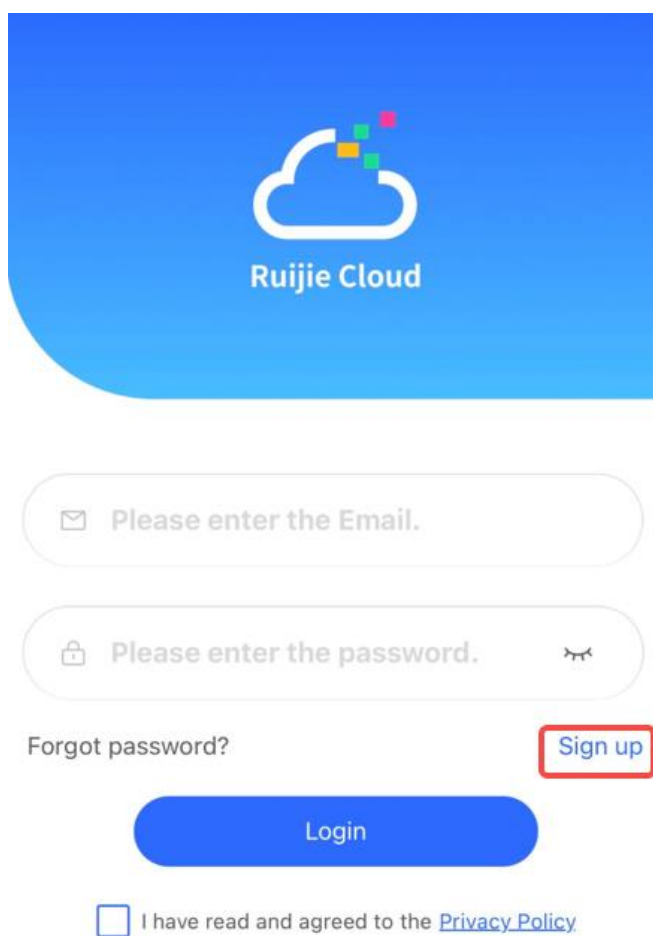
Procedure

- (1) Log in to the web UI 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 for a Ruijie Cloud account.

Note

You can also enter the URL address of Ruijie Cloud in the address bar of your browser and register a Ruijie Cloud account.

- (4) After registering the Ruijie Cloud account, you can log in to view basic device information.

Figure 10-1 Registering an Account

The screenshot shows the registration interface for Ruijie Cloud. At the top, there is a blue banner with the Ruijie Cloud logo and the text 'Ruijie Cloud'. Below the banner, there are two input fields: 'Please enter the Email.' and 'Please enter the password.' with a toggle for visibility. There is a 'Forgot password?' link, a 'Sign up' button (highlighted with a red box), and a 'Login' button. At the bottom, there is a checkbox for 'I have read and agreed to the Privacy Policy'.

Follow-up Procedure

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

① 请用帐号进行管理网关设备。云网地址链接为：<http://cloud.ruijie.com.cn/>
 注意：连接诺客云需要配置DNS，请检查是否已经配置了正确的【DNS服务器】，否则将不能生效！



微信扫一扫随时随地
管理你的网络

设备已绑定帐号：186****3010 [前往云平台管理](#)

[解绑](#)

10.3 Operations on Ruijie Cloud

10.3.1 Viewing Device Information

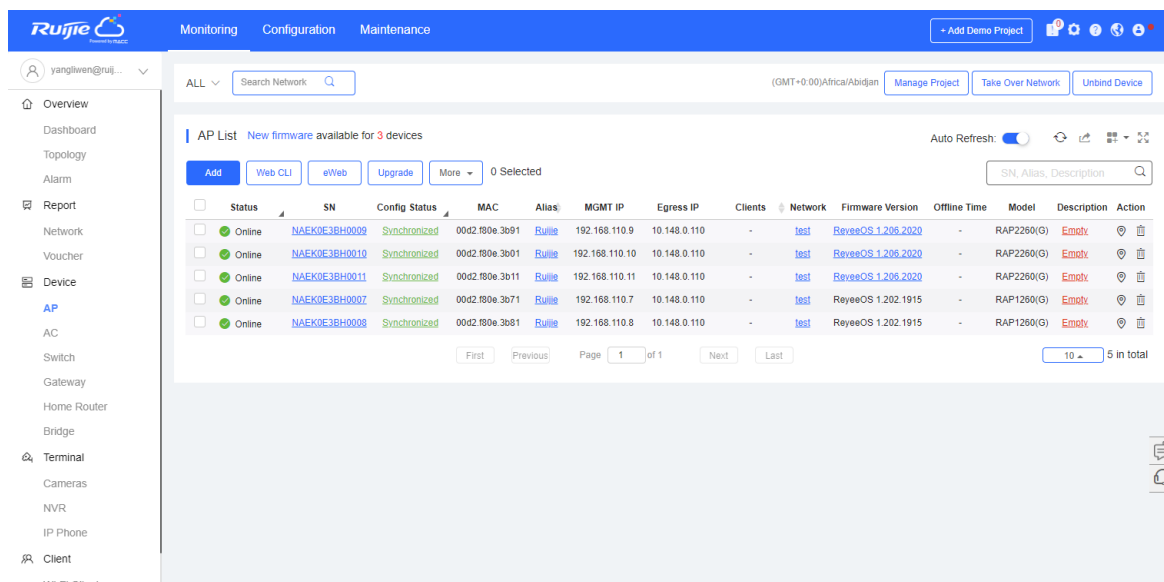
Application Scenario

After enabling Ruijie Cloud, enter the address of Ruijie Cloud (<https://cloud-as.ruijienetworks.com/>) in the address bar of your browser, log in to Ruijie Cloud, and then view device information, online status, and interface information.

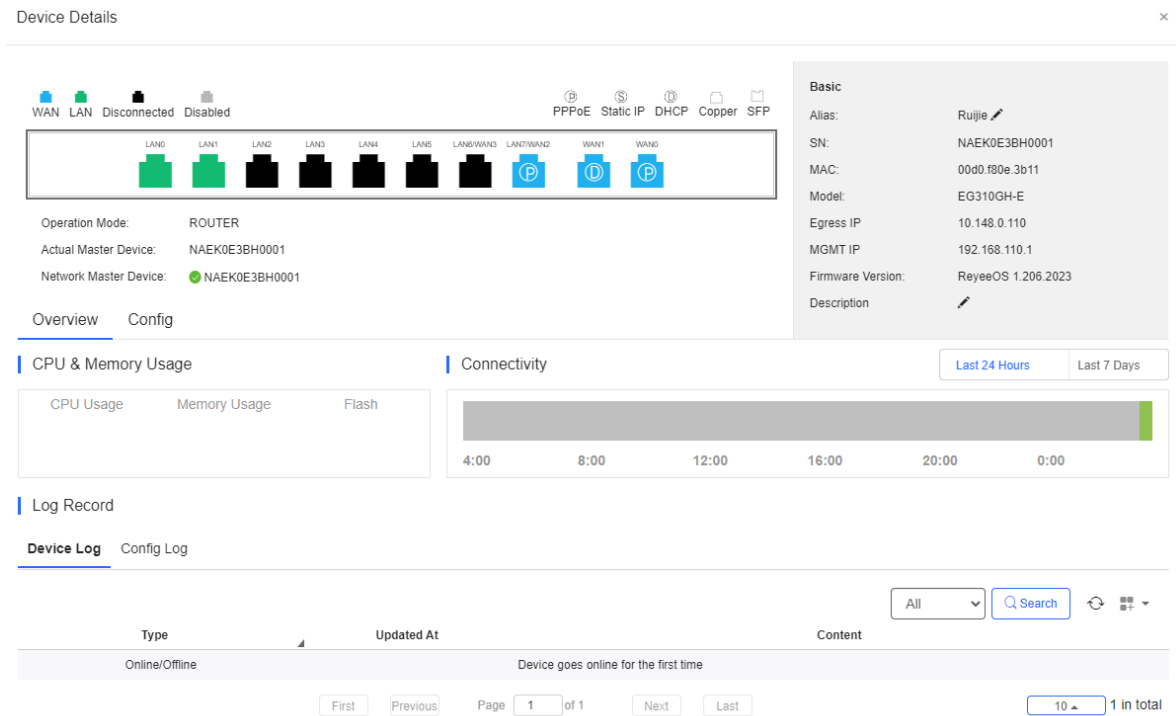
Procedure

- (1) Choose **Monitoring > Device** to access the page of device list.
- (2) View device details.

Figure 10-2 Firewall Details



- (3) The system displays the basic device information such as status, SN, device, management address, software version, and device model.
- (4) Click the value in the **SN** column to access the device management page. On the page that is displayed, you can 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 tabs in status information, you can view detailed interface information, such as WAN/LAN port information (including the port number, mode, and subnet mask).

Figure 10-3 Device Panel Information



Figure 10-4 Basic Information

Basic	
Alias:	Ruijie 
SN:	NAEK0E3BH0001
MAC:	00d0.f80e.3b11
Model:	EG310GH-E
Egress IP	10.148.0.110
MGMT IP	192.168.110.1
Firmware Version:	ReyeeOS 1.206.2023
Description	

Figure 10-5 Status Information

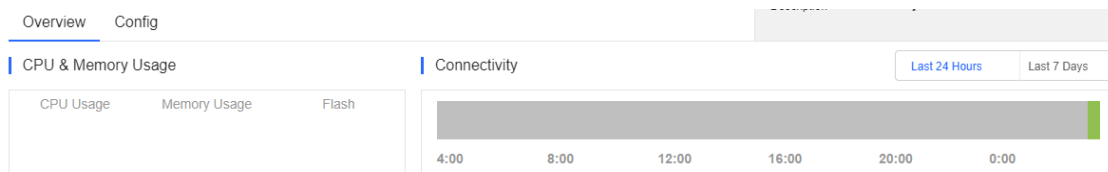


Figure 10-6 Interface Information



The screenshot shows the 'Interface Information' page for the WAN interface. It includes a '端口信息' (Port Information) section with a dropdown menu set to 'Ge0/2'. Below this, there are two main sections: '基本信息' (Basic Information) and '子接口信息' (Sub-interface Information).

基本信息 (Basic Information):

- 模式: 路由模式
- IP: --
- 子网掩码: --
- IP地址类型: 其他类型
- 上行带宽: 100000kbps
- 下行带宽: 100000kbps
- 运营商: --
- 省份: --
- 城市: --

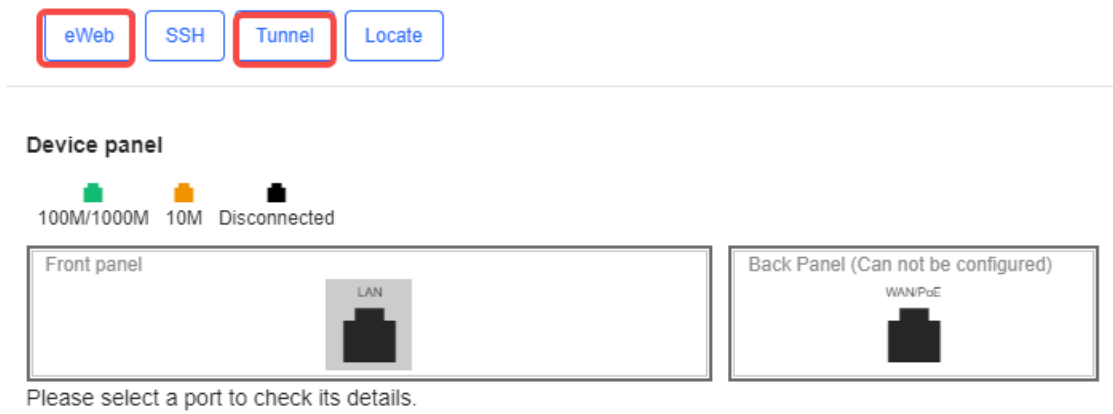
子接口信息 (Sub-interface Information):

子接口名称	VLAN	IP地址
Ge0/2.101	101	--
Ge0/2.102	102	--

10.3.2 Managing Tunnels

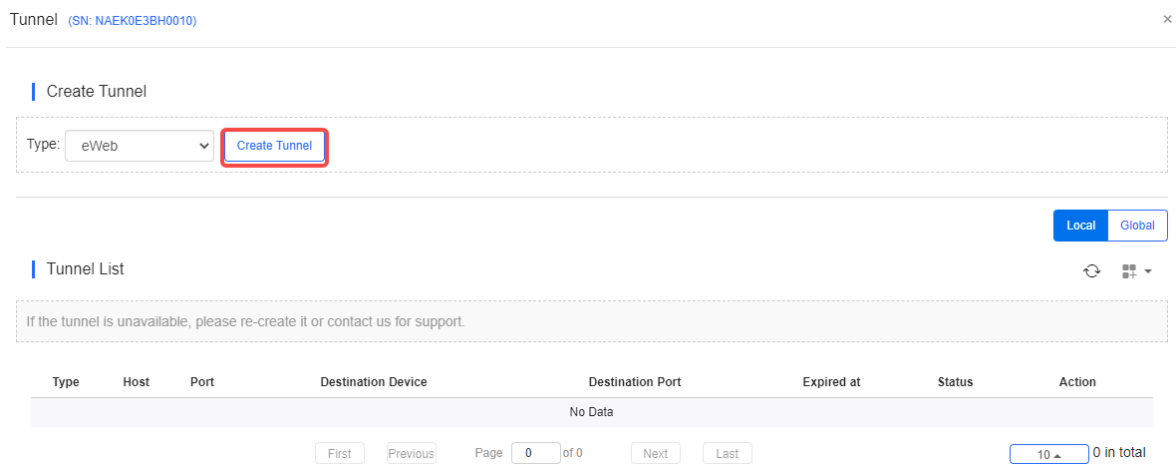
- (1) Click **Tunnel** or **eWeb** to access the EWEB page of the device.

Figure 10-7 Tunnel Management



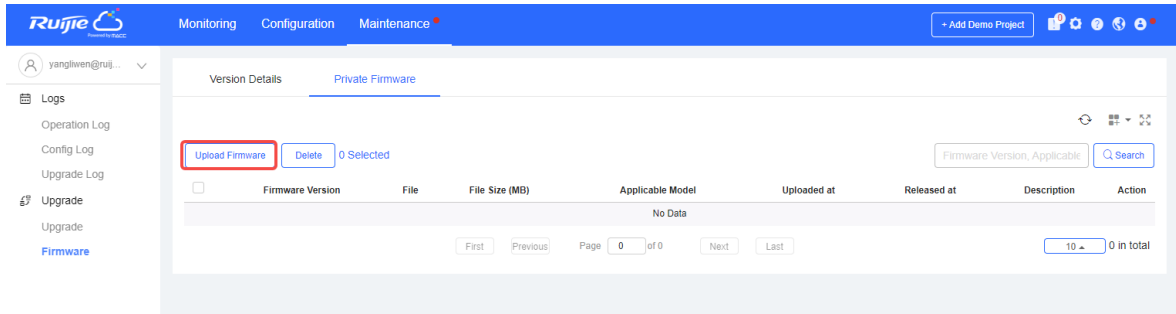
(2) To add a tunnel, click **Create Tunnel**.

Figure 1-1 Creating a Tunnel

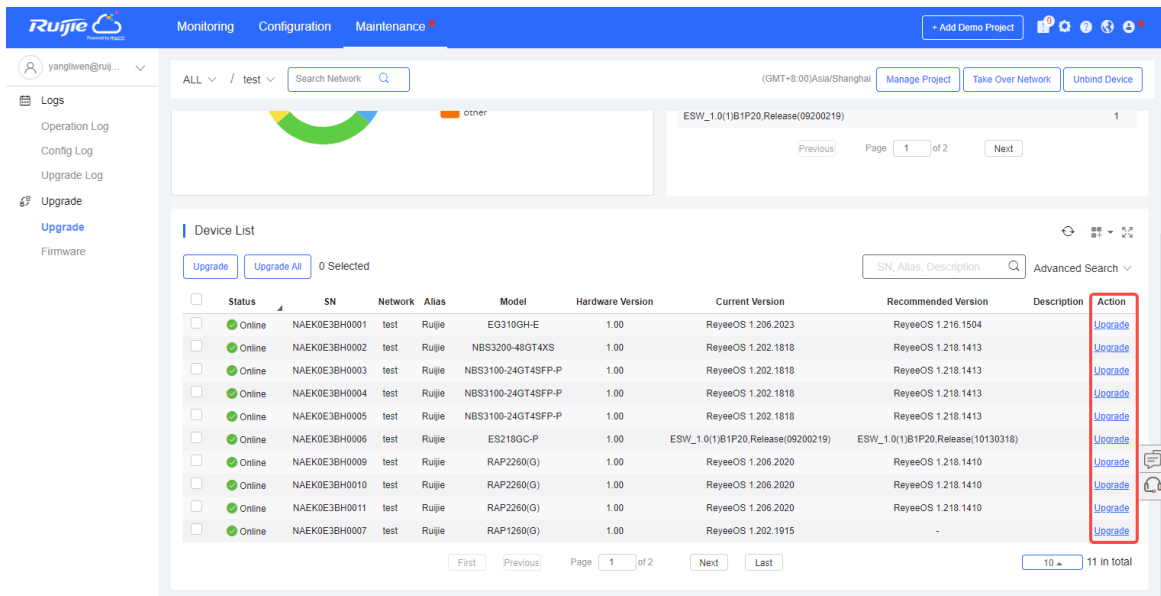


10.3.3 Upgrading Device Software

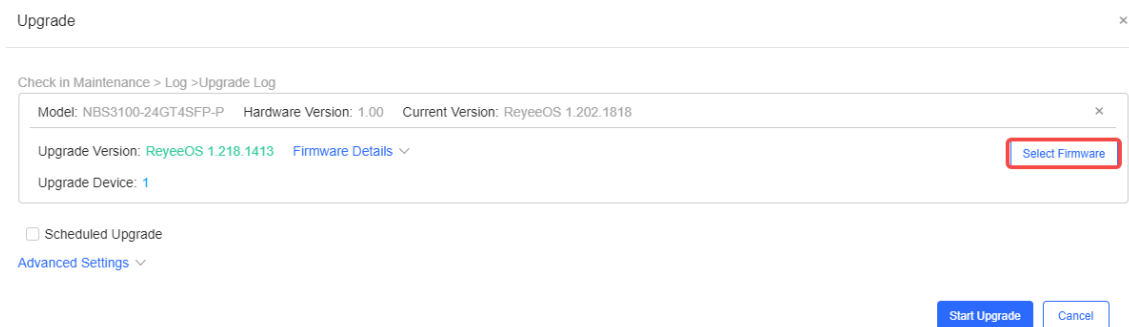
- (1) Choose **Maintenance > Upgrade > Firmware > Private Firmware**.
- (2) Click **Upload Firmware** to upload the software version/firmware version.



(3) Choose **Maintenance > Upgrade > Upgrade**, find the device to be upgraded in the device list, and click **Upgrade** in the **Action** column.



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

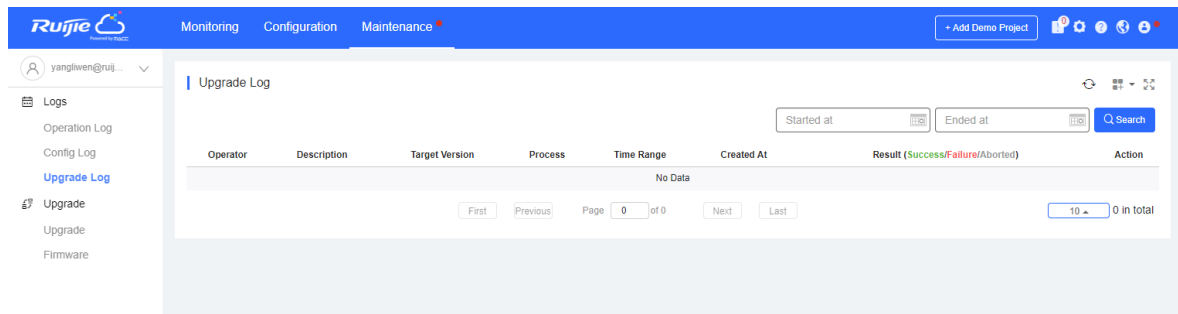


(5) Click **Start Upgrade** to start the upgrade.

Then the device performs upgrade. During the upgrade, the device will automatically restart. Wait until the upgrade is completed.

(6) When the upgrade is completed, choose **Maintenance > Logs > Upgrade Log** to view the upgrade result.

Figure 10-8 Upgrade Result



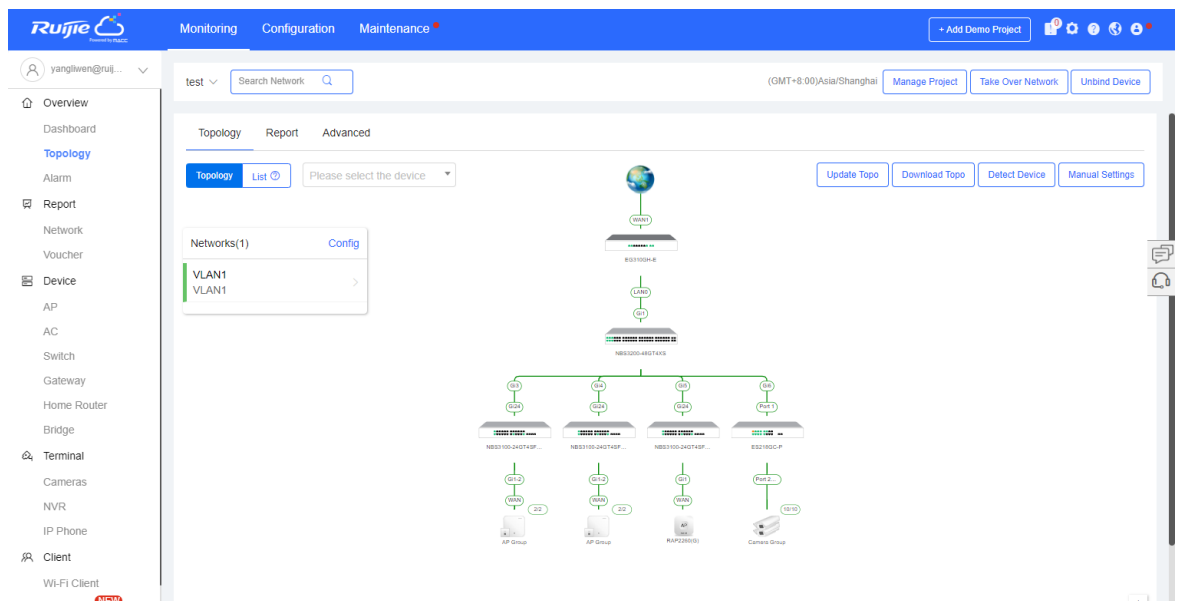
10.3.4 Viewing Network Topology

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 bridge interfaces and routing interfaces are mixedly 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.

(1) Choose **Monitoring > Overview > Topology** to view the topology of the 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 modify the topology or add the devices that are not discovered automatically, click **Manual Settings**.

11 Typical Configuration Examples

11.1 Configuring Extranet Users to Access Intranet Servers

This section describes the configuration of allowing extranet users to access intranet servers using public IP addresses.

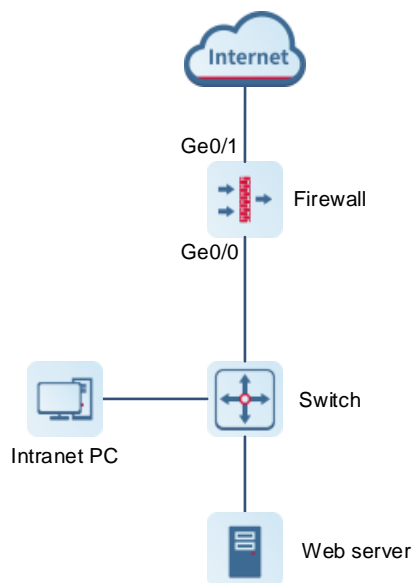
Networking Requirements

A company has deployed a firewall at the network border as a security gateway. To allow external access to an intranet web server, destination NAT needs to be configured on the firewall. This will map the IP address 192.168.1.2 of the intranet web server to a public IP address 172.26.1.116 assigned to the extranet interface. This configuration allows extranet users to access the web server.

Network topology

The network topology is shown in [Figure 11-1](#).

Figure 11-1 Networking Topology



Configuration Points

- (1) Complete basic network access settings.
- (2) Configure a security policy.
- (3) Configure a static NAT policy.

Procedure

- (1) Complete basic network access settings.

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

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	-		Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500	Edit
<input type="checkbox"/>	Ge0/1	-		Routing	untrust	IPv4: DHCP	172.26.1.116/24	-	1500	Edit

(2) Configure the security policy.

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

The policy configuration is as follows:

<input type="checkbox"/>	2	allow_trus...	-	trust	any	untrust	any	any	any	any	
		allow_trust_to_untrust									

(3) Configure a destination NAT policy.

a Choose **Policy > NAT Policy > NAT**.

b Click **Create**.

<input type="checkbox"/>	Name	Time Range	NAT Type	Packet Before NAT				Packet After NAT			Description	Hit Count	Operation	
				Src. Security Zone	Dest. Security Zone	Src. Address	Dest. Address	Service	Src. Address	Dest. Address				Dest. Port
<input type="checkbox"/>	test2345	any	SNAT	any	any	any	any	any	Outbound Interface Address	-	-	ffsv	0 Clear	Edit Delete
<input type="checkbox"/>	nat_rule	any	SNAT	trust	untrust	any	any	any	Outbound Interface Address	-	-		0 Clear	Edit Delete
<input type="checkbox"/>	test	any	SNAT	any	DMZ,untrust...	any	any	ping	Outbound Interface Address	-	-		0 Clear	Edit Delete

c Set parameters of the destination NAT policy.

< 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
Service	Source ports: 0–5535. Destination port: 18080 (extranet port)
Packet After NAT	
IP Address	192.168.1.2

Item	Description
Port	80 (internal port)

- d Click **Save**.

Verification

Access the intranet server at 172.26.1.116 from the extranet.

11.2 Configuring Intranet Users to Access Intranet Servers Through a Public IP Address

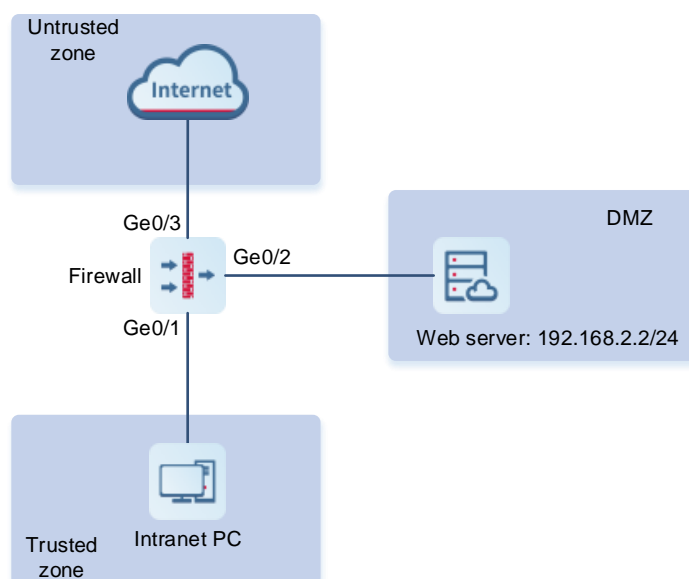
This section describes the configuration of allowing intranet users to access an intranet server using a public IP address.

Networking Requirements

A company has deployed a firewall at the network border as a security gateway and a web server on the intranet to provide services to external users. The company requires that the IP address 192.168.2.2 of an intranet web server is mapped to the IP address 200.10.10.10 of an extranet interface so that both intranet and extranet users can access the web server.

- The web server is in the intranet server zone. The web server in the DMZ zone is at 192.168.2.2 and uses HTTPS.
- Extranet users can access the server through the extranet interface located in the untrust zone at 200.10.10.10 and using port 50000.
- Intranet users in the trust zone can also access the server through the extranet interface located in the untrust zone at 200.10.10.10 and using port 50000, and the extranet interface of the firewall is used as the source address to access the web server.

Network Topology



Configuration Points

- (1) Complete basic network access settings.
- (2) Configure the security policy.
- (3) Configure the destination NAT policy for extranet users.
- (4) Configure the twice NAT policy for intranet users.

Procedure

- (1) Complete basic network access settings by referring to [3 Quick Deployment](#).
- (2) Configure the security policy.

The policy configuration is as follows:

<input type="checkbox"/>	Priority	Name	Type	Src. Security Zone	Src. Addresses	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	Permit	0		<input checked="" type="checkbox"/> Edit Delete

- (3) Configure the destination NAT policy for extranet users.
 - a Choose **Policy > NAT Policy > NAT**.
 - b Click **Create**.
 - c On the **Add NAT** page, set parameters of the destination NAT policy.

< 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	rule_1
Enabled State	Select Enable .
Packet Before NAT	
Src. Security Zone	Select untrust .
Src. Address	Select any .
Dest. Address	Extranet interface IP address of the firewall: 200.10.10.10.

Item	Description
Service	Create a customized service server_map, for example, TCP. The source ports range from 0 to 65535, and the destination port is 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).

- d Click **Save**.
- (4) Configure the twice NAT policy for intranet users.
- a Choose **Policy > NAT Policy > NAT**.
 - b Click **Create**.
 - c On the **Add NAT** page, set parameters of a twice NAT policy.

< 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	Select Enable .
Packet Before NAT	
Src. Security Zone	Select trust .
Src. Address	Select any .

Item	Description
Dest. Address	Outside interface IP address of the firewall: Ge0/3:200.10.10.10.
Service	Create a customized service server_map, for example, TCP. The source ports range from 0 to 65535, and the destination port is 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 you specify the 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 IP address of web server in the DMZ to 192.168.2.2.
Dest. Port Number Translated to	Set the web server port number to 443.

d Click **Save**.

Verification

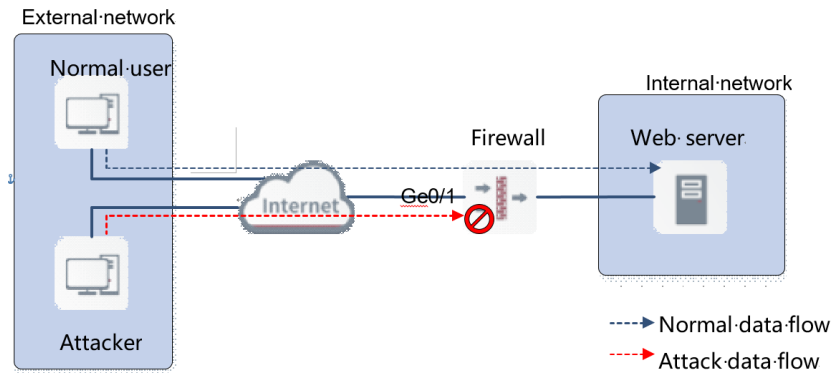
- Visit <http://200.10.10.10:50000> from the intranet.
- Visit <http://200.10.10.10:50000> from the extranet.

The NAT policy is successfully configured if the intranet web server is accessible both from the intranet and extranet.

11.3 Configuring DDoS Attack Defense

Networking Requirements

The firewall is deployed at the border of the intranet, and a web server is deployed on the intranet. Web servers are frequently targeted by different types of DDoS attacks, including SYN, UDP, and ICMP flood attacks. To ensure the normal operation of the web servers and protect them against these attacks, you are advised to configure the attack defense function on the firewall.



Configuration Points

- (1) Enable traffic learning on Ge0/1 connected to the extranet. This function enables the firewall to collect statistics on the traffic that flows between the extranet and intranet.
- (2) Enable SYN, UDP, and ICMP flood attack defense on the firewall. Use default thresholds for each attack defense configuration.

Procedure

- (1) Enable traffic learning on Ge0/1.
 - a Choose Policy > Traffic Learning.
 - b Click **Traffic Learning Address** and configure the address for enabling traffic learning.

Enter the IP address of Ge0/1 in **Add Custom IP Address/Range** and click **Save**.

Set Traffic Learning Address ⊗

① Set a destination IP address for traffic learning to enable the system to discover abnormal ports and provide policy optimization suggestions. **Note:** A larger number of addresses will take longer scanning time. Select only necessary addresses.

Select or Add Addresses

* Add Custom IP Address/Range

Enter an IP address, IP range, IP address/mask, or IP address/prefix.

Add ↑

☰ Quick Import from Address Object

☰ Quick Import from Port Scan Config

IP Address/Range 🗑️ Delete Selected

No Data

Save

Save and Enable Now

Cancel

- c Click Enable Traffic Learning.
- (2) Add Ge0/1 to the **untrust** zone.
 - a Choose **Network > Zone**.
 - b Click **Edit** in the **Operation** column of the untrust area.
 - c In the **Interface** area, select Ge0/1.

- d Click **Save**.
- (3) Configure the DoS and DDoS attack defense function.
 - a Choose **Policy > Security Defense > DoS/DDoS Attack Defense**.
 - b Click **Create**.
 - c Set parameters of the DoS/DDoS attack defense policy.

< Back
 Add Dest. 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

Dest. Defense Against DoS/DDoS Selected Defense Types: SYN Flood Attack Defense,UDP Flood Attack Defense,ICMP Flood Attack Defense,ICMPv6 Flood Attack Defense

Action After Detecting Attacks Log Limit

Advanced Defense

Packet-based Attack All

<input type="checkbox"/> Teardrop Attack Defense	<input type="checkbox"/> Control IP Packets with Source Routes	<input type="checkbox"/> Control IP Packets with Record Routes
<input type="checkbox"/> Smurf Attack Defense	<input type="checkbox"/> ICMP Redirect Attack Defense	<input type="checkbox"/> ICMP Unreachable Attack Defense
<input type="checkbox"/> LAND Attack Defense	<input type="checkbox"/> WinNuke Attack Defense	<input type="checkbox"/> Fraggle Attack Defense
<input type="checkbox"/> Large ICMP Packet Attack Defense <input style="width: 40px;" type="text" value="1500"/>		

Filtering out IPv6 Packets with Specific EHS

d Click **Save**.

Verification

- Once configured, the default thresholds are used for DDoS attack defense. After traffic learning is completed, you can check the result of attack defense. If the web server still suffer from attacks, you can change the attack thresholds as needed.

Scan Attack Defense



IP Scan Defense

Limit (pps)

Blocking Duration (s)

Port Scan Defense

Limit (pps)

Blocking Duration (s)

Confirm
Cancel

- When the configuration is completed, security logs of the detected attacks are recorded. Choose **Monitor > Log Monitoring > Security Log** to check detailed security logs.

12 FAQs

12.1 What Can I Do If I Fail to Log In to the Web Page?

Possible Causes

Possible causes are as follows:

- The firewall is not fully started.
- The address `https://device IP` (default: `https://192.168.1.200`) is incorrect.
- A network connection error occurs between the management PC and the firewall.
- The browser of the management PC is incompatible.
- The login password is incorrect.

Solution

Troubleshoot the fault based on the preceding causes:

- Wait for about 2 minutes until the firewall is started. Observe LEDs (including PWR, SYS, and interface status LEDs) on the firewall until all of them are on and try again.
- Confirm that the address (`https://device IP`) entered in the address bar is correct. (The default address `https://192.168.1.200` can be used.)
- Troubleshoot the connectivity issue between the management PC and the firewall.

Check whether the IP addresses of the management PC and firewall are on the same network segment. The default address `192.168.1.9` can be used.

Log in to the management PC, run **ping** `mgmt-ip-address` in the CLI (`mgmt-ip-address` is the IP address of MGMT port of the firewall device) to check connectivity between the firewall and the management PC.

- If the management PC can receive a message from the firewall, the connectivity is normal. Then troubleshoot the fault based on other possible causes.
 - If the management PC does not receive a message from the firewall, a connectivity issue exists. In this case, reconfigure the IP address of the MGMT port of the firewall.
- Resolve the incompatibility of the browser.

Check whether the browser on the MGMT PC meets compatibility requirements:

- If so, continue troubleshooting based on other possible causes.
- If not, reinstall a browser that meets compatibility requirements.

Note

The compatible browsers include Internet Explorer (IE), Firefox, Google Chrome, and 360 Browser.

- Resolve the incorrect login password error.
 - a Enter the correct password.

- b If you enter incorrect passwords multiple times, you are advised to reset the login password to the default password.

12.2 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 12-1 Modifying the SSH Port Number

