Ruijie Cybrey
RG-CF series next-generation high-performance firewalls

User Manual

Document version: V1.0
Date: May 09, 2026
Copyright © 2026 Ruijie Networks

Copyright

Copyright © 2026 Ruijie Networks

All rights are reserved in this document and this statement.

Without the prior written consent of Ruijie Networks, no organization or individual is permitted to reproduce, extract, back up, modify, or distribute the content of this document in any manner or form. It is also prohibited to translate the document into other languages or use any or all parts of it for commercial purposes.

  and other Ruijie networks logos are trademarks of Ruijie Networks.

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

Disclaimer

The products, services, or features that you purchase are subject to commercial contracts and terms. It is possible that some or all of the products, services, or features described in this document may not be available for purchase or use. Unless agreed upon otherwise in the contract, Ruijie Networks does not provide any explicit or implicit statements or warranties regarding the content of this document.

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

The content of this document is subject to constant change due to product version upgrades or other reasons. Thus, Ruijie Networks reserves the right to modify the content of the document without prior notice or prompt.

This manual serves solely as a user guide. While Ruijie Networks endeavors to ensure the accuracy and reliability of the content when compiling this manual, it does not guarantee that the content of the manual is free of errors or omissions. All information contained in this manual does not constitute any explicit or implicit warranties.

Personal Data Statement

During the operation or troubleshooting of the products, services, or features you have purchased, certain personal data of users may be collected or used. Therefore, it is essential for you to establish and implement appropriate privacy policies, in compliance with the relevant laws and regulations of the applicable countries or regions, to ensure the complete protection of users' personal data.

If Ruijie Networks is involved in this process, we will strictly adhere to the relevant laws and regulations of the applicable countries or regions and take all necessary actions to safeguard users' personal data.

When discarding, reclaiming, or reusing a device, please ensure to back up or clear any stored data to avoid data leakage. For assistance, please contact our after-sales technical support.

Preface

Intended Audience

This document is intended for:

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

Technical Support

- Ruijie Networks website: https://www.ruijie.com/
- Online support center: https://www.ruijie.com/support
- Case portal: https://caseportal.ruijie.com
- Community: https://community.ruijie.com/
- Email support: service_rj@ruijie.com
- Live chat: https://www.ruijie.com/rita
- Documentation feedback: doc@ruijie.com.cn

Conventions

1. GUI Symbols

GUI 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 menu 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. Notes

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 UX Improvement Plan 3

2.3 Web UI Layout 6

2.4 Operations on the Web UI 6

2.4.1 Changing Login User Password 6

2.4.2 Logging Out 8

2.4.3 Resetting the Password 8

2.4.4 Version Upgrade Prompt 10

2.4.5 Configuring a Homepage Card 11

3 Quick Deployment 13

3.1 Deployment Planning 13

3.1.1 Planning Device Locations and IP Addresses 13

3.1.2 Planning Networking Mode 13

3.1.3 Determining the Service Traffic Access Relationship 14

3.2 Deployment 15

3.2.1 Performing Quick Onboarding 15

3.2.2 Configuring Security Policies Using the Wizard 44

4 Policy Configuration and Management 54

4.1 Security Policy 54

4.1.1 Overview 54

4.1.2 Manually Configuring Security Policies 54
4.1.3 Conducting Simulation Run 62
4.1.4 Importing Configuration Files to Configure Security Policies 64
4.1.5 Exporting Security Policies 66
4.1.6 Adjusting Security Policy Order 66
4.1.7 Searching for Security Policies 67
4.1.8 Optimizing Security Policies 70
4.1.9 Viewing Policy Life Cycle 71
4.1.10 Enabling Basic Protocol Packet Control 72
4.2 Enabling Port Scan 73
4.3 Enabling Traffic Learning 78
4.4 Traffic Control Policy 83
4.4.1 Overview 83
4.4.2 Configuring Traffic Control Policies 83
4.5 NAT Policy 89
4.5.1 NAT Overview 89
4.5.2 NAT Types 89
4.5.3 Working Principle 91
4.5.4 Configuring NAT 96
4.5.5 Configuring NAT46 110
4.5.6 Configuring NAT64 114
4.5.7 Configuring NAT66 118
4.5.8 Enabling the ALG Function 124
4.5.9 Configuring an Address Pool 125

4.5.10 Configuring NAT64 Prefixes 125
4.6 Port Mapping Policy 127
4.6.1 Overview 127
4.6.2 Configuring a Port Mapping Policy 127
4.7 Security Defense 131
4.7.1 Overview 131
4.7.2 Attack Types 131
4.7.3 Configuring DoS/DDoS Attack Defense 132
4.7.4 Configuring ARP Attack Defense 138
4.7.5 Configuring Local Defense 142
4.7.6 DNS Protection 145
4.7.7 IP-MAC Binding 149
4.8 Threat Intelligence 154
4.8.1 Overview 154
4.8.2 Enabling Threat Intelligence 154
4.8.3 Customizing Threat Intelligence 156
4.8.4 Configuring an Excluded Threat 160
4.8.5 Viewing Threat Intelligence Logs 161
4.8.6 Upgrading a Threat Intelligence Signature Library 162
4.9 Session Control 162
4.9.1 Configuring the Uplink Packet Rate Limit 162
4.9.2 Configuring New Session Rate Limiting 164
4.9.3 Configuring a Session Number Limit Policy 167
4.10 Blocklist and Allowlist 171

4.10.1 Overview 171
4.10.2 Creating an IPv4 Allowlist 172
4.10.3 Creating an IPv6 Allowlist 173
4.10.4 Creating an IPv4 Blocklist 174
4.10.5 Creating an IPv6 Blocklist 176
4.10.6 Creating a Temporary IPv4 Blocklist 177
4.10.7 Creating a Temporary IPv6 Blocklist 179
4.10.8 Creating a MAC Address Blocklist 180
4.10.9 Creating a User Blocklist 182
4.11 SSL Proxy 184
4.11.1 Configuring an SSL Proxy Policy 184
4.11.2 Configuring an SSL Proxy Allowlist 192
5 Object Configuration and Management 196
5.1 Address Object 196
5.1.1 Overview 196
5.1.2 Creating an IPv4 Address Object 197
5.1.3 Creating an IPv4 Address Group Object 198
5.1.4 Creating an IPv6 Address Object 199
5.1.5 Creating an IPv6 Address Group Object 201
5.1.6 Creating a MAC Address Object 202
5.1.7 Creating a MAC Address Group Object 203
5.1.8 Creating a Domain Name Object 204
5.2 Application 206
5.2.1 Overview 206

5.2.2 Viewing Application Information in a Signature Library 206
5.2.3 Creating a Custom Application 208
5.2.4 Creating a Custom Application Group 210
5.2.5 Upgrading an Application Identification Signature Library 211
5.3 Content Identification Library 211
5.3.1 Configuring a Keyword Set 211
5.3.2 URL Category 213
5.3.3 File Type Group 218
5.4 Services 221
5.4.1 Overview 221
5.4.2 Predefined Service 221
5.4.3 Configuring a Custom Service 222
5.4.4 Creating a Service Group 224
5.5 Region 226
5.5.1 Overview 226
5.5.2 Predefined Region 226
5.5.3 Custom Region 226
5.5.4 Upgrading a Regional Signature Library 228
5.6 Time Plan 228
5.6.1 Overview 228
5.6.2 Creating a Cyclic Time Plan 228
5.6.3 Creating a One-Off Time Plan 229
5.7 ISP Address Library 231
5.7.1 Overview 231

5.7.2 Creating an ISP Address Library Manually....231
5.7.3 Creating an ISP Address Library by Importing an Address File....232
5.8 User Authentication....233
5.8.1 Overview....233
5.8.2 User Management....234
5.8.3 User Tag....243
5.8.4 User Import....246
5.8.5 User Package Management....249
5.8.6 Online User....251
5.8.7 Authentication Domain Management....252
5.8.8 Authentication Policies....257
5.8.9 Authentication Template - Local Portal Authentication....259
5.8.10 Authentication Template - WiFiDog Authentication....268
5.8.11 Authentication Settings....271
5.8.12 RADIUS Authentication Server....277
5.8.13 LDAP Authentication Server....280
5.8.14 SMS Authentication Server....285
5.9 Certificate Management....287
5.9.1 Overview....287
5.9.2 Local Certificate....287
5.9.3 SSL Certificate....288
5.10 Content Template....294
5.10.1 Virus Protection....294
5.10.2 Intrusion Prevention....299

5.10.3 URL Filtering 308
5.10.4 Web App Protection 315
5.10.5 Keyword Filtering 322
5.10.6 File Filtering 324
5.10.7 AI-based Threat Detection 328
5.10.8 Advanced Settings 333
5.11 Security Rule Base Management 334
5.11.1 Intrusion Prevention Rule Base 334
5.11.2 Web App Protection Rule Base 337
6 Network Configuration 337
6.1 Interface 337
6.1.1 Configuring a Physical Interface 337
6.1.2 Configuring a Sub-interface 350
6.1.3 Configuring a Bridge Interface 358
6.1.4 Configuring a Switching Interface 364
6.1.5 Configuring an Aggregate Interface 371
6.1.6 Configuring a Tunnel Interface 382
6.1.7 Configuring a GRE Interface 387
6.1.8 Multi-PPPoE 392
6.1.9 Configuring a Cellular Interface 393
6.2 Security Zone 399
6.2.1 Overview 399
6.2.2 Creating a Security Zone 400
6.3 Route Management 402

6.3.1 Overview 402
6.3.2 Creating a Static Route 402
6.3.3 Creating an Intelligent Routing Policy 404
6.3.4 Viewing Address Library Routes 409
6.3.5 Configuring a Routing Policy 409
6.3.6 Viewing Route Tables 413
6.4 OSPF 413
6.4.1 Overview 413
6.4.2 Concepts 414
6.4.3 Working Principle of OSPF 418
6.4.4 OSPF Route Advertisement 421
6.4.5 OSPF Route Summarization 421
6.4.6 OSPF Configurations 421
6.5 OSPFv3 433
6.5.1 Overview 433
6.5.2 Concepts 433
6.5.3 Working Principle of OSPFv3 437
6.5.4 OSPFv3 Route Advertisement 439
6.5.5 OSPFv3 Configurations 439
6.6 Outbound Interface Load Balancing 447
6.6.1 Overview 447
6.6.2 Configuring Load Balancing Based on the Source IP Address 449
6.6.3 Configuring Load Balancing Based on the Source IP Address and Destination IP Address 452
6.6.4 Configuring Load Balancing Based on Bandwidth 455

6.6.5 Configuring Load Balancing Based on the Link Weight 459
6.6.6 Configuring Load Balancing Based on the Link Priority 463
6.6.7 Configuring Load Balancing Based on the Number of Sessions 467
6.6.8 Configuring Load Balancing Based on Bandwidth and Sessions 471
6.6.9 Viewing Load Balancing Session Information 474
6.7 PPTP VPN 475
6.7.1 Overview 475
6.7.2 Configuring the PPTP Server 475
6.7.3 Viewing PPTP Tunnel Information 478
6.7.4 Performing PPTP VPN Client Management 479
6.8 L2TP VPN 480
6.8.1 Overview 480
6.8.2 Configuring the L2TP Server 481
6.8.3 Viewing L2TP Tunnel Information 488
6.8.4 Performing L2TP VPN User Management 489
6.9 SSL VPN 490
6.9.1 Overview 490
6.9.2 Creating an SSL VPN Gateway 491
6.9.3 Hardware Signature Management 503
6.9.4 Operation Monitoring 505
6.10 IPsec VPN 506
6.10.1 Overview 506
6.10.2 Principles 506
6.10.3 Configuring an IPsec Tunnel Using the Wizard 508

6.10.4 Custom Tunnel 528
6.10.5 Advanced Settings 544
6.10.6 Tunnel Monitoring 546
6.10.7 Viewing IPsec VPN Logs 548
6.11 DNS 548
6.11.1 Configuring DNS Server 548
6.11.2 Configuring DNS Transparent Proxy 550
6.11.3 Configuring DNS Proxy 557
6.11.4 Configuring DDNS 560
6.12 DHCP Management 562
6.12.1 Overview 562
6.12.2 Configuring a DHCP Server 562
6.12.3 Configuring a DHCP Relay Agent 569
6.12.4 Address Management List 571
6.13 PPPoE Server 572
6.13.1 Overview 572
6.13.2 PPPoE Server Configuration 573
6.13.3 PPPoE User Management 577
6.13.4 Viewing Online Users 579
6.14 Link Detection 581
6.14.1 Link Quality Detection 581
6.15 VRRP 586
6.15.1 Overview 586
6.15.2 Working Process 587

6.15.3 Configuring a VRRP Group 587
6.15.4 Viewing VRRP Logs 592
6.16 Neighbor Status 592
6.16.1 ARP Entries 592
6.16.2 ND Entries 593
6.16.3 LLDP 594
7 System Management 595
7.1 Administrators 595
7.1.1 Overview 595
7.1.2 Enabling Default Accounts 595
7.1.3 Creating an Administrator Account 596
7.1.4 Modifying the Administrator Password Security Policy 602
7.1.5 Modifying the Administrator Password 603
7.2 System Configuration 604
7.2.1 Setting System Time 604
7.2.2 Configuring SNMP 605
7.2.3 Configuring Service Parameters 608
7.2.4 Activating the License 614
7.2.5 Hardware Acceleration 616
7.3 Association Configuration 617
7.3.1 Identity System Association 617
7.3.2 Network Device Association 619
7.4 Log Configuration 622
7.4.1 Configuring the Syslog Server 622

7.4.2 Log Storage Management 625
7.5 Signature Library Upgrade 628
7.6 High Availability 630
7.6.1 Overview 630
7.6.2 Working Principle 630
7.6.3 Configuring High Availability 634
7.6.4 Viewing High Availability Status 641
7.7 Overload Protection 641
7.7.1 Configuring System Overload Protection 641
7.7.2 Displaying the System Overload Protection Status 643
7.8 Information Push 644
7.8.1 Overview 644
7.8.2 Setting the Logo Image 644
7.8.3 Editing Text Information 646
7.8.4 Enabling Information Push 648
7.9 System Maintenance 649
7.9.1 Viewing Device Information 649
7.9.2 Managing Configuration Backup 650
7.9.3 Upgrading the System 653
7.9.4 Installing Patches 657
7.9.5 Speed Test Mode 659
7.9.6 Restarting the Device 660
7.9.7 Restoring to Factory Settings 661
8 Operation Management 663

8.1 Viewing Authenticated Online Users 663
8.2 Security 664
8.2.1 Security Cockpit 664
8.2.2 Source Tracing 669
8.3 Log Monitoring Management 671
8.3.1 Log Overview 671
8.3.2 Querying Logs 671
8.4 Network 685
8.4.1 Traffic Monitoring 685
8.4.2 Session Monitoring 691
8.4.3 URL Ranking 697
8.5 Device Hardware Monitoring 697
8.6 Fault Diagnosis 700
8.6.1 Diagnostic Center 700
8.6.2 Device Self-Test 713
8.6.3 Ping 716
8.6.4 Tracert 717
8.6.5 Packet Obtaining Tool 718
8.6.6 One-Click Fault Information Collection 720
8.7 Report 721
8.7.1 Generating and Viewing Reports 721
9 Ruijie Cloud Connection 725
9.1 Overview 725
9.2 Connecting to Ruijie Cloud 726

9.2.1 Starting Ruijie Cloud 726
9.2.2 Binding Devices 726
9.3 Operations on Ruijie Cloud 726
9.3.1 Viewing Device Information 726
9.3.2 Managing Tunnels 727
9.3.3 Upgrading Device Software 728
9.3.4 Viewing Network Topology 729
10 FAQs 731
10.1 What Can I Do If I Fail to Log In to the Web Page? 731
10.2 What Can I Do If I Fail to Log In to the System Through SSH? 732

1 Overview

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

The CF 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 CF 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 or HTTP, the administrator can configure and manage firewalls on the UI.

Prerequisites

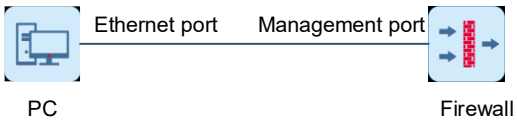
- The CF series firewall provides the default web configurations, as listed in Table 2-1. You can log in to the management page with the default values.

Table 2-1 Default Web Configurations

Item	Default Value
Web service	Enabled
Management port IP address	MGMT: 10.20.30.42/24 Ge0/0: 10.20.40.42/20
Username/Password	admin/admin
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.

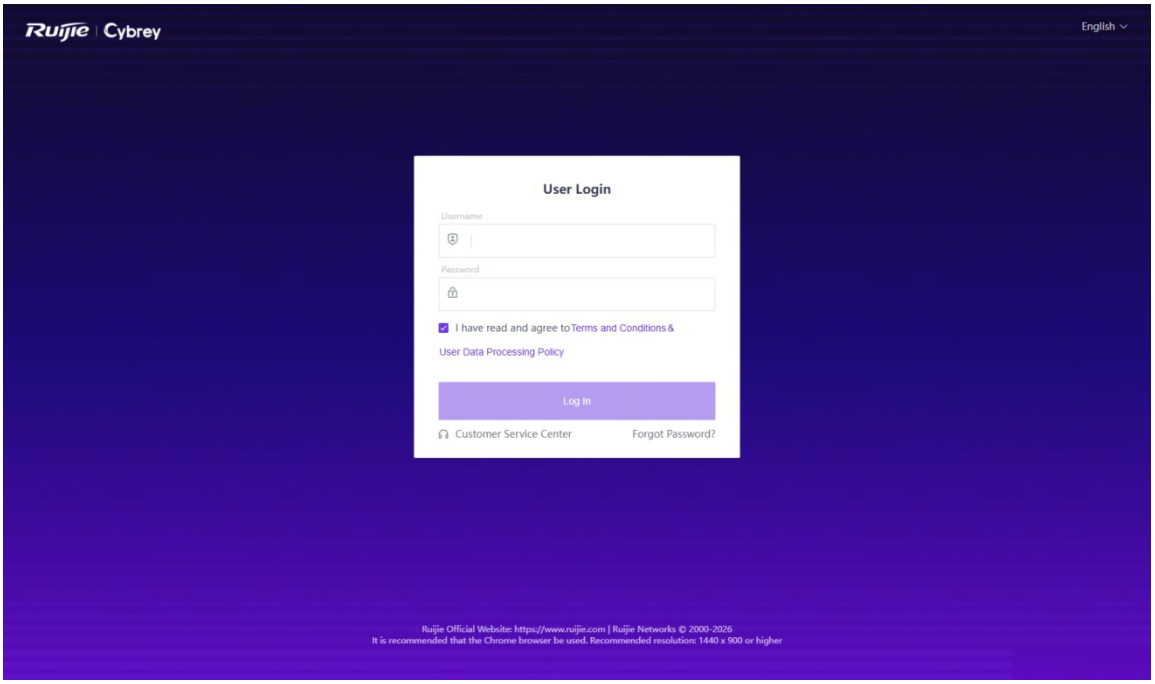


  - The DHCP server is enabled for port 0/MGMT by default so that the local NIC of the management PC can automatically obtain an IP address from and communicate with the firewall. No manual IP address configuration is required.
- The management PC meets relevant requirements on the browser and resolution.
  - 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://10.20.30.42 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.

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 UX Improvement Plan

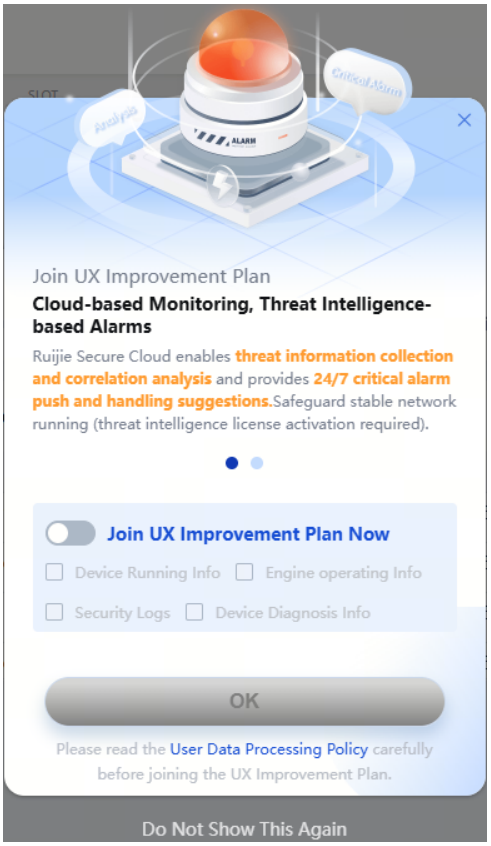
After you log in to the web UI, the system prompts you whether to join **UX Improvement Plan**.

Ruijie Security Cloud Platform (https://secloud1.ruijie.com.cn/) is a cloud-based O&M platform for devices. It delivers signature and software updates to devices, and also supports license activation and remote service monitoring. After a device joins **UX Improvement Plan**, you can configure the device to automatically upload operational data (such as device operational information and security logs) to the security cloud. Then, the cloud collects the data, analyzes the running status of the device and services, and pushes alarms and handling suggestions to users in a timely manner, improving the user experience.

Note

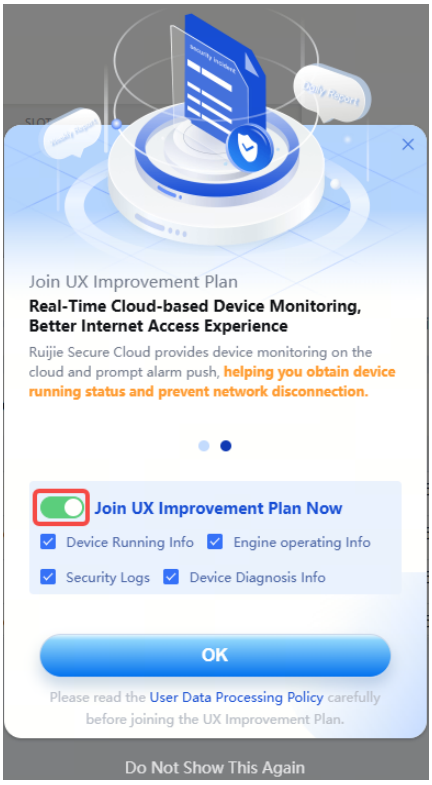
If you do not want to participate in **UX Improvement Plan** or be prompted again the next time you log in to the web UI, click **Do Not Show This Again**.

Figure 2-1 Prompt for Enabling UX Improvement Plan

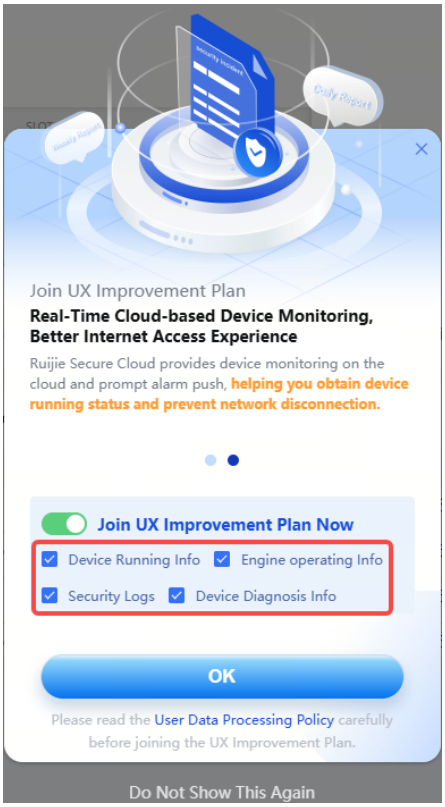


Procedure

(1) Join **UX Improvement Plan** as required. You can toggle on  to join the plan.



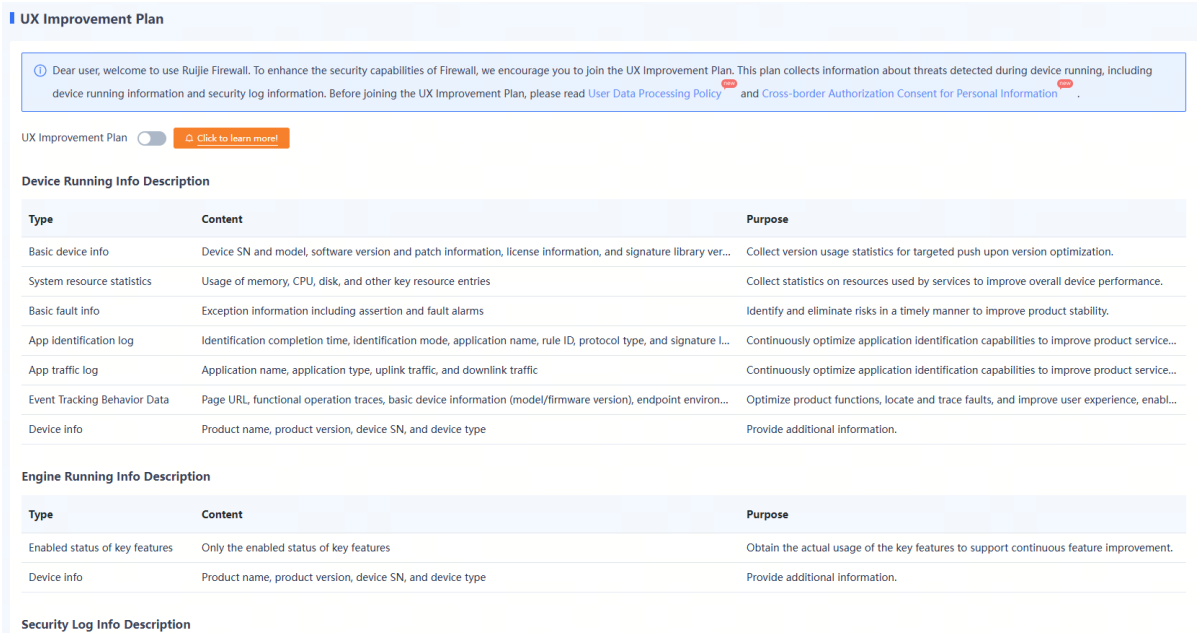
(2) Select the types of logs that can be sent to the cloud based on scenario requirements.



(3) Click **OK**.

Follow-up Procedure

- Choose **System** > **UX Improvement Plan** to view and modify the configuration of logs uploaded to the cloud.



UX Improvement Plan

Dear user, welcome to use Ruijie Firewall. To enhance the security capabilities of Firewall, we encourage you to join the UX Improvement Plan. This plan collects information about threats detected during device running, including device running information and security log information. Before joining the UX Improvement Plan, please read User Data Processing Policy and Cross-border Authorization Consent for Personal Information.

UX Improvement Plan Click to learn more!

Device Running Info Description

Type	Content	Purpose
Basic device info	Device SN and model, software version and patch information, license information, and signature library ver...	Collect version usage statistics for targeted push upon version optimization.
System resource statistics	Usage of memory, CPU, disk, and other key resource entries	Collect statistics on resources used by services to improve overall device performance.
Basic fault info	Exception information including assertion and fault alarms	Identify and eliminate risks in a timely manner to improve product stability.
App identification log	Identification completion time, identification mode, application name, rule ID, protocol type, and signature I...	Continuously optimize application identification capabilities to improve product service...
App traffic log	Application name, application type, uplink traffic, and downlink traffic	Continuously optimize application identification capabilities to improve product service...
Event Tracking Behavior Data	Page URL, functional operation traces, basic device information (model/firmware version), endpoint environ...	Optimize product functions, locate and trace faults, and improve user experience, enabl...
Device info	Product name, product version, device SN, and device type	Provide additional information.

Engine Running Info Description

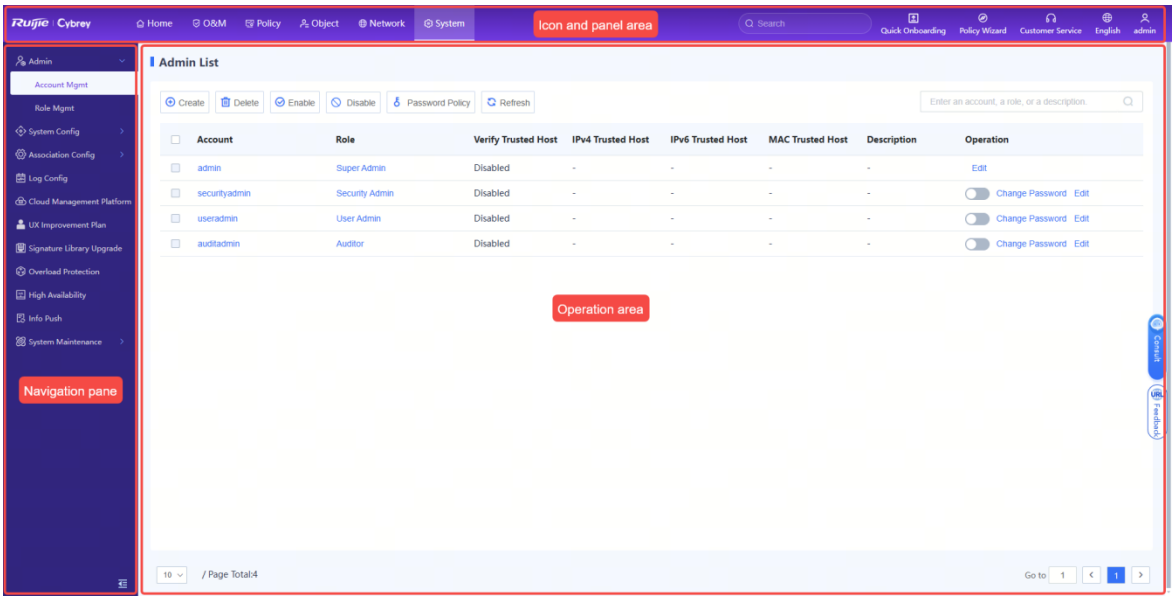
Type	Content	Purpose
Enabled status of key features	Only the enabled status of key features	Obtain the actual usage of the key features to support continuous feature improvement.
Device info	Product name, product version, device SN, and device type	Provide additional information.

Security Log Info Description

2.3 Web UI Layout

After login, the web UI is displayed, as shown in Figure 2-2.

Figure 2-2 Web UI Layout



Area	Description
Icon and panel area	This area displays the company logo, device name, and function panel. This area supports 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.

2.4 Operations on the Web UI

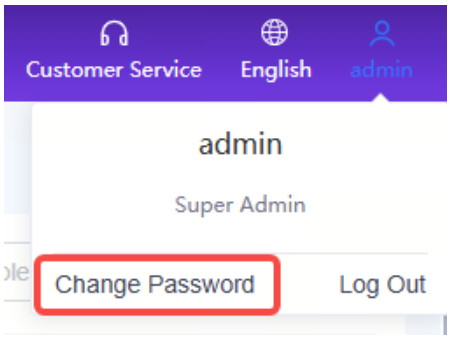
2.4.1 Changing Login User Password

Application Scenario

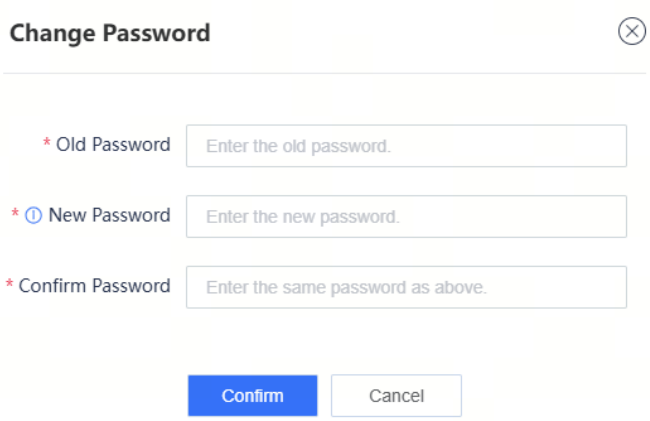
After login using a default account, change your password to ensure account security.

Procedure

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



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



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: 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.

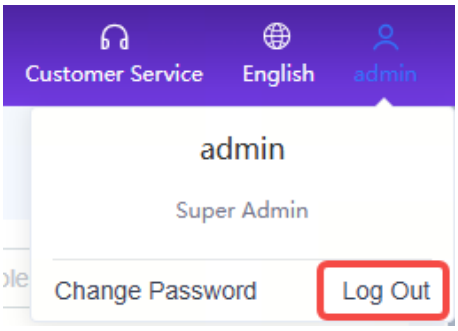
2.4.2 Logging Out

Application Scenario

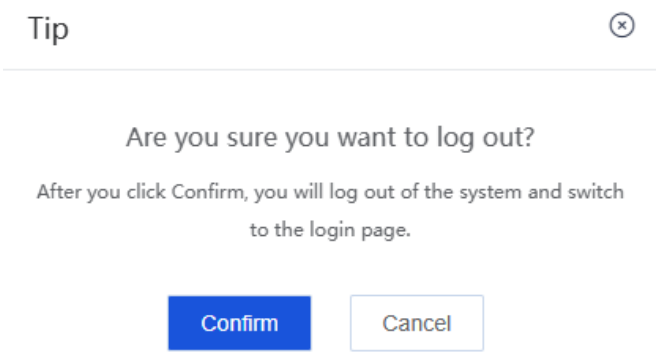
If no operation is performed on the web UI within a period of time, the administrator should log out to ensure account security.

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.

2.4.3 Resetting the Password

Application Scenario

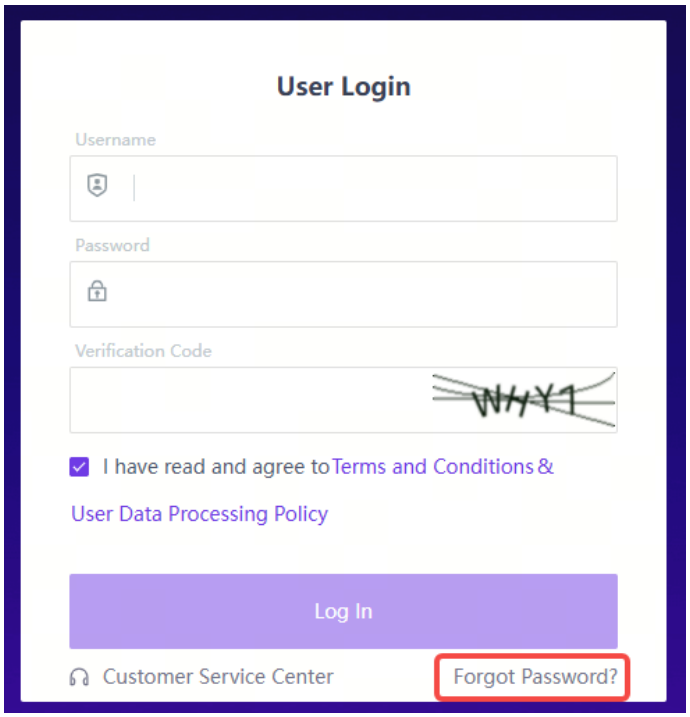
Reset the password if you forget the login password of the device.

Prerequisites

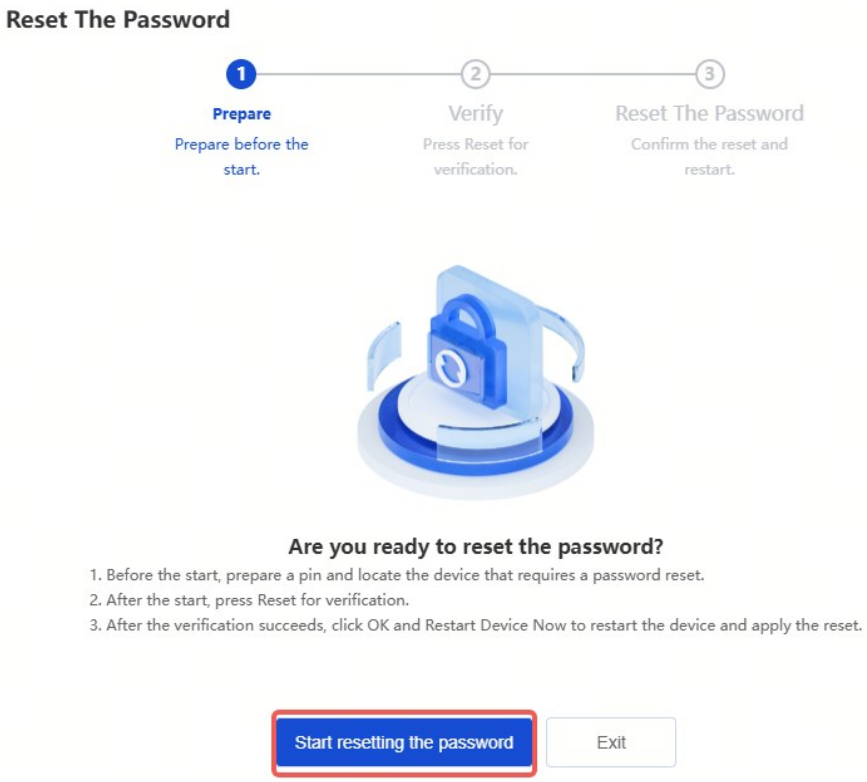
The device for which the password needs to be reset is ready.

Procedure

(1) On the login page of the web UI, click **Forgot Password?** in the lower right corner.

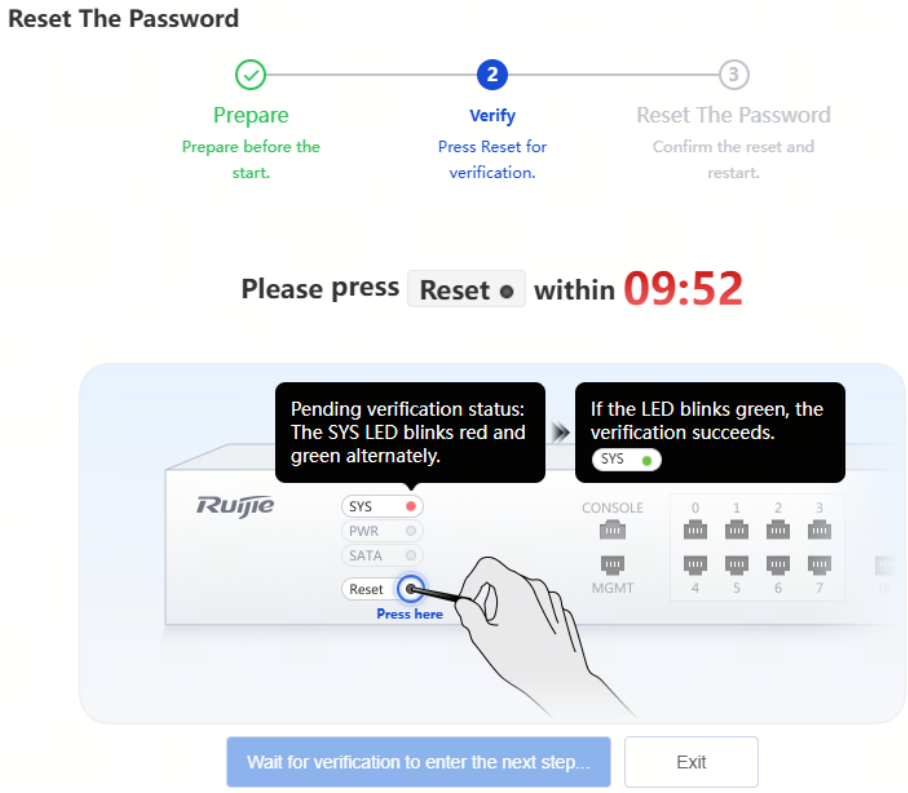


(2) On the **Reset The Password** page, click **Start resetting the password**.



(3) Press the Reset button on the device within 10 minutes according to the prompt on the page.

If the operation is not complete within 10 minutes, an operation timeout message is displayed, and the verification needs to be performed again.



(4) After the verification is complete on the device, the reset default username and password are displayed on the web page. Click **OK and Restart Device Now** to restart the device. After the restart, the login password of the web UI is successfully reset.

2.4.4 Version Upgrade Prompt

Application Scenario

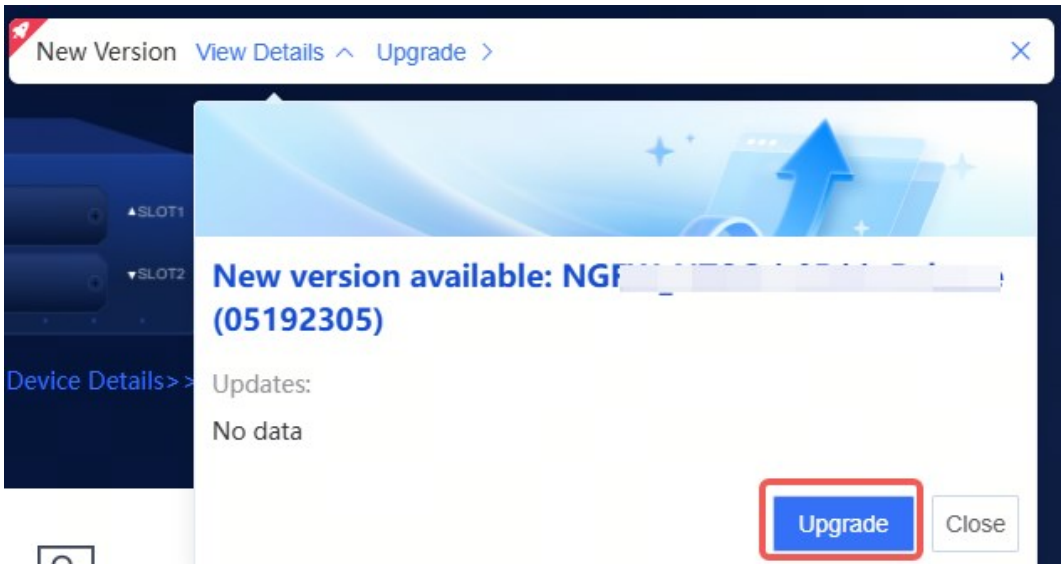
If the recommended version is updated, a new version prompt is automatically displayed upon web UI login for you to quickly obtain version update information and upgrade the device on the web UI.

Prerequisites

- The device has connected to Ruijie Security Cloud Platform.
- If device information has been reported upon device onboarding and the device is not restarted, the cloud pushes version prompt information only when the recommended version is updated.
- If a device is restarted, the cloud pushes version prompt information regardless of whether the recommended version is updated.

Procedure

(1) Click **Upgrade** to go to the **System Upgrade** page. For details about upgrade steps, see 7.9.3 Upgrading the System.



(2) Click **Close** to hide new version details and display only the brief new version prompt. Click **View Details** to expand version details.

(3) Click **X** in the upper right corner of the **New Version** pop-up window to close it. The system will not display the pop-up window again during this login session and will prompt you again upon your next login to the web UI.



2.4.5 Configuring a Homepage Card

Application Scenario

You can customize card information to be displayed on the homepage of the web UI and flexibly configure the monitoring view based on O&M requirements. In this way, key information is displayed in a visualized manner for quick access.

The system provides a variety of card types for selection. Major card types are as follows:

- Device and license management: device panel, basic license, and security capability license
- Security trend awareness: alarm events, recent attack events, attack trend, trend of being attacked, attack type, attack sources and attacked hosts, and threat intelligence
- Network performance monitoring: new session rate, concurrent sessions, and traffic monitoring
- Traffic analysis and ranking: top 5 apps by real-time traffic, top 5 users by real-time traffic, and top 5 IP addresses by real-time traffic
- Remote access monitoring: SSL VPN monitoring
- Short-cut operations: quick link to functions and policy optimization

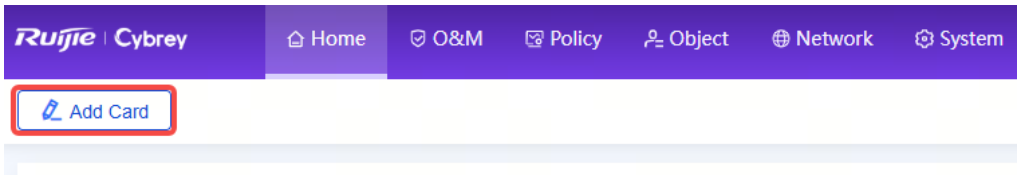
You can flexibly combine the cards to display key information such as the device status, security threats, and network traffic on one screen, improving O&M efficiency.

Note

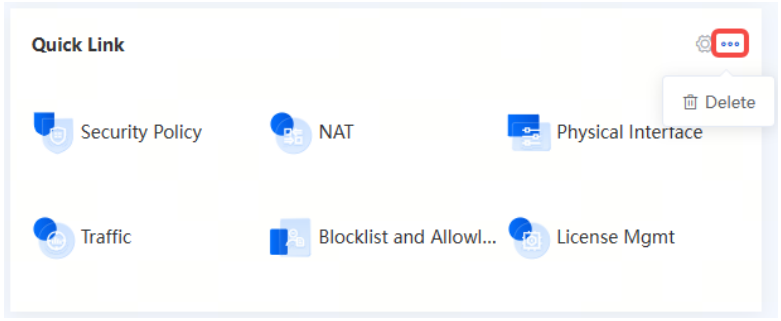
The card types actually supported by the device prevails.

Procedure

- Adding a card: Click **Add Card** in the upper left corner of the web homepage. In the dialog box that is displayed, select the card to be added.



- Deleting a card: Click the ... icon in the upper right corner of a card and select **Delete**.



- Adjusting the card position: Press and hold the left mouse on a card to drag the card to the desired position.

3 Quick Deployment

3.1 Deployment Planning

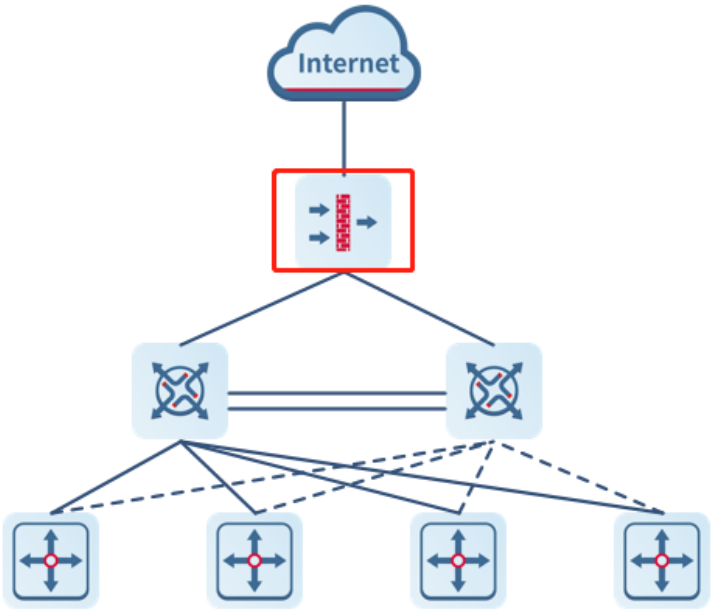
3.1.1 Planning Device Locations and IP Addresses

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

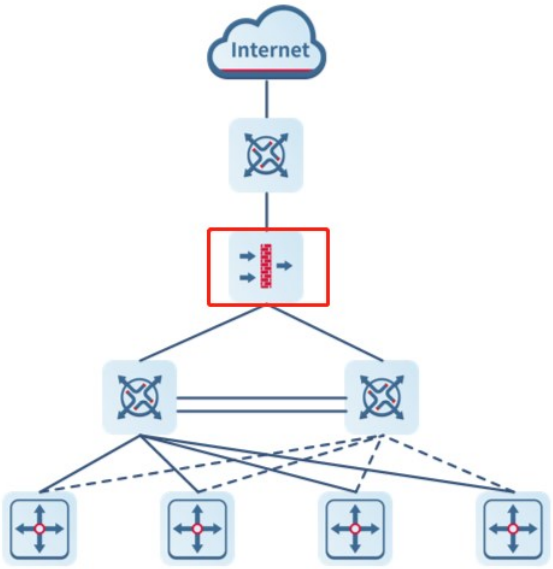
3.1.2 Planning Networking Mode

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

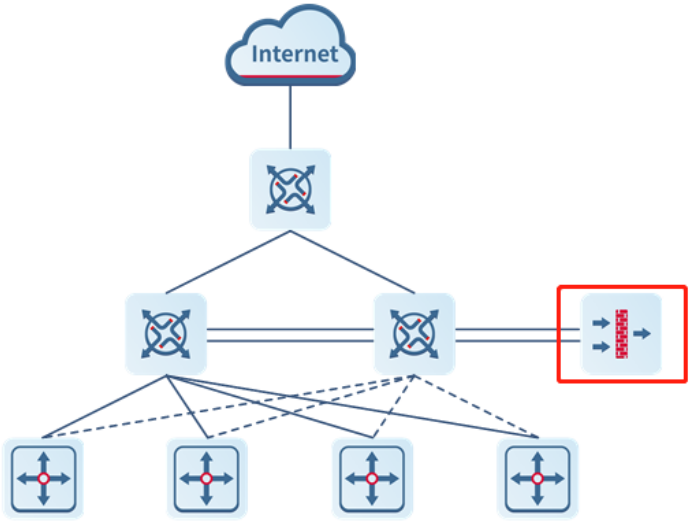
- At the network egress: Select the routing mode for the firewall to provide both security defense and some router functions, such as network address translation (NAT) and multi-ISP network access. Before configuring the routing mode, verify the Internet access mode. If the access mode is not configured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

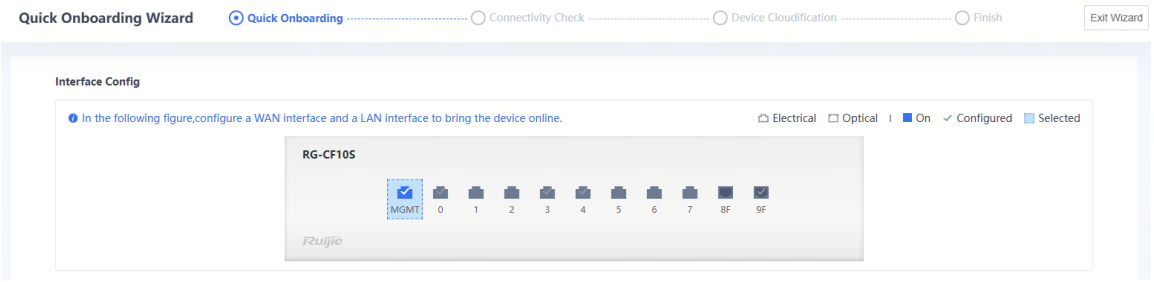
Prerequisites

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

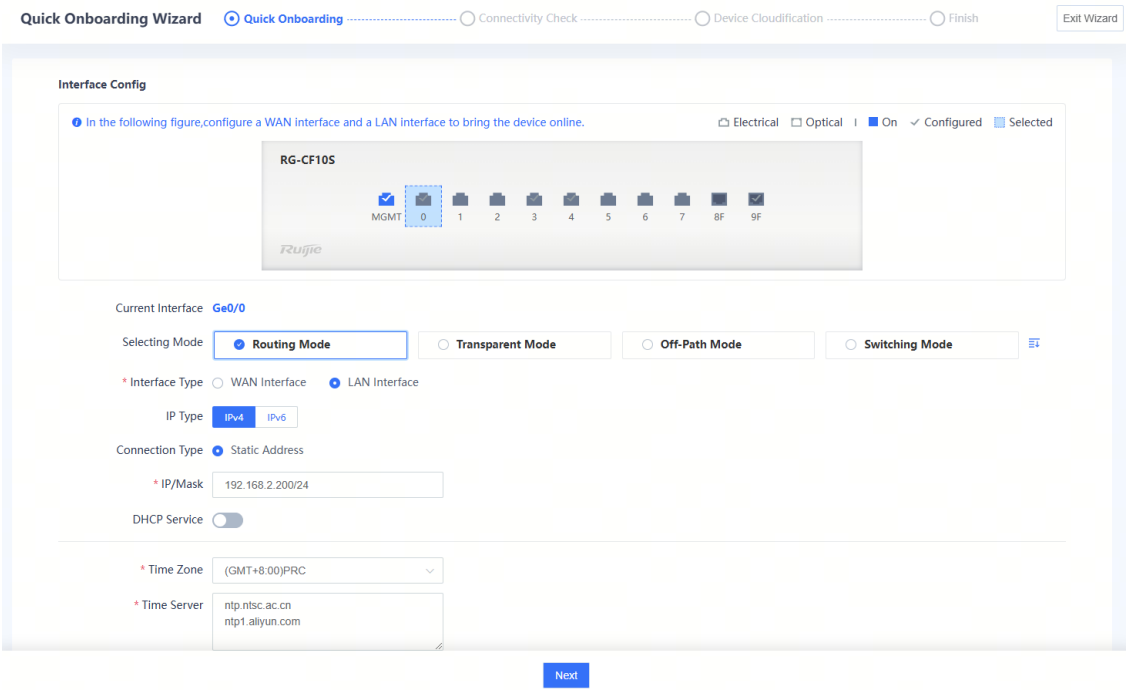
Procedure

(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 Select the interface that functions as the LAN interface.

b Set **Selecting Mode** to **Routing Mode**.

c Set parameters for the LAN interface.

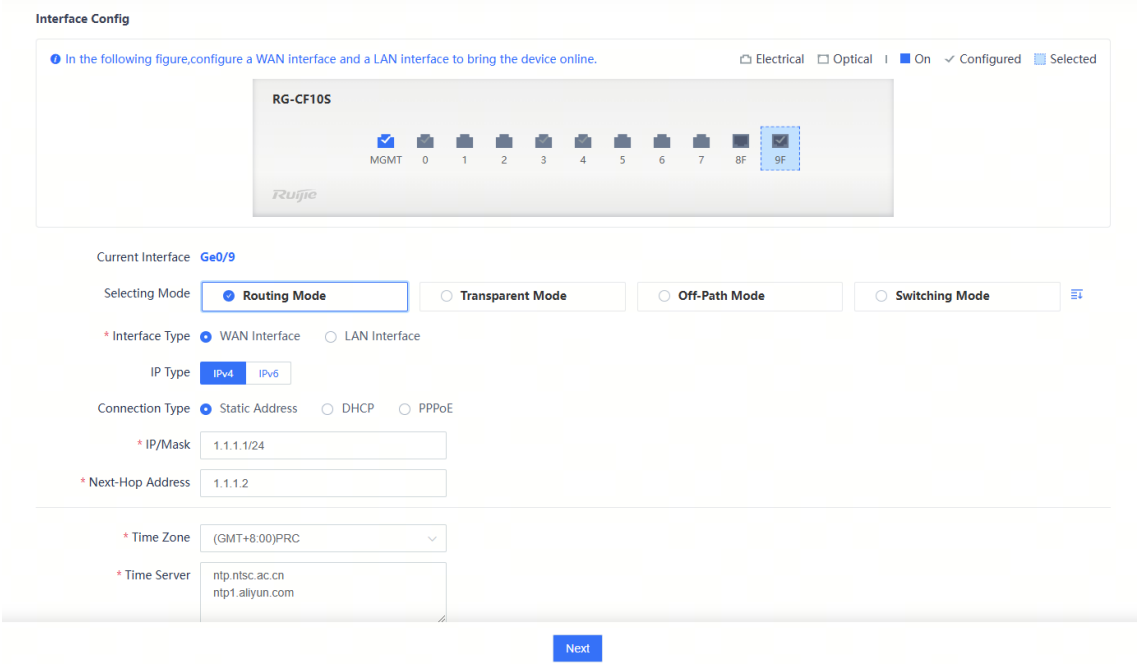
Item	Description	Remarks
Interface Type	**LAN Interface:** applicable for connection to LAN devices, such as PCs, switches, and printers.	[Example] LAN Interface
IP Type	Set the interface address type based on the network environment. Valid values: **IPv6** and **IPv4**. Both IPv4 and IPv6 addresses can be configured for an interface.	[Example] IPv4
IP Type: IPv4		
Connection Type	Connection type of the interface. The options are as follows: **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 Service	Whether the DHCP server function is enabled on the interface to assign IPv4 addresses to connected devices.	This parameter is available when **Connection Type** of the LAN interface is set to **Static Address**. [Example] Enable
IP Assignment Range	Set the range of IP addresses that can be assigned to downstream DHCP clients.	Configure this parameter when the DHCP service is enabled. Enter an IP address range per line. Use a hyphen (-) between two IP addresses to specify a range. [Example] 192.168.110.17-192.168.110.254
Primary DNS Server	Set the primary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 192.168.10.1
Secondary DNS Server	Set the secondary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 192.168.10.2
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

Item	Description	Remarks
Connection Type	Connection type of the interface. The options are as follows: **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. **DHCP**: The interface automatically obtains an IPv6 address through DHCP. **Prefix Delegation**: An IPv6 address is automatically generated for the interface using the prefix pool obtained through DHCPv6 prefix delegation (PD). This option applies to the scenario where the device functions as a DHCPv6 client and dynamically obtains an IPv6 address prefix pool from the upstream DHCPv6 server. DHCPv6 PD needs to be enabled on the WAN interface of the device for this option to take effect.	The connection type of a LAN interface can be set to DHCPv6 PD only when DHCPv6 PD has been configured on the WAN interface of the device and the device has applied for an IPv6 address prefix pool from the DHCPv6 server. When the connection type of a LAN interface is set to **Prefix Delegation**, RA is automatically enabled. In this case, the downstream terminals connected to the LAN interface can automatically obtain IPv6 addresses through Stateless Address Autoconfiguration (SLAAC). [Example] Static Address
Prefix Pool ID	Bind the prefix pool ID applied by the WAN interface. The IPv6 address prefix pool applied by the WAN interface has a unique ID, and a LAN interface needs to bind to a prefix pool ID for generating IPv6 addresses.	You need to set this parameter only when **Connection Type** is set to **Prefix Delegation**.
IP/Prefix Length	If the connection type of an interface is set to **Static Address**, this parameter needs to be set to specify the IPv6 address and prefix length of the interface. If the connection type of an interface is **Prefix Delegation**, this parameter is used to configure the IPv6 address bound to DHCPv6 PD. The device generates the IPv6 address of the interface by combining the obtained prefix and the configured IPv6 address. The prefix length must be 64 bits.	[Example] 2000::1/96

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
DHCP Service	Whether the DHCPv6 server function is enabled on the interface to assign IPv6 addresses to connected devices.	This parameter is available when IPv6 is enabled for the LAN interface and **Connection Type** of the LAN interface is set to **Static Address**. [Example] Enabled
Primary DNS Server	Set the primary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 2001::1
Secondary DNS Server	Set the secondary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 2001::2

(3) Configure the WAN interface.



a Select the interface that functions as the WAN interface.

b Set **Selecting Mode** to **Routing Mode**.

c Set parameters for the WAN interface.

Note

If you configure a cellular interface as the WAN interface, complete the configuration according to 6.1.9 Configuring a Cellular Interface.

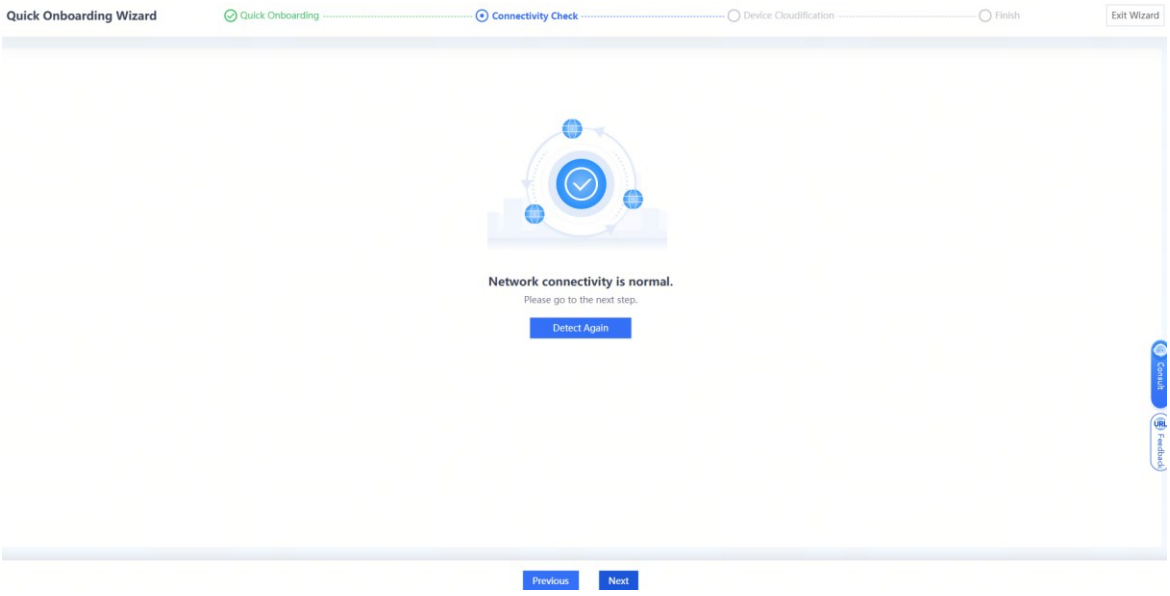
Item	Description	Remarks
Interface Type	**WAN Interface**: is used to connect the firewall to the Internet. Typically, the WAN interface is directly connected to the fiber-to-the-home (FTTH) Optical Network Terminal (ONT) of the ISP.	[Example] WAN Interface
IP Type	Set the interface address type based 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		
Connection Type	Connection type of the interface. The options are as follows: **Static Address**: Applicable when the network administrator specifies an IP address for the device based on the predefined IP address planning. This connection type requires the network administrator to possess 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.	[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
Next-Hop Address	IP address of the next-hop node to reach the destination address.	You need to set this parameter when **Connection Type** is set to **Static Address**. [Example] 192.168.20.2
Account/ Password	Username and password for dialup access. Typically, they are assigned by an ISP.	You need to set this parameter when **Connection Type** is set to **PPPoE**.
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: **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. **DHCP**: The interface automatically obtains an IPv6 address through DHCP. **PPPoE**: The interface functions as an IPv6 PPPoE client and obtains an IPv6 address from the IPv6 PPPoE server.	[Example] Static Address
Account/ Password	Username and password for dialup access. Typically, they are assigned by an ISP.	You need to set this parameter when **Connection Type** is set to **PPPoE**.

Item	Description	Remarks
IP/Prefix Length	IPv6 address and prefix length of the interface.	You need to set this parameter when **Connection Type** is set to **Static Address.** [Example] 2001:1::1/64
Next-Hop Address	IP address of the next node for forwarding data.	You need to set this parameter when **Connection Type** is set to **Static Address**. [Example] 2003::1
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

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

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



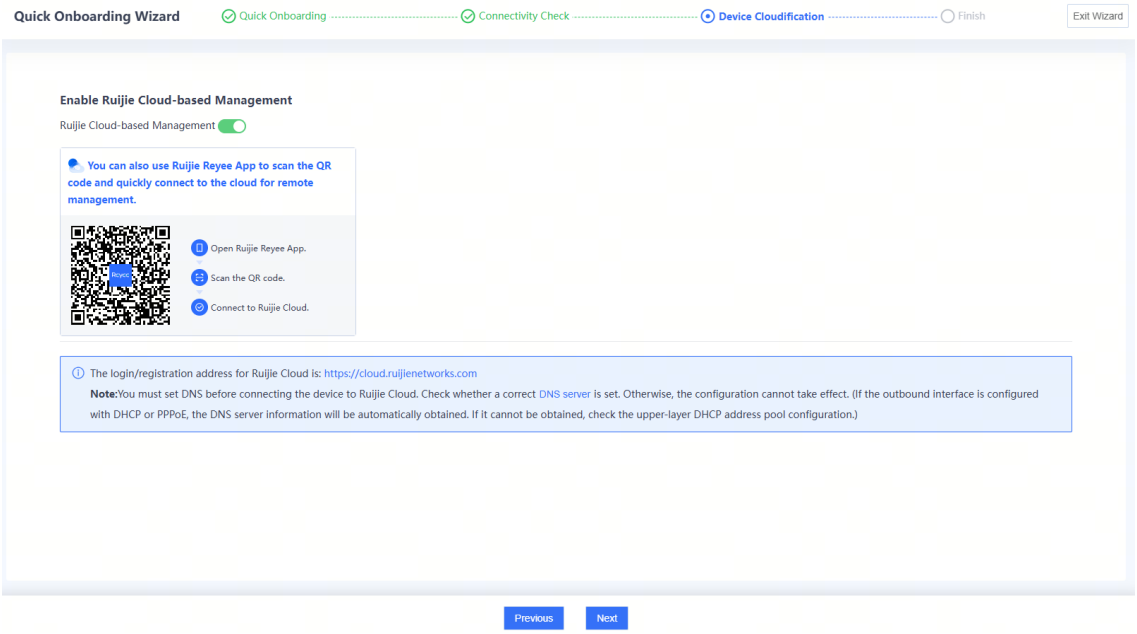
Note

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

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

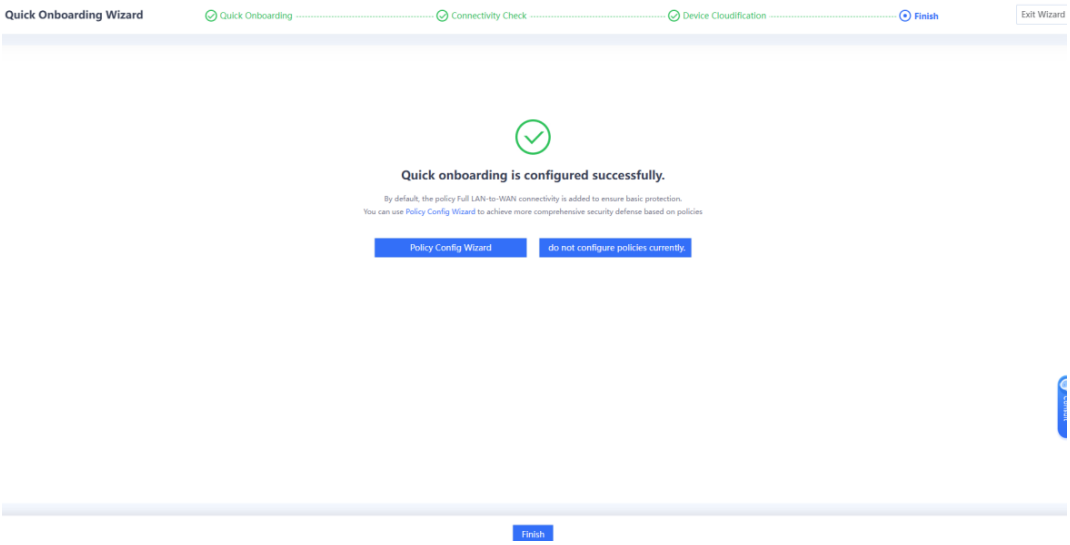
Note

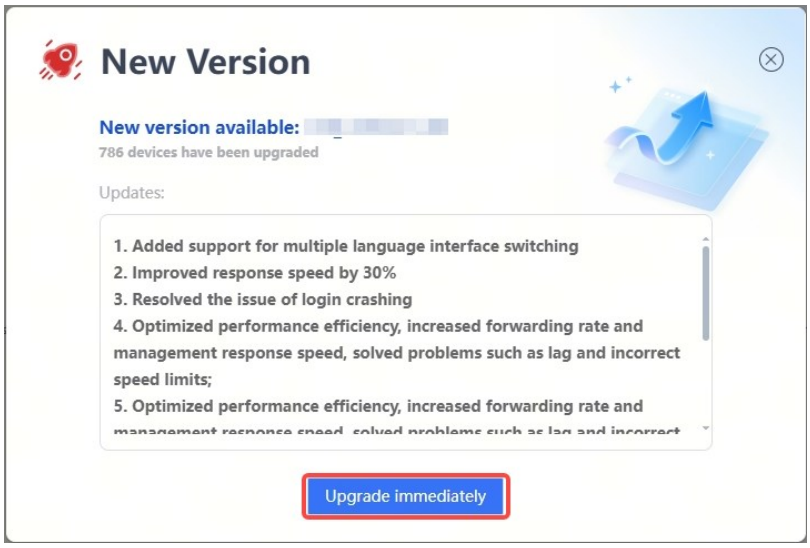
If the device cannot connect to the Internet, connect it to the cloud management platform according to 9 Ruijie Cloud Connection.



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

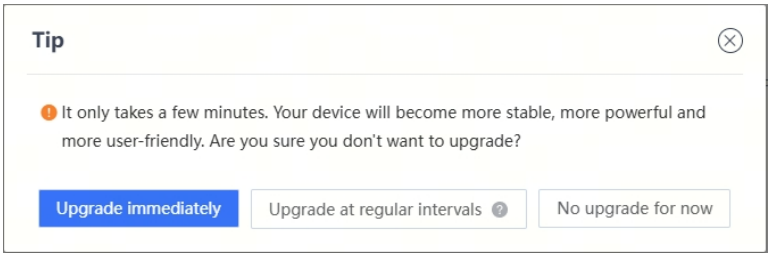
If the device can normally access Ruijie Security Cloud Platform and a new version is available on the cloud, the system automatically displays the **New Version** window. You can click **Upgrade immediately** to upgrade the version.





Note

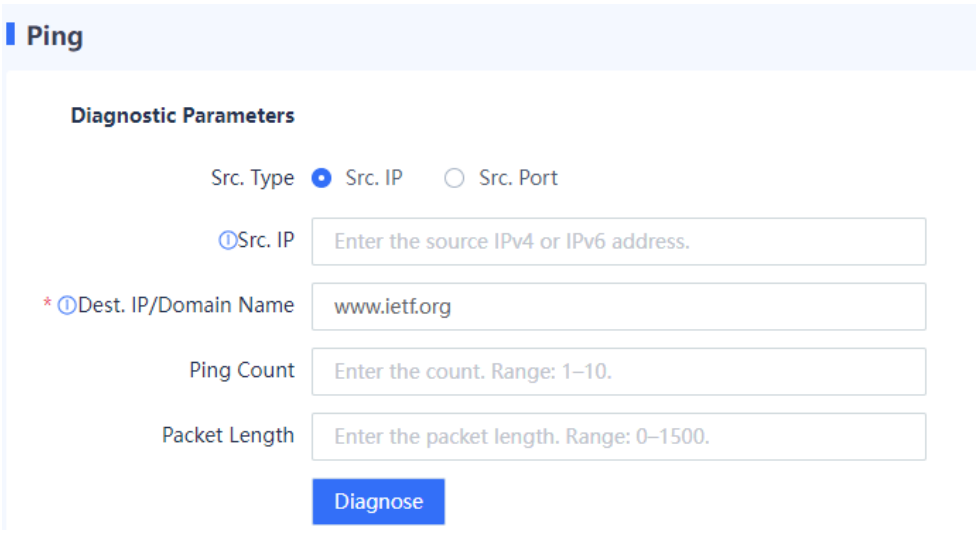
If the upgrade operation cannot be executed immediately, click **x** to close the pop-up window. Then, click **Upgrade at regular intervals** in the **Tip** window that is displayed in later steps and specify an interval for periodic upgrade of the system version. After that, the system pre-downloads the version file to the local device and performs version upgrade and restart at the specified time.



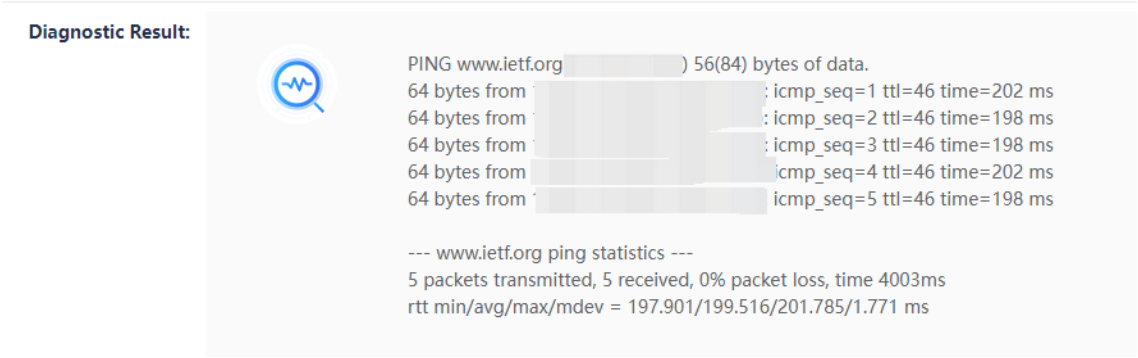
Verification

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

Figure 3-1 Ping Example



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



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.

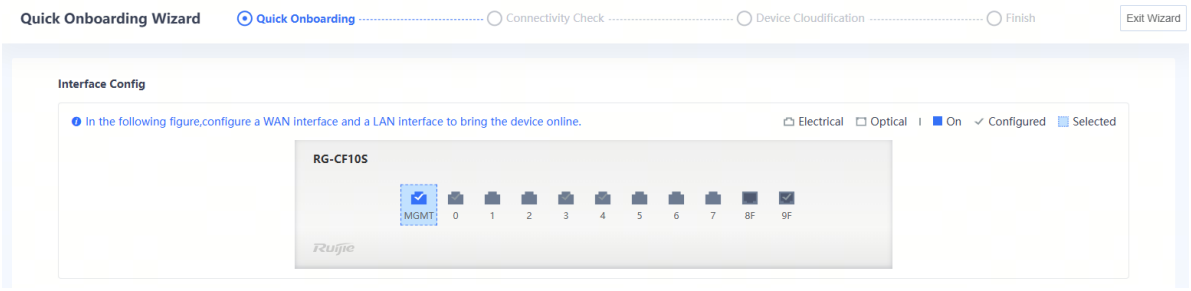
Note

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

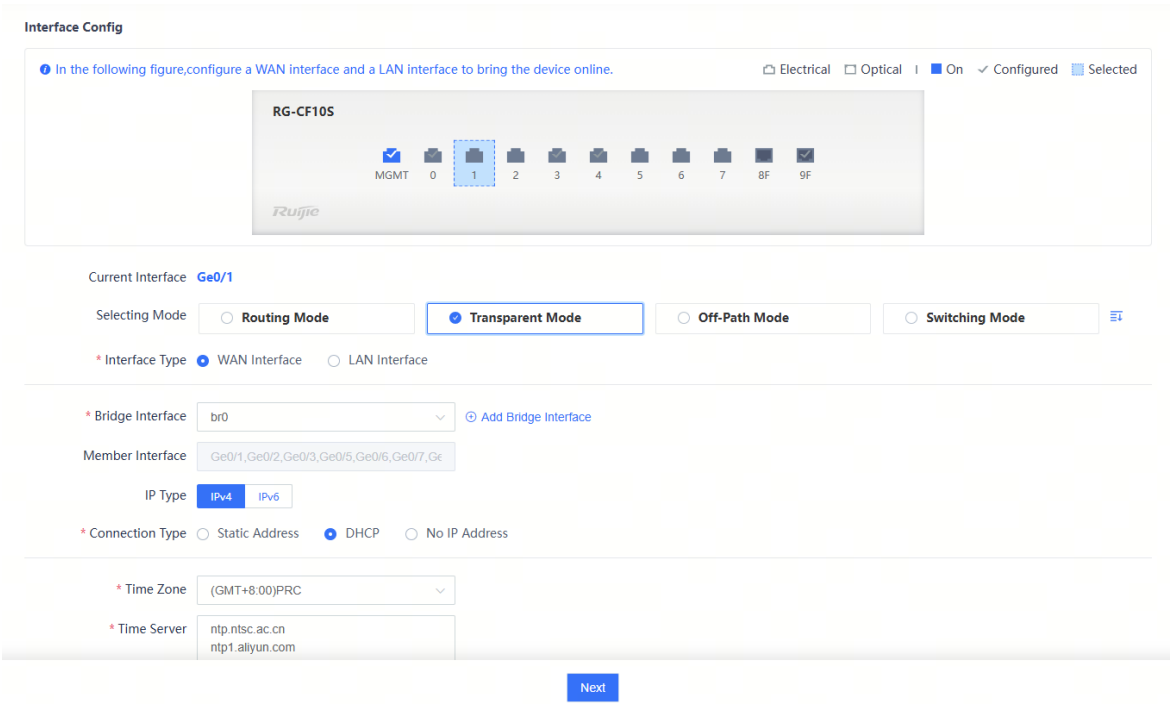
Procedure

(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.

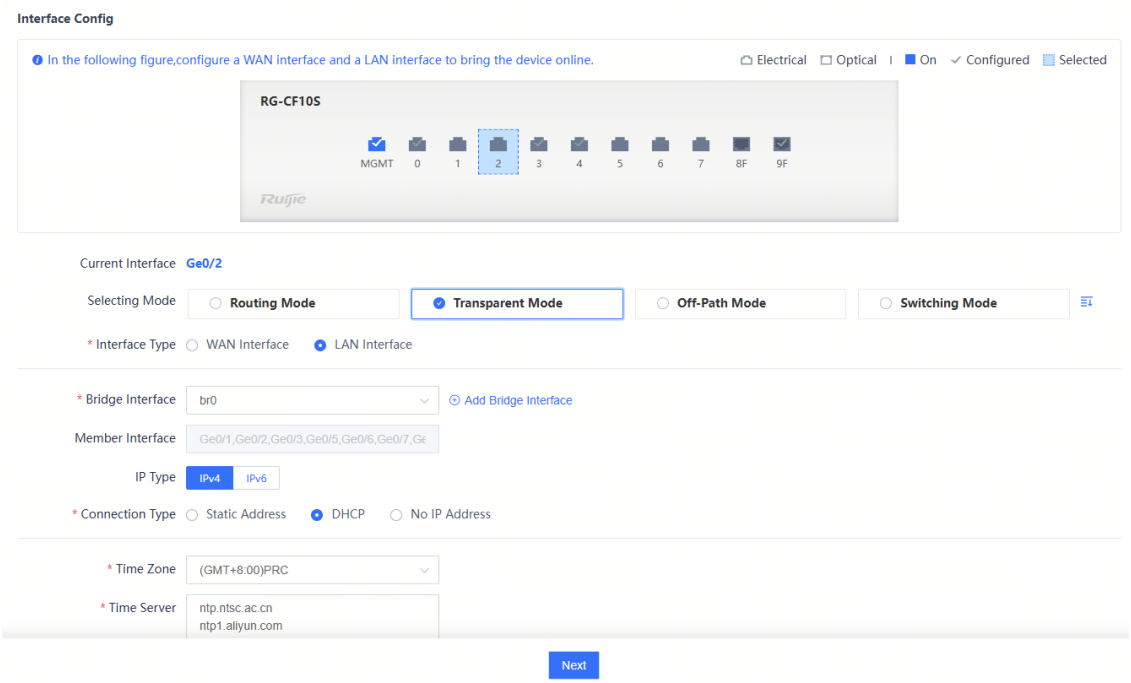


a Select the interface that functions as the WAN interface.

b Set **Selecting Mode** to **Transparent Mode**.

c Set **Interface Type** to **WAN Interface**.

(3) Configure the LAN interface.



a Select the interface that functions as the LAN interface.

b Set **Selecting Mode** to **Transparent Mode**.

c Set **Interface Type** to **LAN Interface**.

(4) Configure a bridge interface.

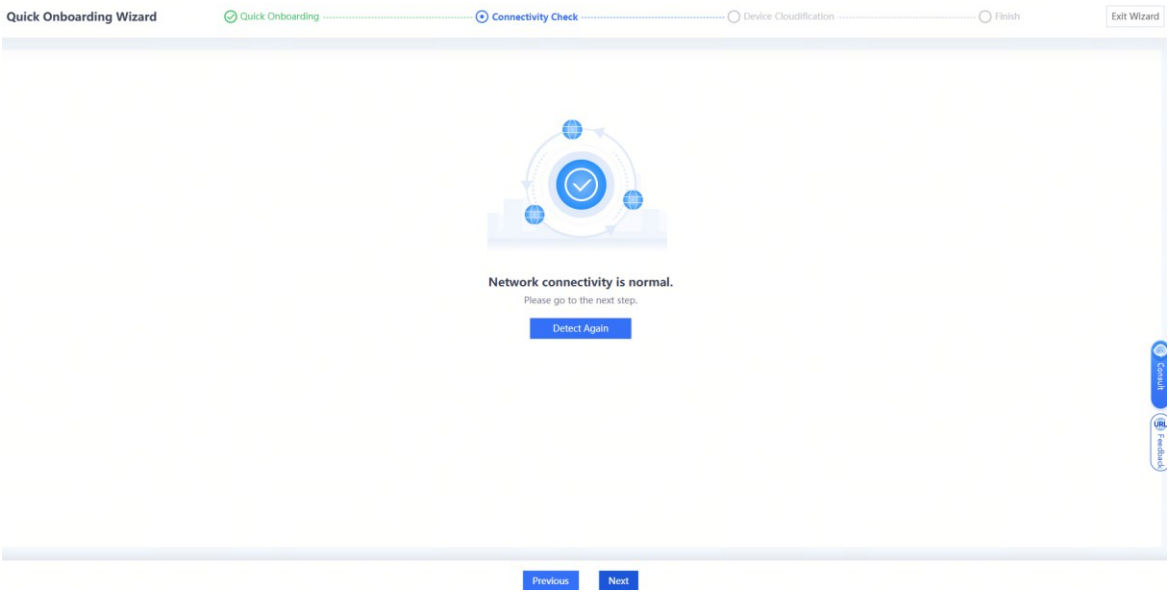
a Set parameters for the bridge interface.

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, see6.1.3 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] Ge0/1,Ge0/2

Item	Description	Remarks
Connection Type	Connection type of the interface. The options are as follows: **Static Address**: Applicable when the network administrator specifies an IP address for the device based on the predefined IP address planning. This connection type requires the network administrator to possess 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. **No IP Address**: Applicable when no IP address needs to be configured for the bridge interface. In this mode, you cannot access or manage the device through the bridge interface. Therefore, ensure that another management channel (for example, the IP address of another interface) has been configured for accessing the device.	[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	IP address of the next-hop node to reach the destination address.	You need to set this parameter when **Connection Type** is set to **Static Address**. [Example] 192.168.20.2

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

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



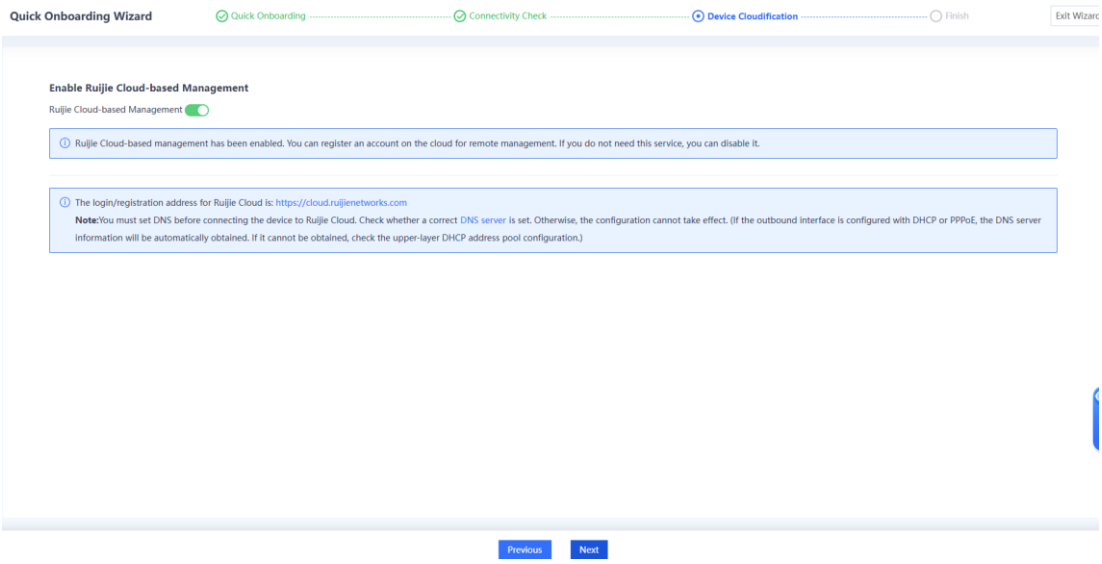
Note

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.

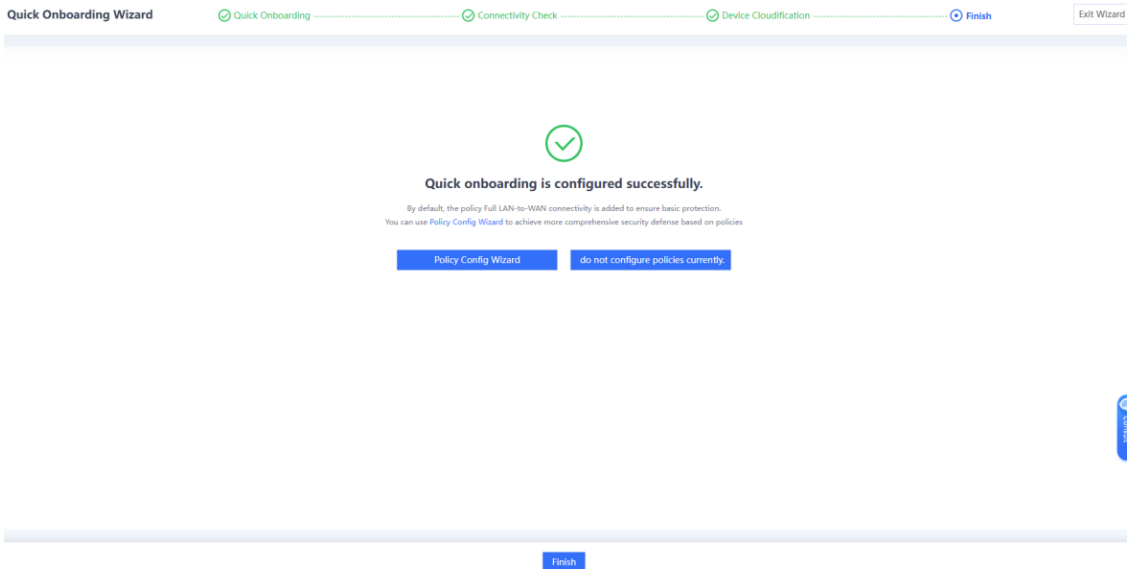
Note

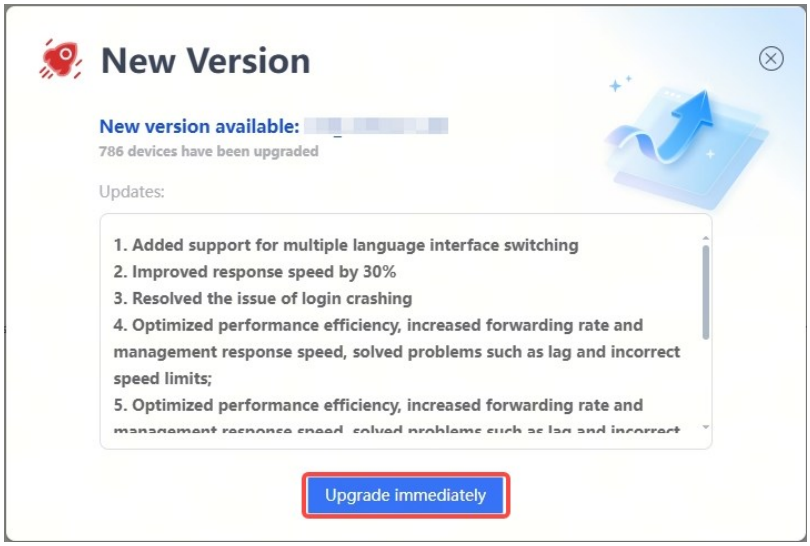
If the device cannot connect to the Internet, connect it to the cloud management platform according to 9 Ruijie Cloud Connection.



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

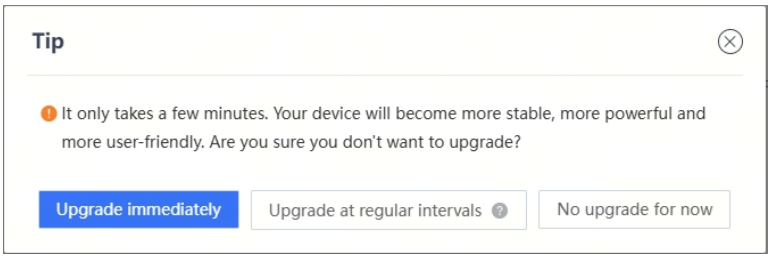
If the device can normally access Ruijie Security Cloud Platform and a new version is available on the cloud, the system automatically displays the **New Version** window. You can click **Upgrade immediately** to upgrade the version.





Note

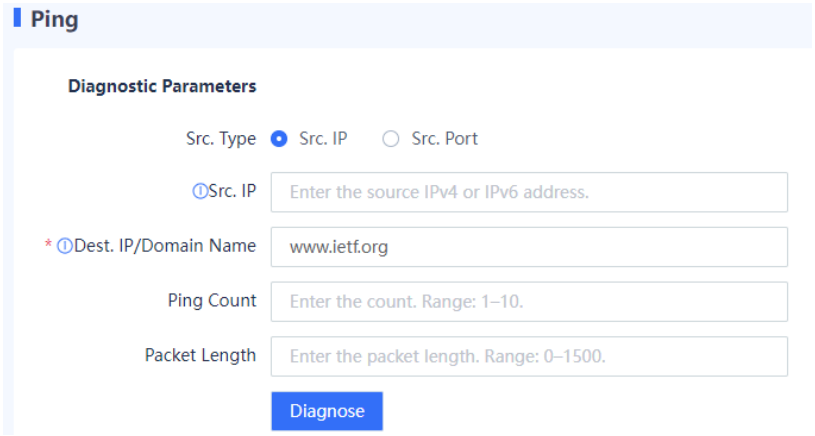
If the upgrade operation cannot be executed immediately, click **x** to close the pop-up window. Then, click **Upgrade at regular intervals** in the **Tip** window that is displayed in later steps and specify an interval for periodic upgrade of the system version. After that, the system pre-downloads the version file to the local device and performs version upgrade and restart at the specified time.



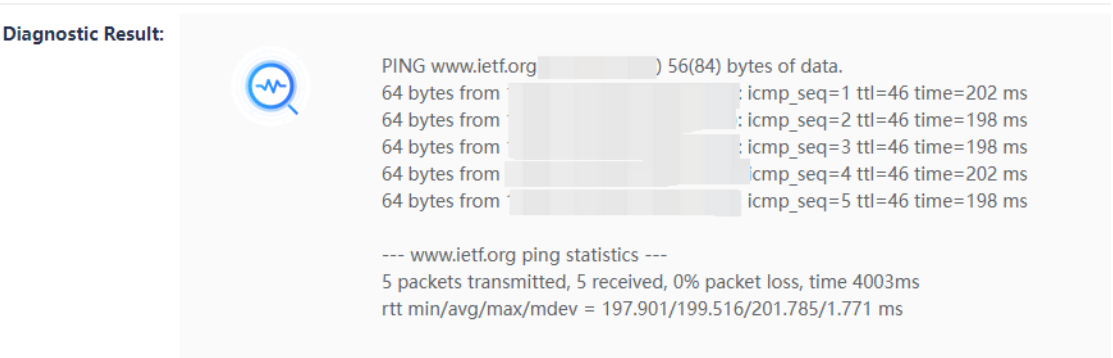
Verification

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

Figure 3-2 Ping Example



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



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 external network (for example, through a core switch) and configured the IP address and next-hop address for the port to enable external network connectivity.

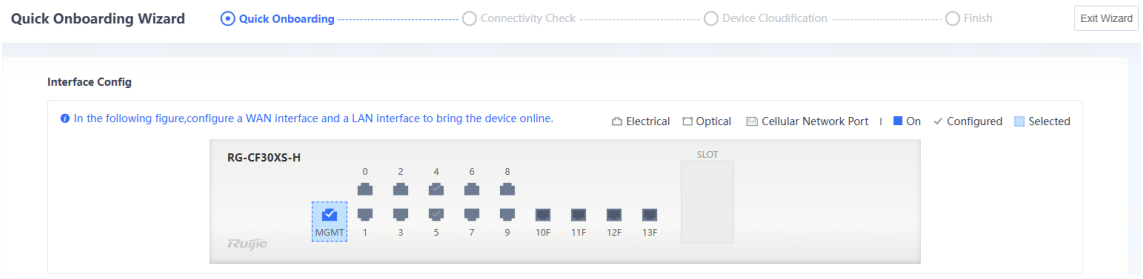
Note

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

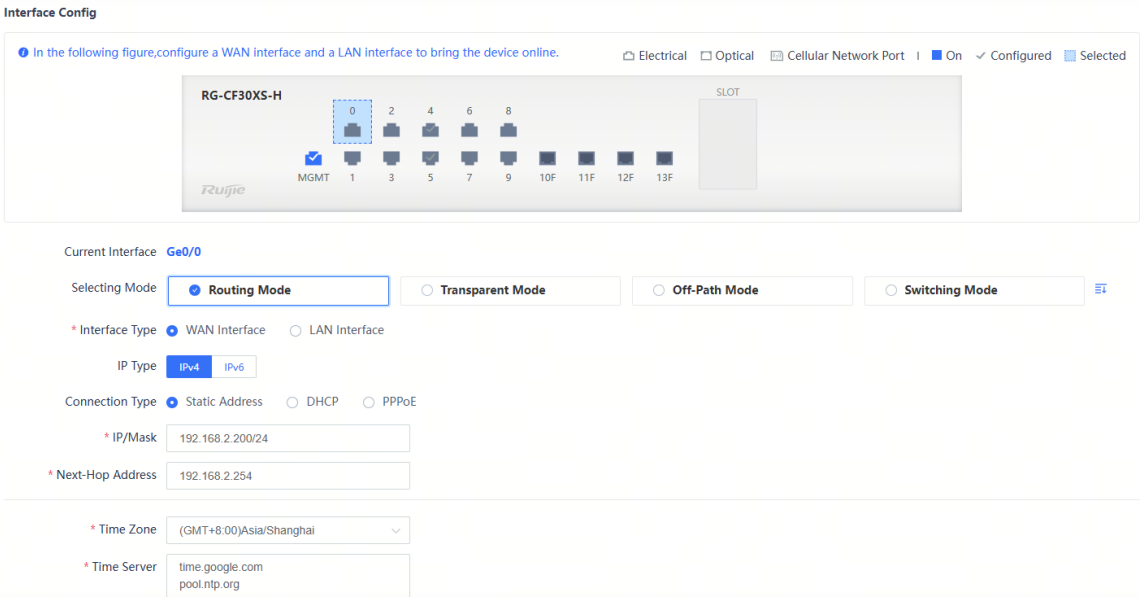
Procedure

(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.

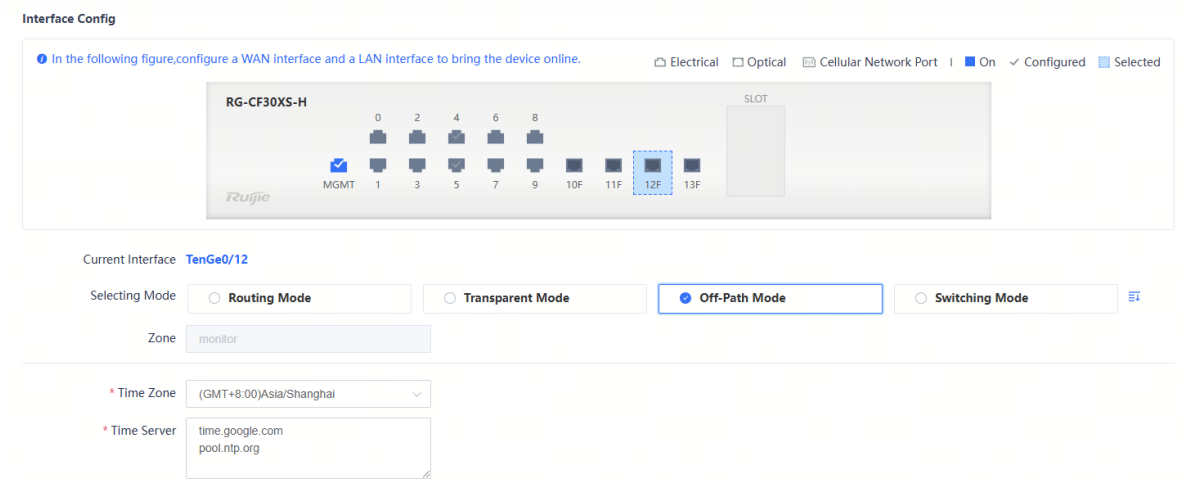


a Click port Ge0/0.

b Set **Selecting Mode** to **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.



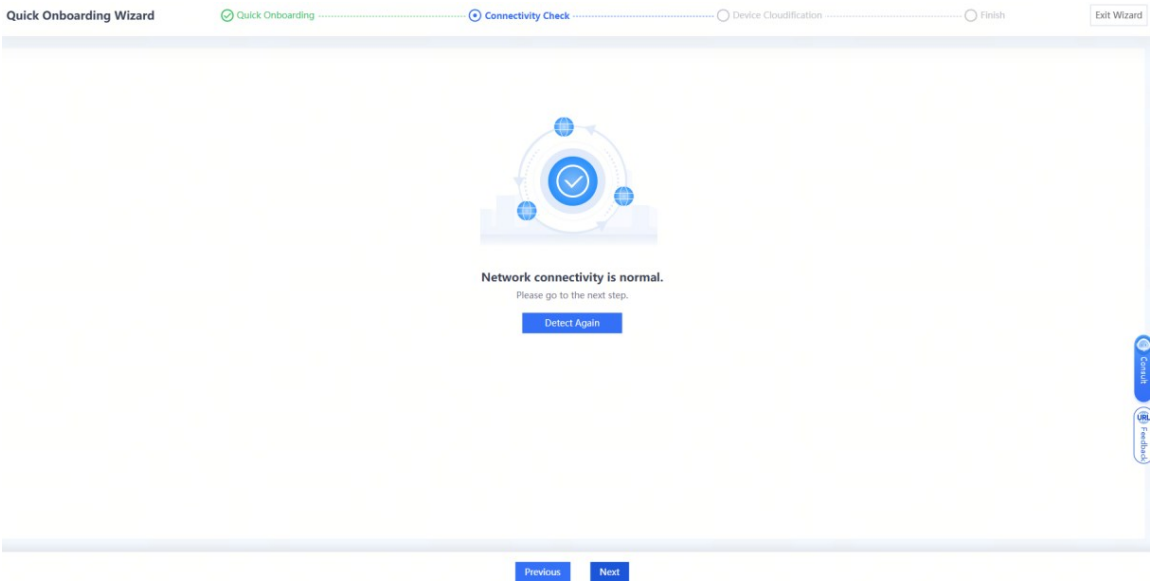
a Select the interface that functions as the off-path interface for connecting to a switch.

b Set **Selecting Mode** to **Off-Path Mode**.

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.

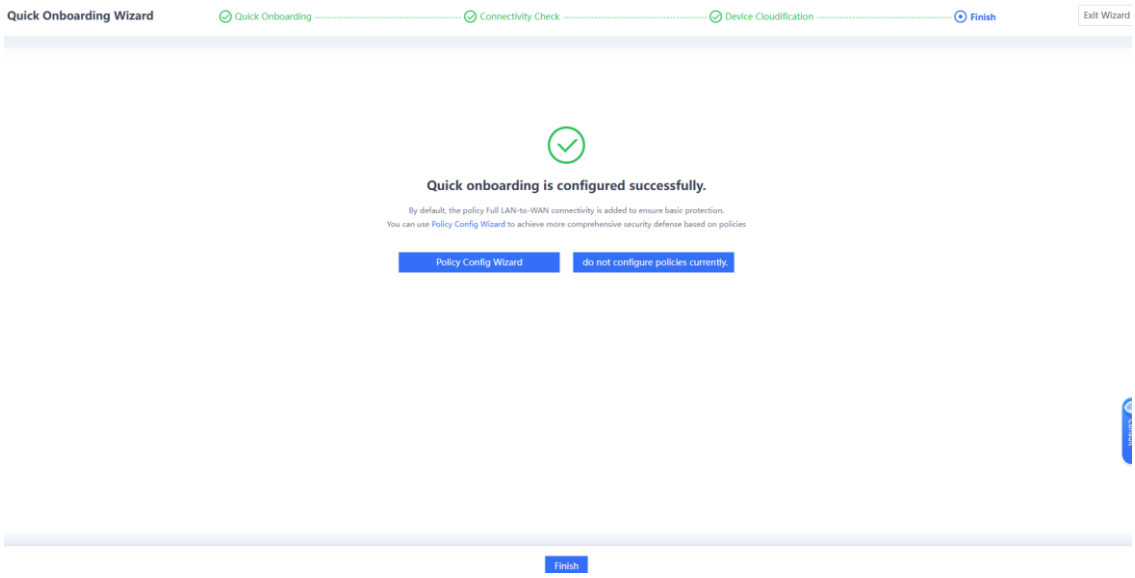
(5) (Optional) If the firewall can connect to the Internet, the **Enable Ruijie Cloud-based Management** page is displayed. Enable the cloud management platform function and bind the device as prompted.

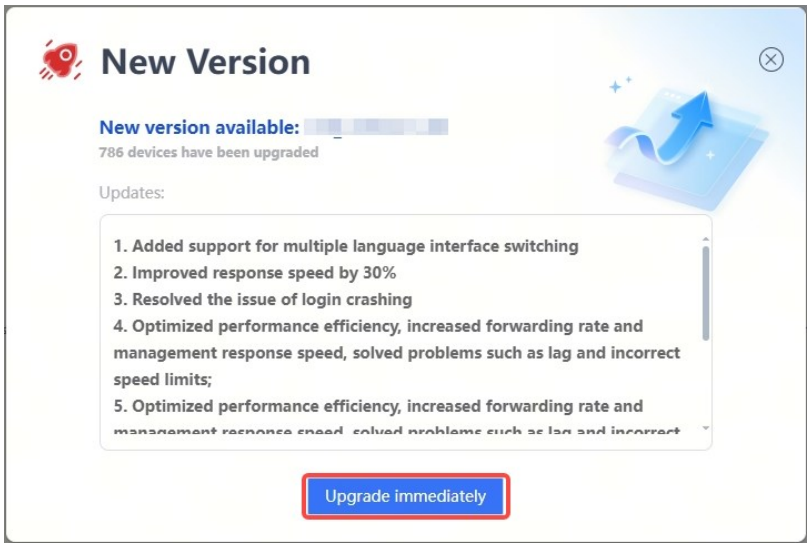
Note

If the device cannot connect to the Internet, connect it to the cloud management platform according to 9 Ruijie Cloud Connection.

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

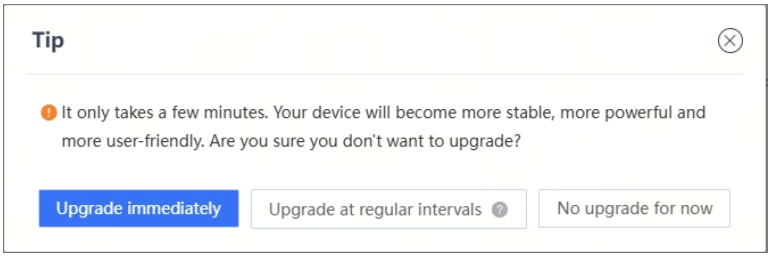
If the device can normally access Ruijie Security Cloud Platform and a new version is available on the cloud, the system automatically displays the **New Version** window. You can click **Upgrade immediately** to upgrade the version.





Note

If the upgrade operation cannot be executed immediately, click **x** to close the pop-up window. Then, click **Upgrade at regular intervals** in the **Tip** window that is displayed in later steps and specify an interval for periodic upgrade of the system version. After that, the system pre-downloads the version file to the local device and performs version upgrade and restart at the specified time.



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 **O&M** > **Network** > **Traffic** > **Interface Traffic** > **Interface Traffic Statistics**, and check traffic on the off-path interface.

4. Quick Onboarding (Switching Mode)

Application Scenario

When the switching 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.

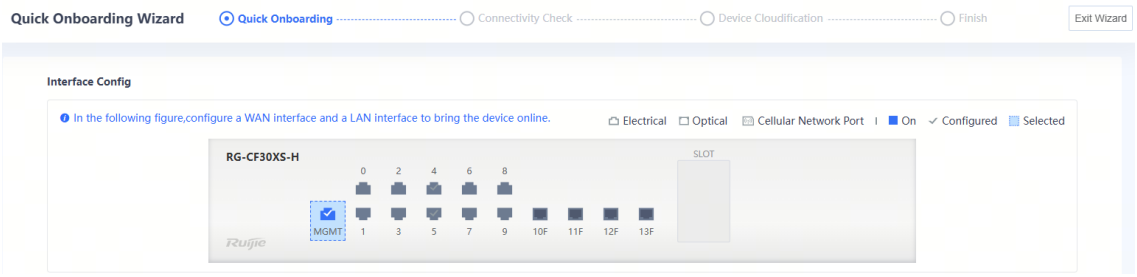
Note

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

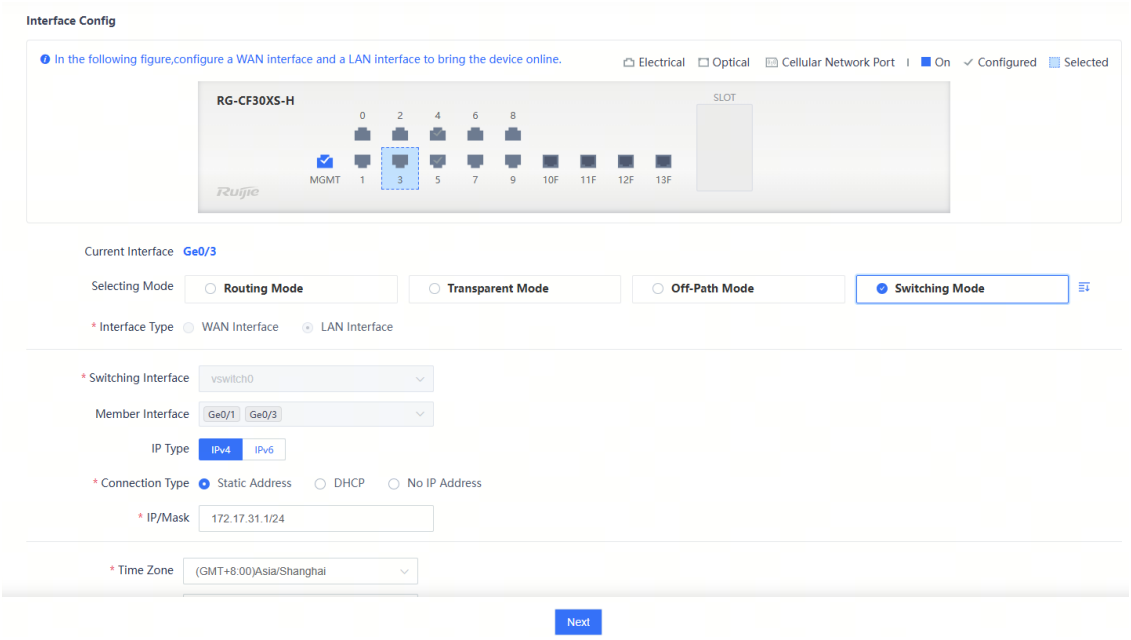
Procedure

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

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



(2) Configure the LAN interface.



a Select the interface that functions as the LAN interface.

b Set **Selecting Mode** to **Switching Mode**.

c The default value of **Interface Type** is **LAN Interface**.

(3) Configure the interface in switching mode.

a Set parameters for the interface in switching mode.

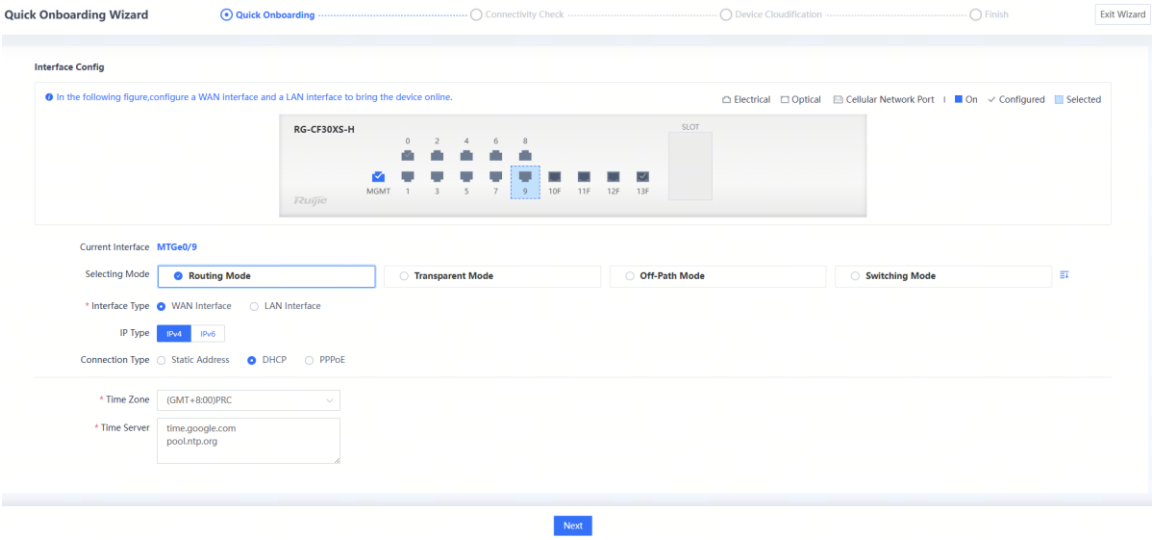
Item	Description	Remarks
Switching Interface	Select the switching interface to which the current interface belongs.	The default switching interface of the system is **vswitch0**.

Item	Description	Remarks
Member Interface	Member interface of the switching interface. After an interface is added to the switching interface, it becomes a member of the switching interface.	[Example] Ge0/1, Ge0/3
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: **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. **DHCP**: Applicable when the network administrator is not professional. The interface in switching mode automatically obtains an IP address from the connected ISP network or upper-layer DHCP server for Internet access. **No IP Address**: Applicable when no IP address needs to be configured for the interface in switching mode. In this mode, you cannot access or manage the device through the interface in switching mode. Therefore, ensure that another management channel (for example, the IP address of another interface) has been configured for accessing the device.	[Example] Static Address
IP/Mask	IP address and mask of the interface in switching mode.	You need to set this parameter when **Connection Type** is set to **Static Address**. [Example] 192.168.20.1/24
IP Type: IPv6		

Item	Description	Remarks
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: **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. **DHCP**: The interface automatically obtains an IPv6 address through DHCP.	[Example] Static Address
IP/Prefix Length	IPv6 address and prefix length of an interface.	You need to set this parameter when **Connection Type** is set to **Static Address**. [Example] 2001:1::1/64
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

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

(4) Configure the WAN interface.



a Select the interface that functions as the WAN interface.

b Set **Selecting Mode** to **Routing Mode**.

c Set parameters for the WAN interface.

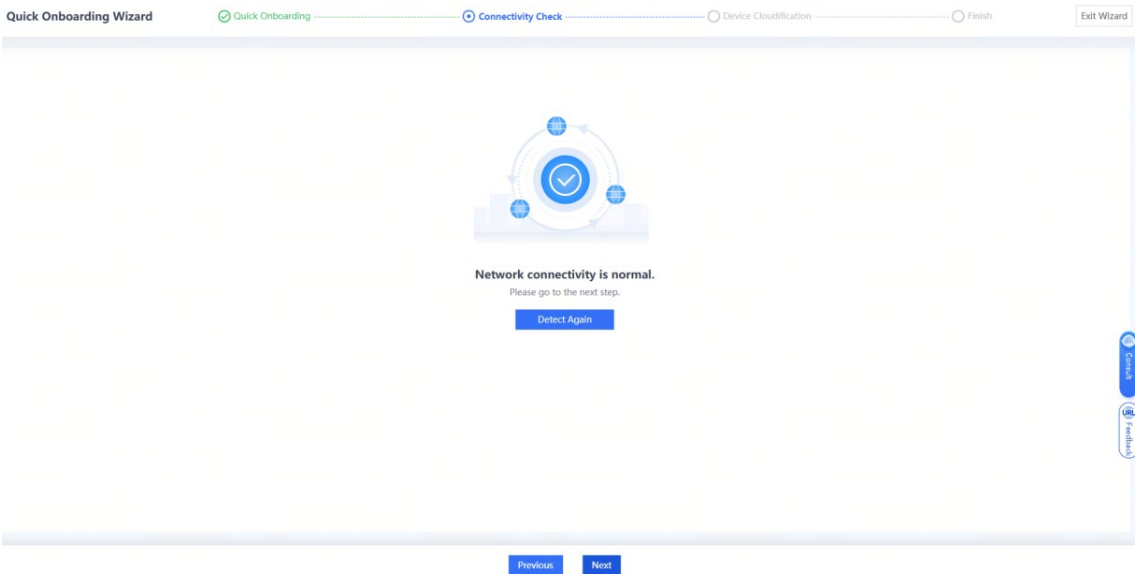
Item	Description	Remarks
Interface Type	**WAN Interface**: is used to connect the firewall to the Internet. Typically, the WAN interface is directly connected to the FTTH ONT of the ISP.	[Example] WAN Interface
IP Type	Set the interface address type based on the network environment. Valid values: **IPv6** and **IPv4**. Both IPv4 and IPv6 addresses can be configured for an interface.	[Example] IPv4
IP Type: IPv4		

Item	Description	Remarks
Connection Type	Connection type of the interface. The options are as follows: **Static Address**: Applicable when the network administrator specifies an IP address for the device based on the predefined IP address planning. This connection type requires the network administrator to possess 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 automatically obtains an IP address for Internet access. **PPPoE**: Applicable for dialup access to the ISP network. The username and password of the dialup user must be configured.	[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	IP address of the next-hop node to reach the destination address.	You need to set this parameter when **Connection Type** is set to **Static Address**. [Example] 192.168.20.2
Account/ Password	Username and password for dialup access. Typically, they are assigned by an ISP.	You need to set this parameter when **Connection Type** is set to **PPPoE**.
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

Item	Description	Remarks
Connection Type	Connection type of the interface. The options are as follows: **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. **DHCP**: The interface automatically obtains an IPv6 address through DHCP. **PPPoE**: The interface functions as an IPv6 PPPoE client and obtains an IPv6 address from the IPv6 PPPoE server.	[Example] Static Address
Account/ Password	Username and password for dialup access. Typically, they are assigned by an ISP.	You need to set this parameter when **Connection Type** is set to **PPPoE**.
IP/Prefix Length	IPv6 address and prefix length of the interface.	You need to set this parameter when **Connection Type** is set to **Static Address**. [Example] 2001:1::1/64
Next-Hop Address	IP address of the next node for forwarding data.	You need to set this parameter when **Connection Type** is set to **Static Address**. [Example] 2003::1
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

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

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



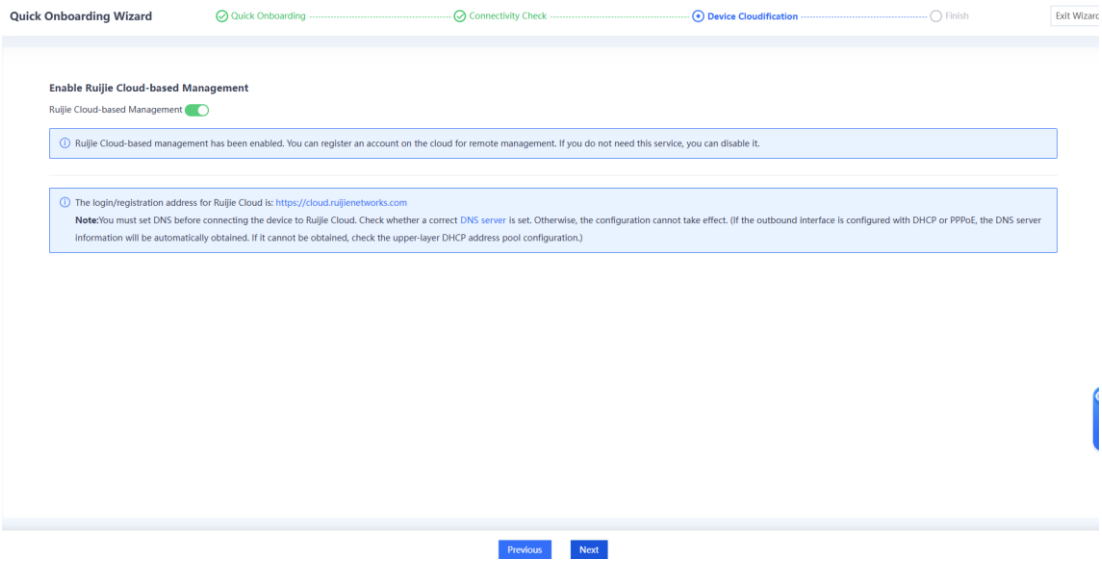
Note

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

(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.

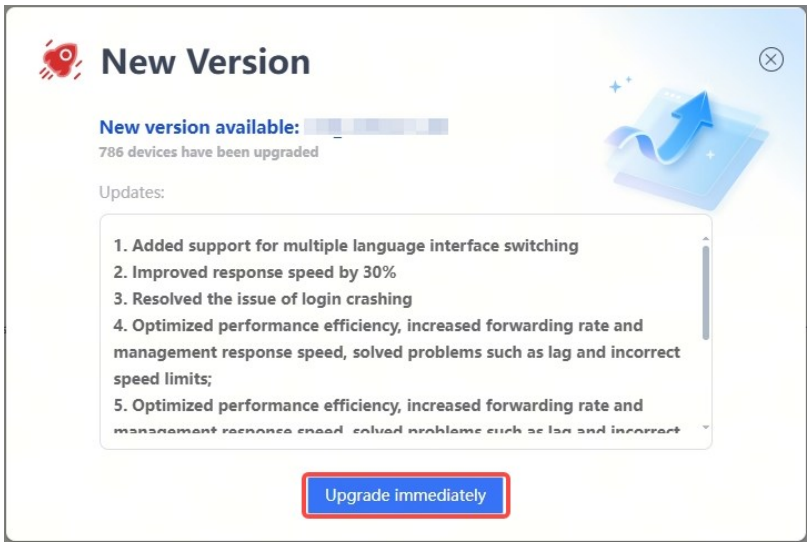
Note

If the device cannot connect to the Internet, connect it to the cloud management platform according to 9 Ruijie Cloud Connection.



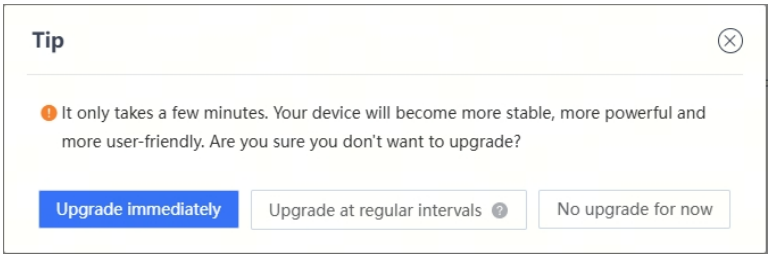
(7) After completing the configuration, click **Next**. Click **Finish** to complete quick onboarding configuration.

If the device can normally access Ruijie Security Cloud Platform and a new version is available on the cloud, the system automatically displays the **New Version** window. You can click **Upgrade immediately** to upgrade the version.



Note

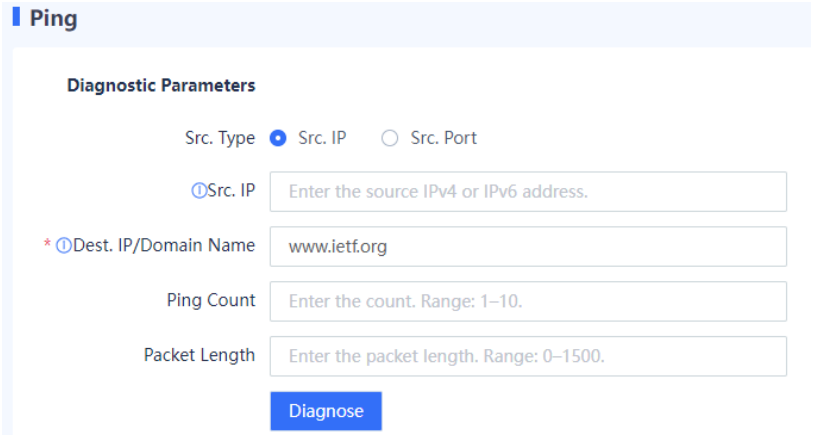
If the upgrade operation cannot be executed immediately, click **x** to close the pop-up window. Then, click **Upgrade at regular intervals** in the **Tip** window that is displayed in later steps and specify an interval for periodic upgrade of the system version. After that, the system pre-downloads the version file to the local device and performs version upgrade and restart at the specified time.



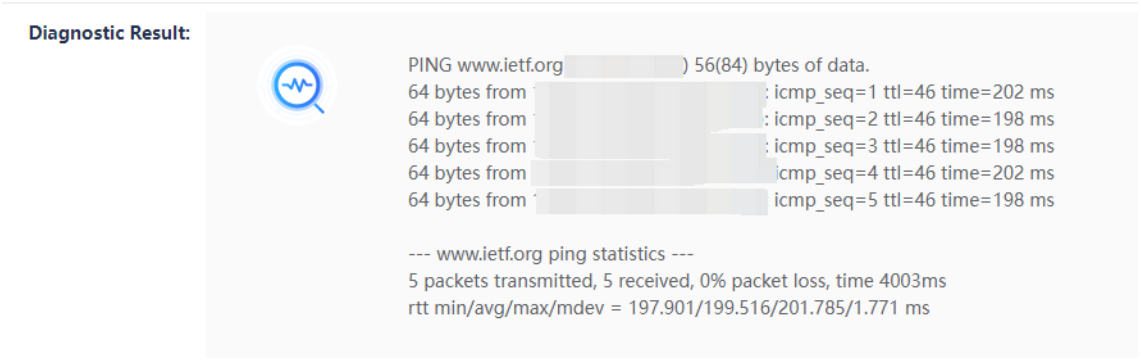
Verification

Connect the WAN interface of the device to the optical modem (or ONT), log in to the device through the management port, and choose **O&M** > **Fault Diagnosis** > **Ping**. Then, configure diagnostic parameters, as shown in Figure 3-3, and click **Diagnose**.

Figure 3-3 Ping Example



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



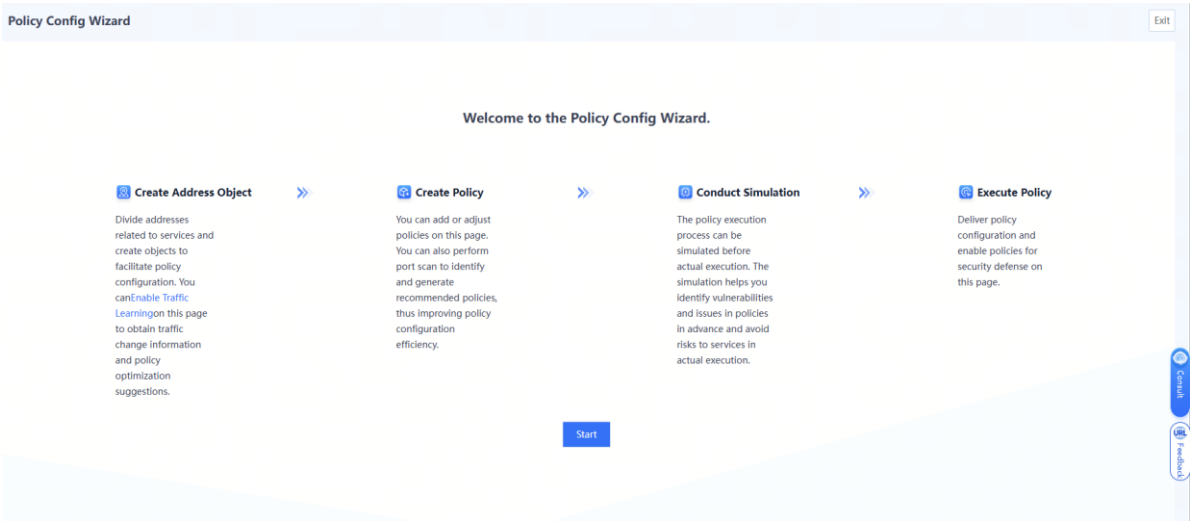
3.2.2 Configuring Security Policies Using the Wizard

The web UI of CF 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.



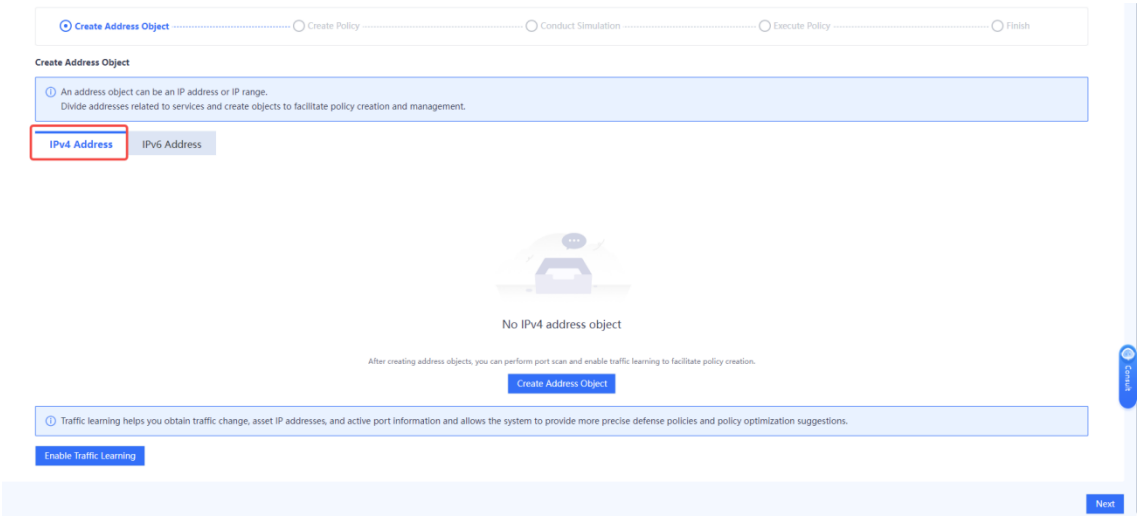
1. Creating Address Objects

Application Scenario

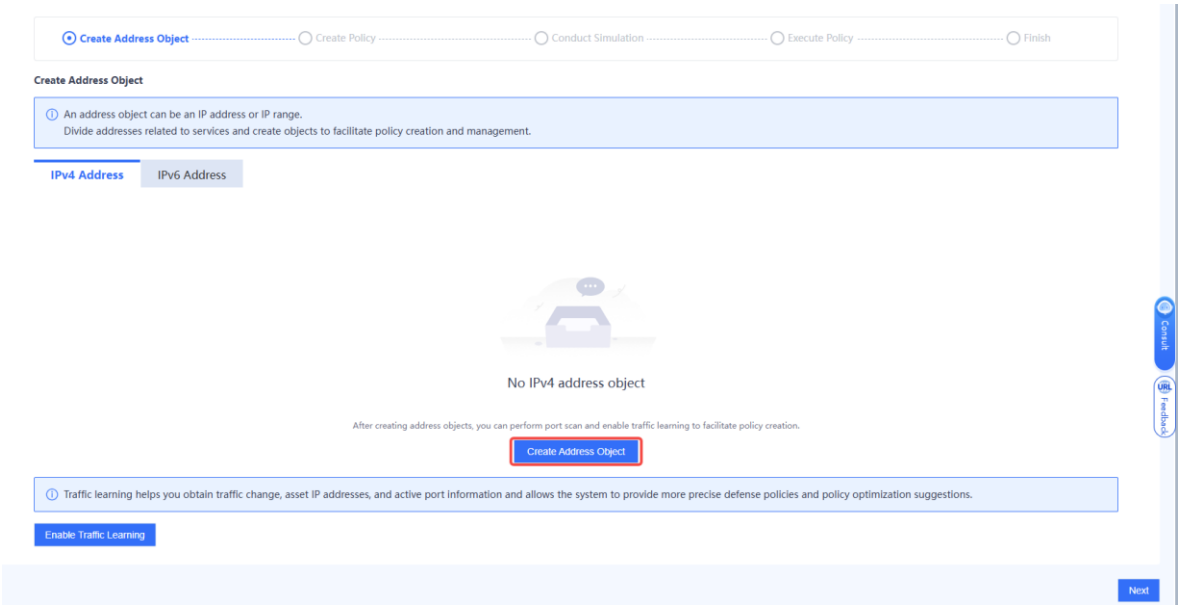
By using the address object, you can classify service-related IP addresses (including internal or external IP addresses), facilitating management of traffic within the specified IP address range.

Procedure

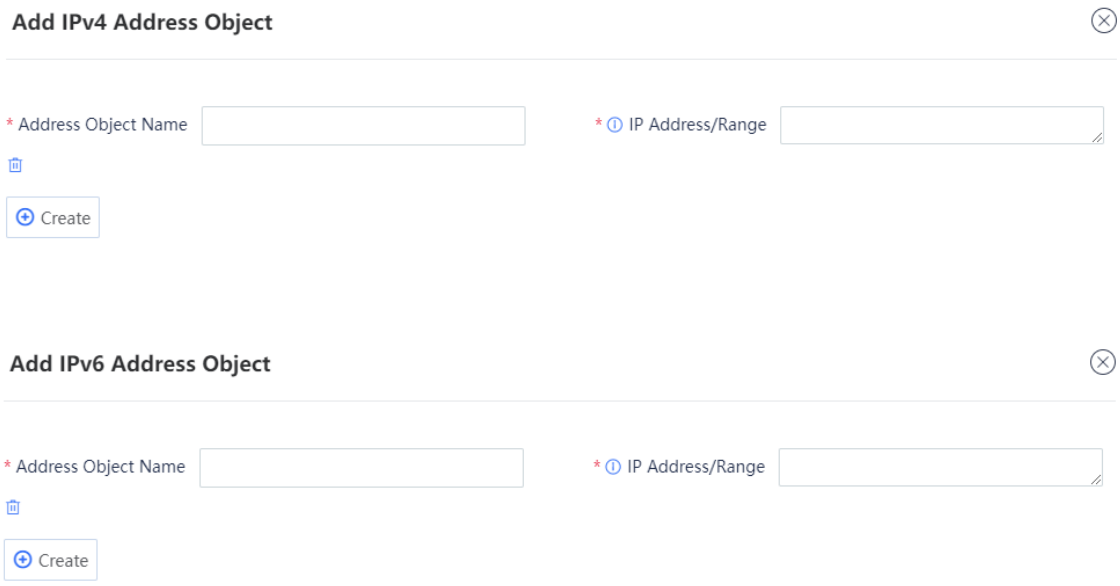
(1) Address objects include IPv4 address objects and IPv6 address objects. Configure the address objects based on the actual applications. On the **Create Address Object** page, select the tab of the address object to be created, for example, **IPv4 Address**.



(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.



Item	Description	Remarks
Address Object Name	Name of the IP address object.	[Example] Addr1

Item	Description	Remarks
IP Address/Range	IP address or range.	Three configuration methods are supported: **IP address**: One or multiple IP addresses. Input an IP address per line. Press **Enter** to separate lines. Example 1: 192.168.20.3 Example 2: 1234::100 **IP range**: A contiguous range of addresses. Connect the start IP address and end IP address with a hyphen (-). Example 1: 192.168.20.1-192.168.20.3 Example 2: 1234::100-2345::100 **Subnet**: IP range. Example 1: 192.168.1.0/24 or 192.168.1.0/255.255.255.0 Example 2: 1234::/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 external network. A security policy is configured to establish a designated channel between the intranet and external network to filter sensitive data access.

Prerequisites

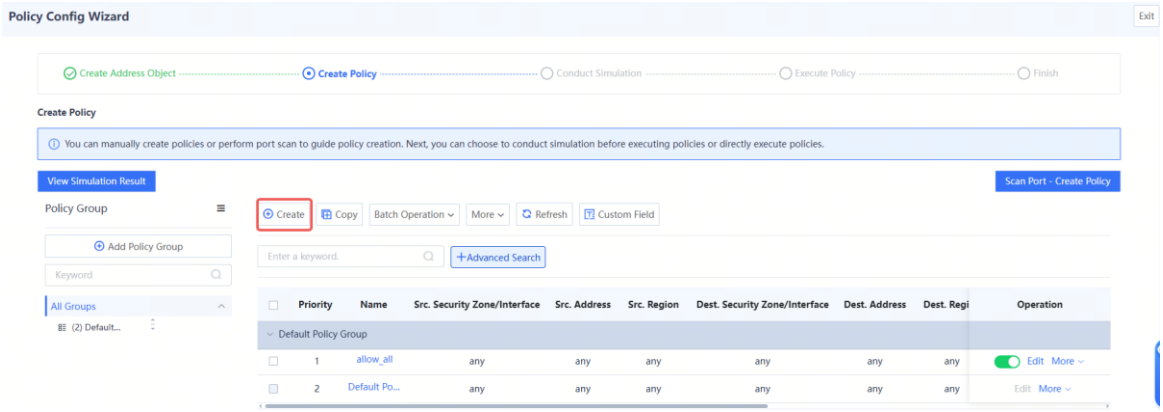
The security zone, service, service group, application group, time plan, intrusion protection policy, virus protection policy, and other required configurations have been created according to service requirements.

- For details on how to create a security zone, see 6.2 Security Zone.
- For details on how to create a service, see 5.4.3 Configuring a Custom Service.
- For details on how to create a service group, see 5.4.4 Creating a Service Group.
- For details on how to create an application zone, see 5.2 Application.

- For details on how to create a time plan, see 5.6 Time Plan.
- For details on how to create an intrusion protection policy, see 5.10.2 Intrusion Prevention.
- For details on how to create a virus protection policy, see 5.10.1 Virus Protection.

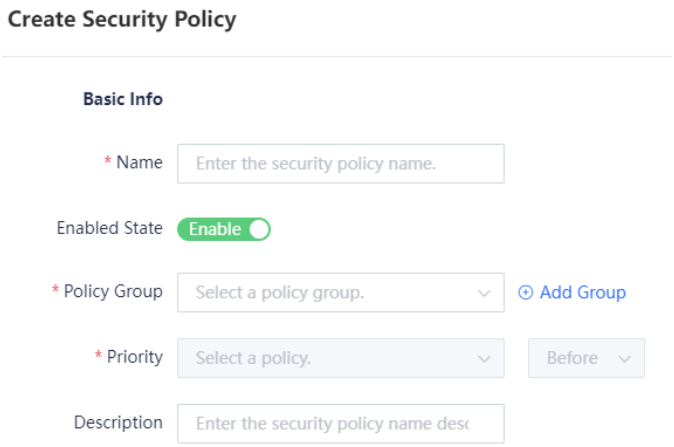
Procedure

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

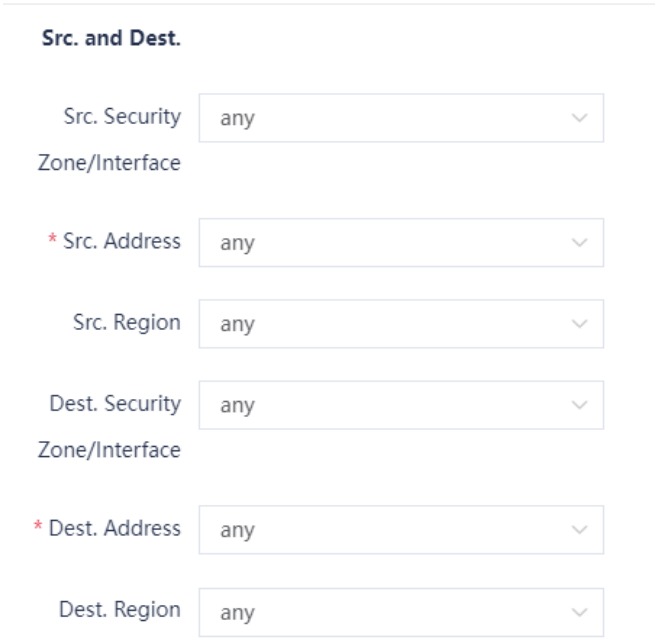


(2) Set parameters related to the security policy.

a Configure basic information about the security policy.



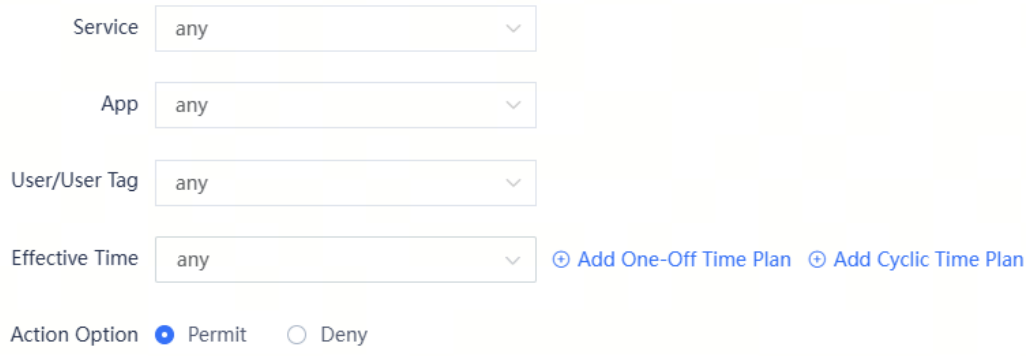
b Set the source and destination security zones or interfaces, addresses, and regions of the target data connection.



Item	Description	Remarks
Src. Security Zone/Interface	Security zone or interface initiating the target data connection.	● Click the drop-down list, and select a source security zone or interface in the **To-be-selected** area. The selected item is automatically added to the **Selected** area. ● Click **Add Security Zone** to add a security zone. ● **Any** indicates all interfaces. [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. ● Click **Add Address** or **Add Address Group** to add an address or address group object. Example any
Src. Region	Region initiating the target data connection.	● Click the drop-down list, and select a source region in the **To-be-selected** area. The selected region is automatically added to the **Selected** area. ● Click **Add Custom Region** to add a region. [Example] any

Item	Description	Remarks
Dest. Security Zone/Interface	Destination security zone or interface of the target data connection.	● Click the drop-down list, and select a destination security zone or interface in the **To-be-selected** area. The selected item is automatically added to the **Selected** area. ● Click **Add Security Zone** to add a security zone. ● **Any** indicates all interfaces. [Example] trust
Dest. Address	Destination address (IP address or domain name) 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. ● Click **Add Address** or **Add Address Group** to add an address or address group object. [Example] any
Dest. Region	Destination region of the target data connection.	● Click the drop-down list, and select a destination region in the **To-be-selected** area. The selected region is automatically added to the **Selected** area. ● Click **Add Custom Region** to add a custom region object. [Example] any

c (Optional) Select the services, applications, and users/user tags for the target data connection request, and configure the effective time range for the policy.



d Configure the action taken by the security policy to permit or deny the target data connection.

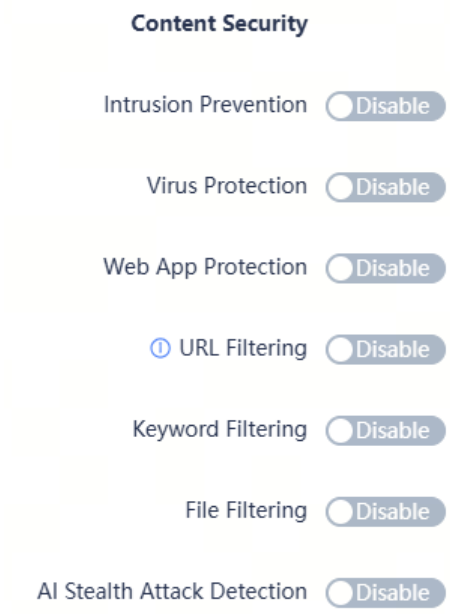


Action Option	Description
Permit	If the action is set to Permit, the device performs check according to whether content security check is enabled: Content security check is not enabled: Directly permit the traffic. Content security check is enabled: Process the traffic according to the content check policy.
Deny	Block the traffic.

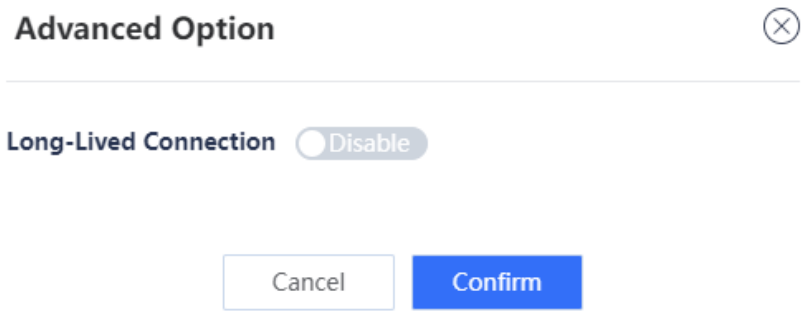
e Specify whether to record session logs for traffic matching this policy. This configuration item takes effect only when the hard disk module is installed on the device.



f Set whether to enable content security checks for the target data connection.



g Click **Settings** in the **Advanced** area. Configure long-lived connection attributes and click **Confirm**.



h Click **Save**.

3. Conducting Simulation Run

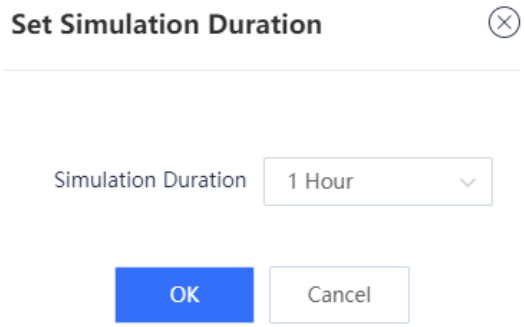
Application Scenario

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

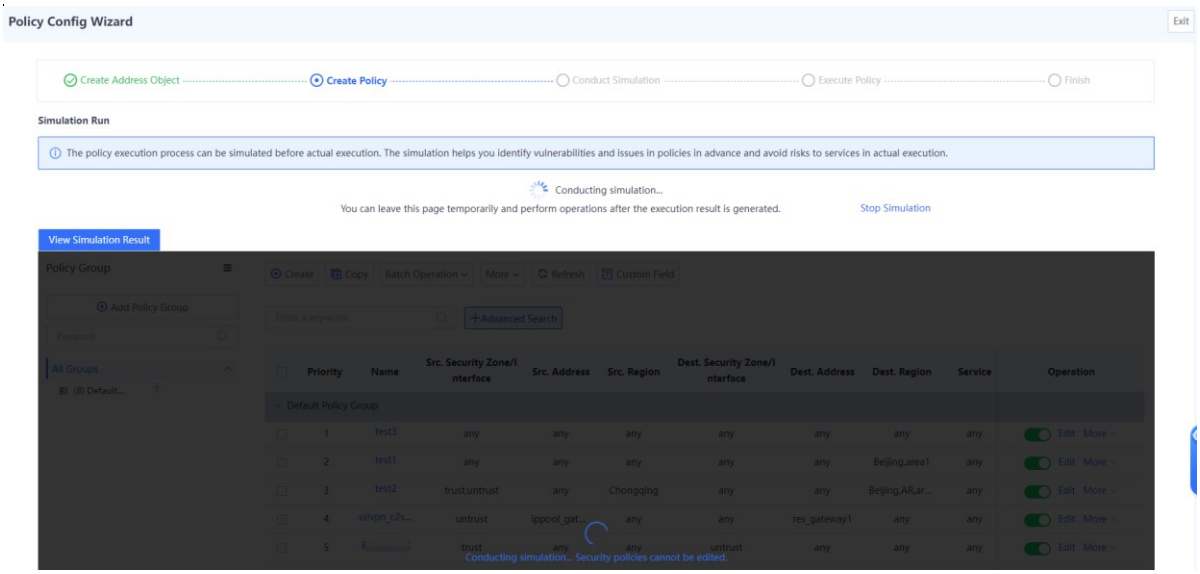
(1) On the **Create Policy** page, select the policy for which simulation run will be performed, and click **Start Simulation**.

(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.

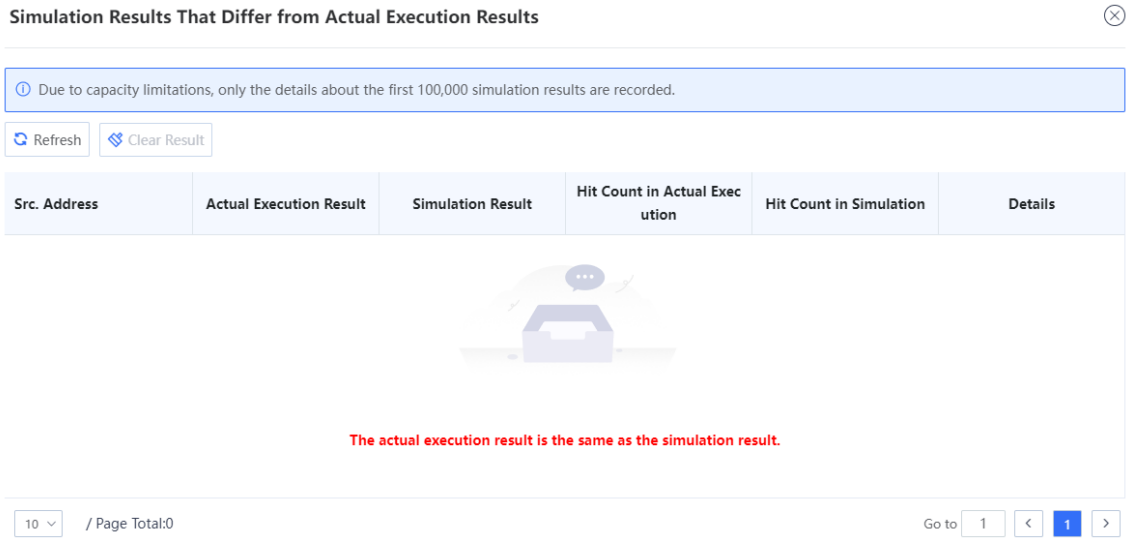


(4) When simulation run is finished, click **View Simulation Result**.

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.



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

4 Policy Configuration and Management

4.1 Security Policy

4.1.1 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 (such as IPS and AV) 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, virus protection, and other functions are enabled in the security policy, the matched packet is forwarded to the corresponding modules for content security check.

(4) If a packet matches the URL filtering, intrusion prevention, virus protection, or other content security rules, 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 the content security rule 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.

4.1.2 Manually Configuring Security Policies

Application Scenario

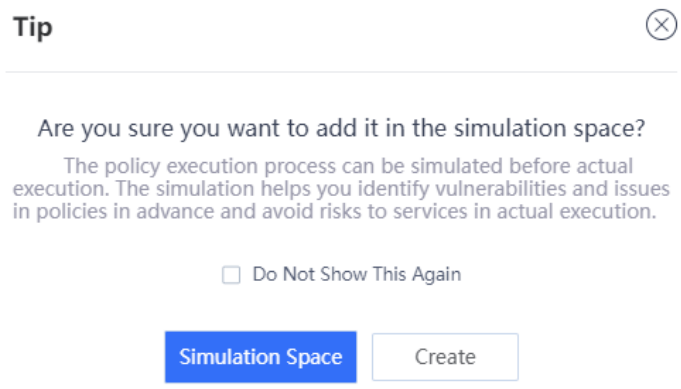
In addition to the wizard, CF series firewalls support manual configuration. You can manually configure security policies according to service needs.

Procedure

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

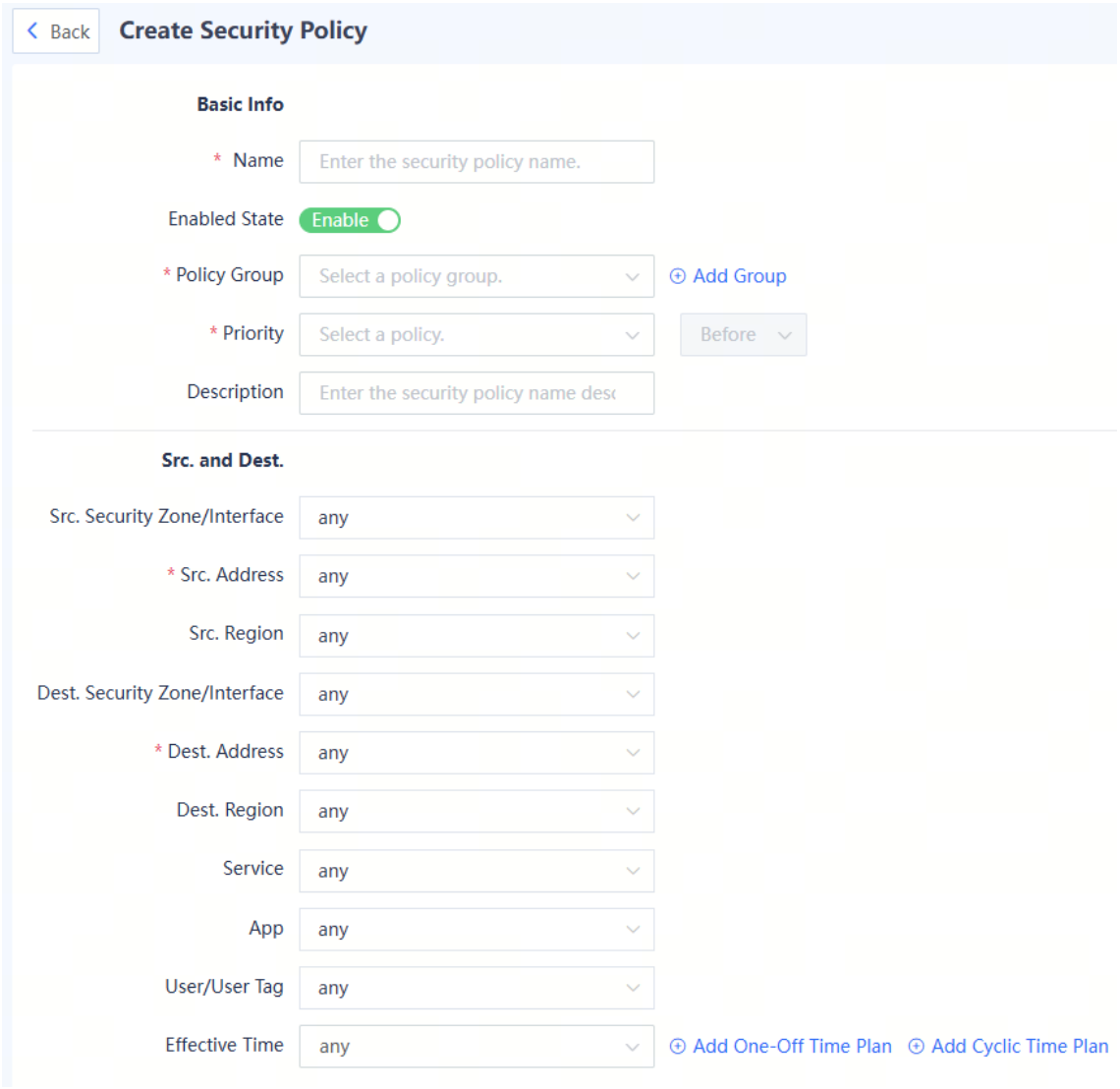
(2) In the operation area, click **Create.**

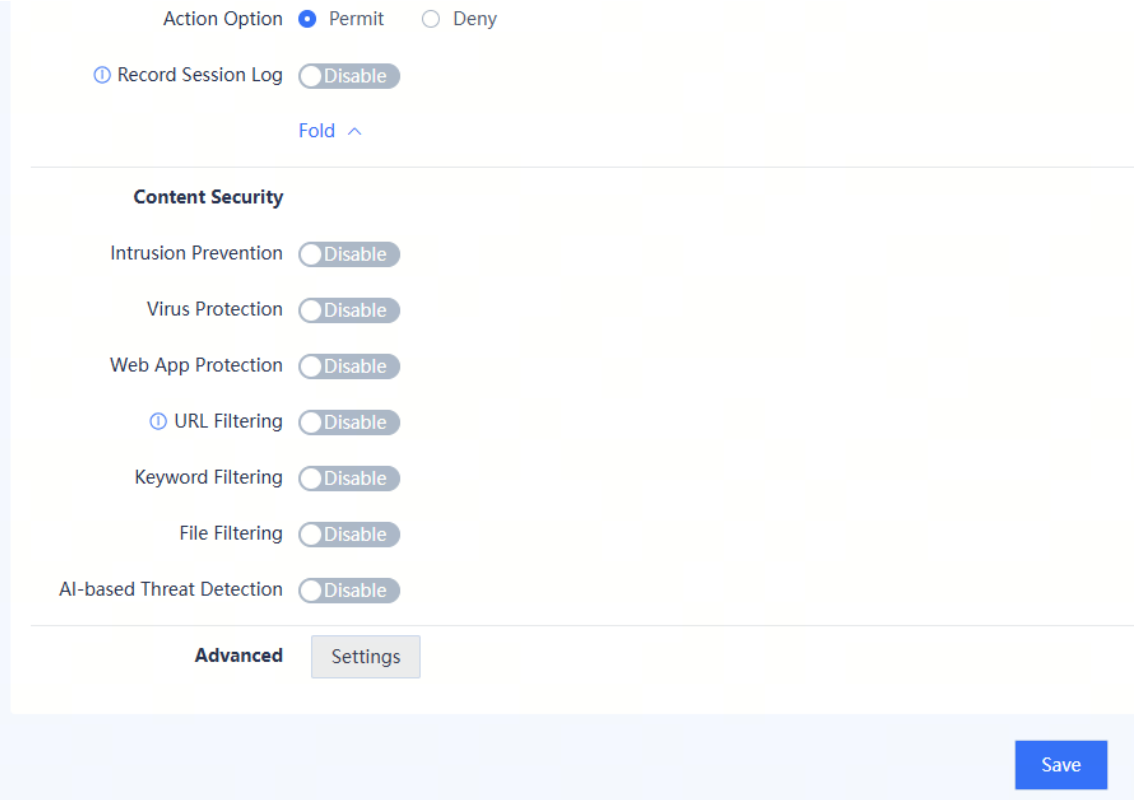
A tip dialog box is displayed.



(3) Click **Create**.

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


Back
Create Security Policy
Basic Info
* Name
Enter the security policy name.
Enabled State
Enable
* Policy Group
Select a policy group.
Add Group
* Priority
Select a policy.
Before
Description
Enter the security policy name desc
Src. and Dest.
Src. Security Zone/Interface
any
* Src. Address
any
Src. Region
any
Dest. Security Zone/Interface
any
* Dest. Address
any
Dest. Region
any
Service
any
App
any
User/User Tag
any
Effective Time
any
Add One-Off Time Plan
Add Cyclic Time Plan



(4) Set the parameters for the security policy.

Item	Description	Remarks
Basic Info		
Name	Security policy name.	[Example] Trust_to_untrust
Enabled State	Whether to enable the new security policy.	[Example] Enable
Policy Group	Policy group to which the new security policy belongs.	Select from the drop-down list. Click **Add Group** to customize the new policy group. [Example] Default Policy Group
Priority	Move the new security policy before or after the specified policy. The policy listed before has a higher matching priority.	N/A

Item	Description	Remarks
Description	Security policy description.	[Example] Perform virus detection for the HTTP traffic from security zone 1 to security zone 2.
Src. and Dest.		
Src. Security Zone/Interface	Source security zone or interface initiating the target data.	● Click the drop-down list, and select a source security zone or interface in the **To-be-selected** area. The selected item is automatically added to the **Selected** area. ● Click **Add Security Zone** to add a custom security zone. ● **Any** indicates all interfaces. [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. ● Click **Add Address** or **Add Address Group** to create an address or address group object. [Example] any
Src. Region	Region initiating the target data connection.	● Click the drop-down list, and select a source region in the **To-be-selected** area. The selected region is automatically added to the **Selected** area. ● Click **Add Custom Region** to add a region. [Example] CN
Dest. Security Zone/Interface	Destination security zone or interface of the target data connection.	● Click the drop-down list, and select a destination security zone or interface in the **To-be-selected** area. The selected item is automatically added to the **Selected** area. ● Click **Add Security Zone** to add a custom security zone. ● **Any** indicates all interfaces. [Example] trust

Item	Description	Remarks
Dest. Address	Destination address (IP address or domain name) 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
Dest. Region	Destination region of the target data connection.	● Click the drop-down list, and select a destination region in the **To-be-selected** area. The selected region is automatically added to the **Selected** area. ● Click **Add Custom Region** to create a custom region object. [Example] CN
Service	Service type of the target data connection request.	● 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**. [Example] any
App	Application type of the target data connection request.	● 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**. [Example] any
User/User Tag	Traffic of specified users, user groups, or user tags will match the policy.	● Click the drop-down list. On the **User/User Group** tab page, select users or user groups in the to-be-selected area. The selected users or user groups are automatically added to the **Selected** area. ● Click **Add User** or **Create User Group** to add a user or a user group. ● Click the drop-down list. On the **User Tag** tab page, select user tags in the to-be-selected area. The selected user tags are automatically added to the **Selected** area. ● Click **Add User Tag** to add a user tag.

Item	Description	Remarks
Effective Time	Time segment in which the security policy is valid. You can associate the policy with a one-off time plan. That is, the policy takes effect only once. You can also associate the policy with a cyclic time plan. That is, the policy periodically takes effect in the specified time segment.	● To add a one-off time plan, click **Add One-Off Time Plan**. ● To add a cyclic time plan, click **Add Cyclic Time Plan**. [Example] any
Action Option	Action taken by the security policy to permit or deny the target data connection.	[Example] Permit
Record Session Log	Whether to record session logs for traffic matching this policy. This configuration item takes effect only when the hard disk module is installed on the device.	[Example] Enable
Content Security	Whether intrusion prevention, virus detection, URL filtering, keyword filtering, Web App Protection, AI-based Threat Detection, and file filtering are enabled for the target data connection. To enable content security checks, you must specify corresponding templates. For intrusion prevention, virus protection and web app protection templates, configure the actions. The action in the security policy takes precedence over the action in the template.	The configuration of content security takes effect on only IPv4 traffic. [Example] Intrusion Prevention: Enable Virus Protection: Enable Web App Protection: Enable URL Filtering: Disable Keyword Filtering: Enable File Filtering: Enable AI-based Threat Detection: Enable

Item	Description	Remarks
Advanced	Advanced settings of the security policy, including: **Long-Lived Connection**: applies to the special servers that require long-lived connections. After this function is enabled, the server's connection request is not restricted by the connection timeout setting of the firewall. The connection duration needs to be set. After this function is enabled, the connection release may be delayed. Therefore, exercise caution when enabling this function.	● Before enabling the long-lived connection function, configure the destination address and service of the policy. ● Click **Settings**, and set parameters on the displayed **Advanced Option** page. [Example] Disable

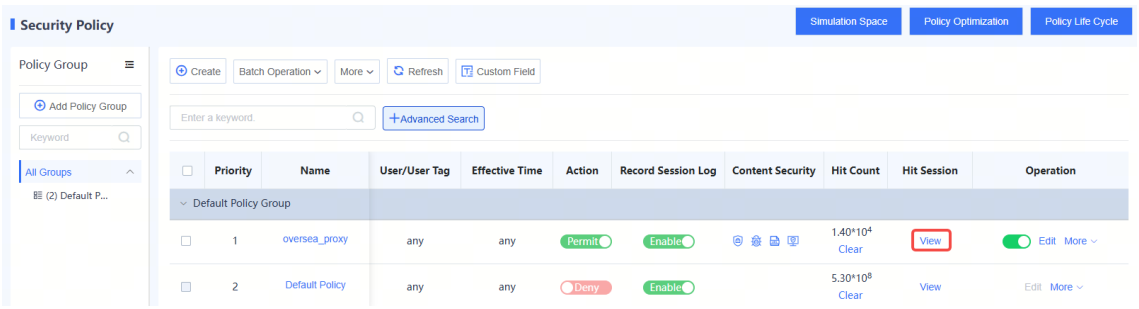
(5) Click **Save.**

Follow-up Procedure

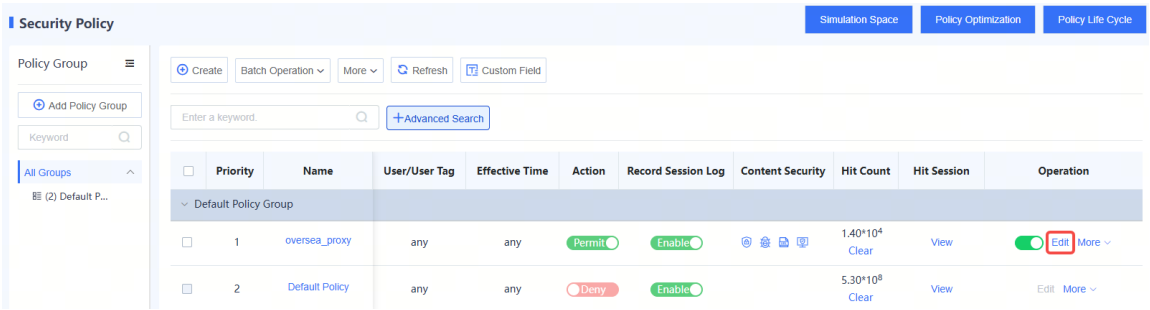
- When the security policy, virus protection policy, or intrusion prevention policy is hit, a security log is recorded. You can choose **O&M** > **Logs** > **Security Log** to view the log information.
- When user traffic hits the security policy, click **View** in the **Hit Session** column to view the session information.

Note

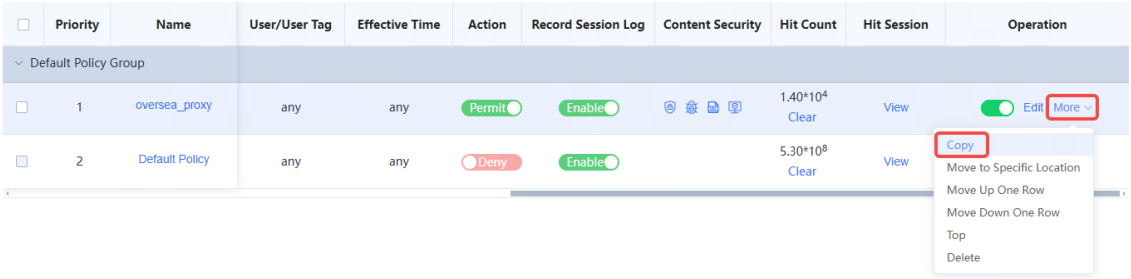
If **Record Session Log** is disabled, you cannot view the matching session information.



- Click **Edit** to modify security policy information, such as renaming the security policy.



- Click **More** and select **Copy** to copy the current policy. Then, adjust the relevant configuration to improve configuration efficiency.



4.1.3 Conducting Simulation Run

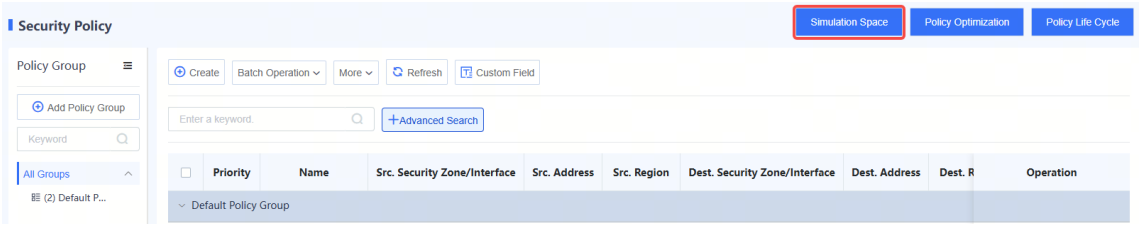
Application Scenario

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.

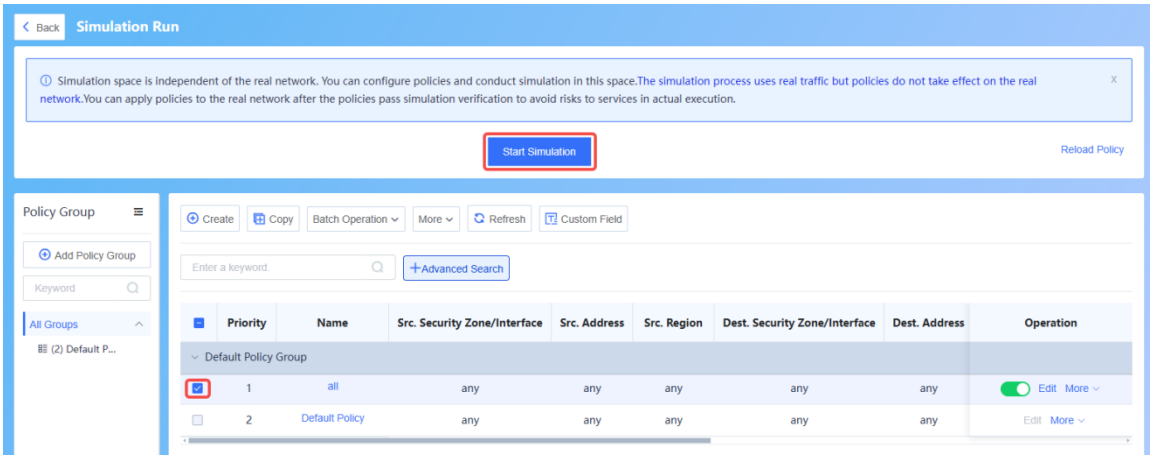
Procedure

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

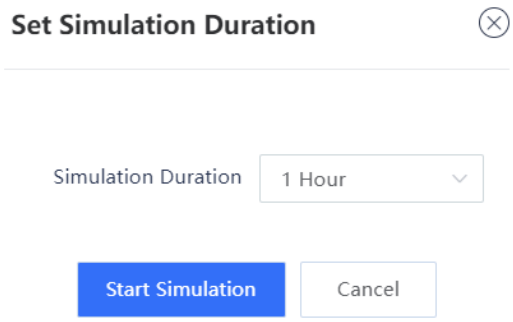
(2) Click **Simulation Space** in the upper right corner of the operation area.



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

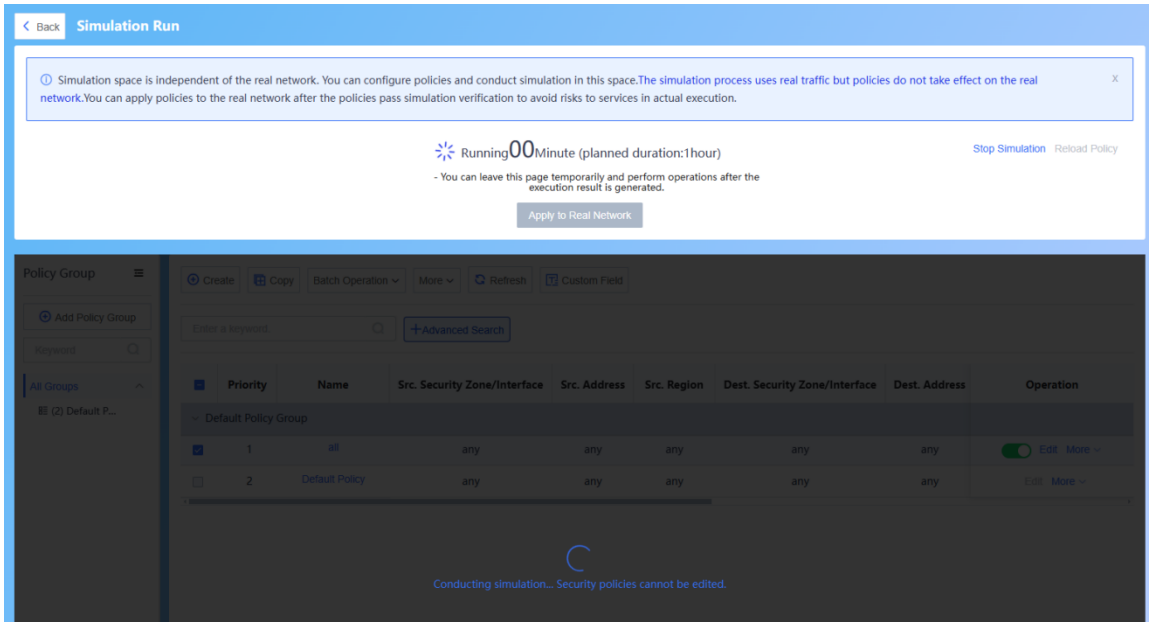


(4) In the **Set Simulation Duration** dialog box, set the duration of simulation run.



(5) Click **Start Simulation**.

The system automatically performs simulation run for the selected policies.

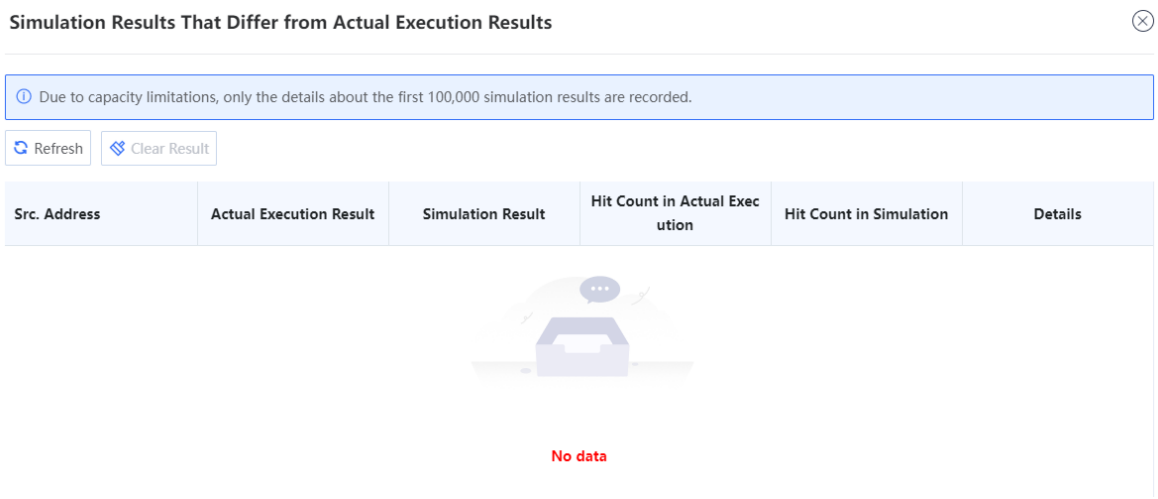


(6) When simulation run is finished, click **View Simulation Result**.

Simulation run results are displayed based on the source IP address:

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

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



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

4.1.4 Importing Configuration Files to Configure Security Policies

Application Scenario

CF series firewalls support fast generation of security policies by importing configuration files.

Caution

The security policies containing IPv6 addresses cannot be imported in batches.

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 CF series firewall, you can configure the policy migration tool to obtain the corresponding configuration file.

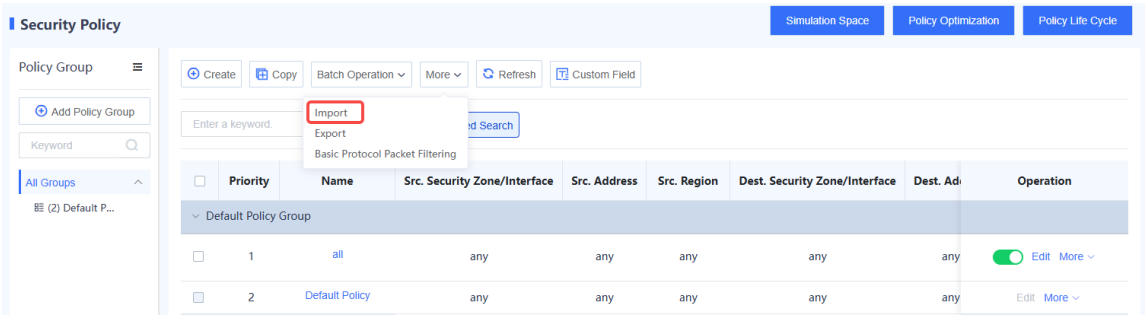
Note

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

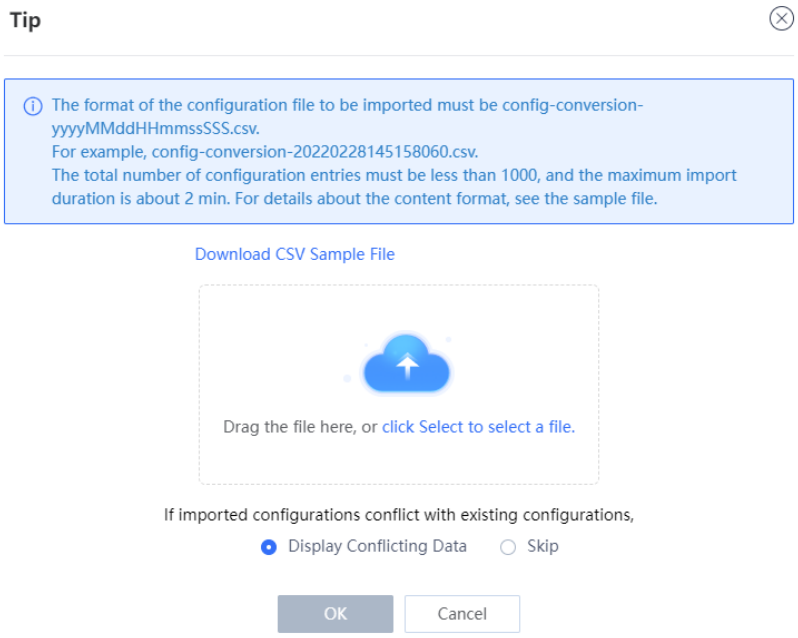
Procedure

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

(2) Click **More** in the operation area and select **Import** from the drop-down list.



(3) A tip dialog box is displayed.



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

Note

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

(5) Drag the configuration file to the upload area or click **Select** to 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.

4.1.5 Exporting Security Policies

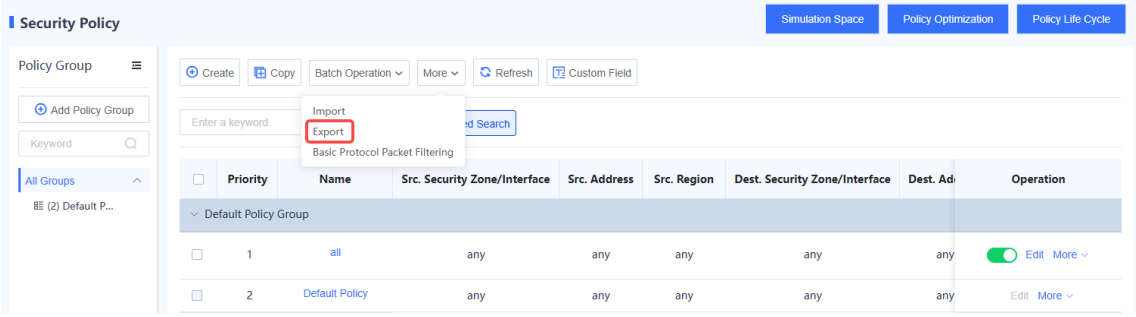
Application Scenario

On the CF 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 Defense** > **Security Policy**.

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



4.1.6 Adjusting Security Policy Order

Application Scenario

When multiple security policies are configured in the list, the closer a policy is to the top, the higher its priority in matching. That is, security policy matching is performed in sequence from the top to the bottom of the policy list. If the traffic matches a security policy, subsequent policies will not be matched.

You can adjust the sequence of security policies to modify their priorities and meet service requirements.

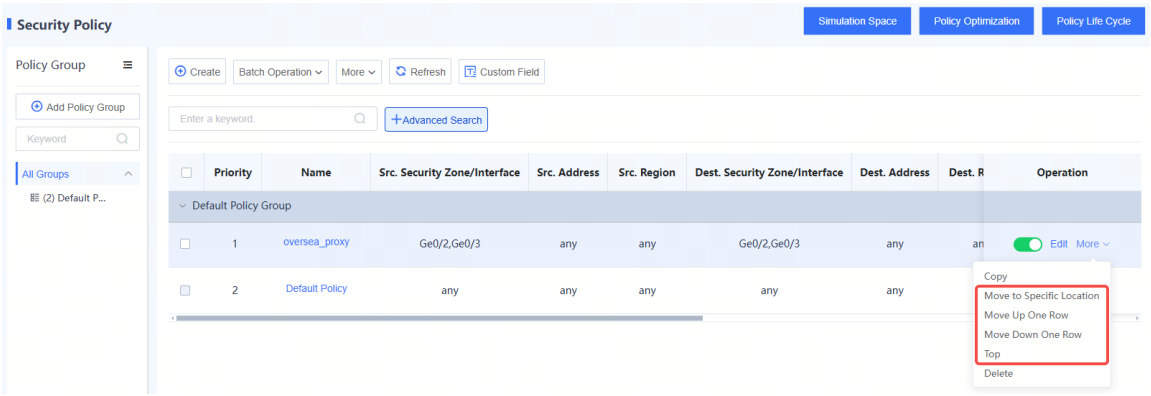
Note

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

Procedure

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

(2) Click **More** in the **Operation** column. In the drop-down list, select an operation to adjust the sequence of the policy or delete the policy.



4.1.7 Searching for Security Policies

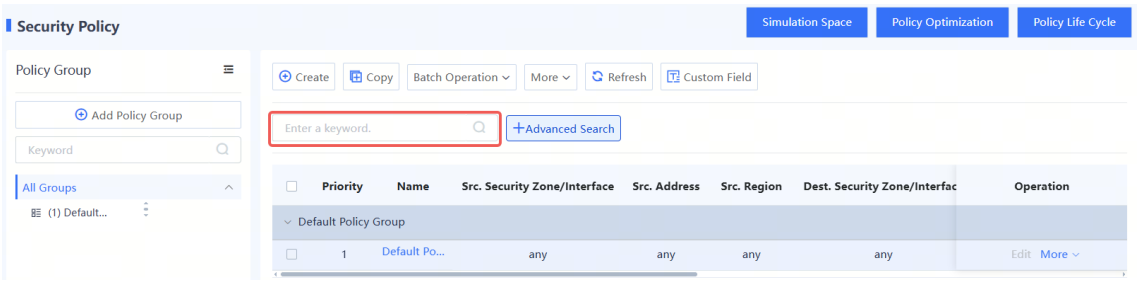
Application Scenario

When a large number of security policies are configured, you can use the security policy search function to accurately match and quickly locate related security policies by setting specific search criteria, thereby efficiently managing security policies.

Procedure

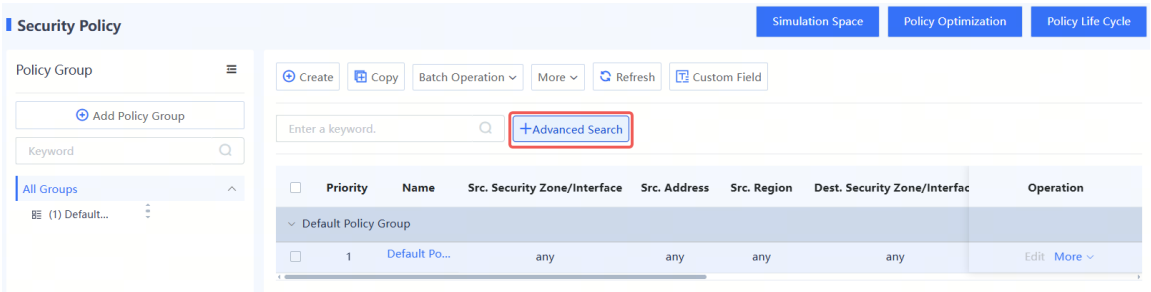
(1) Choose **Policy** > **Security Defense** > **Security Policy**.

(2) The search box on the left supports a fuzzy match for the security policy names and matching conditions based on keywords. Enter a keyword and click to display security policies that match the keyword.

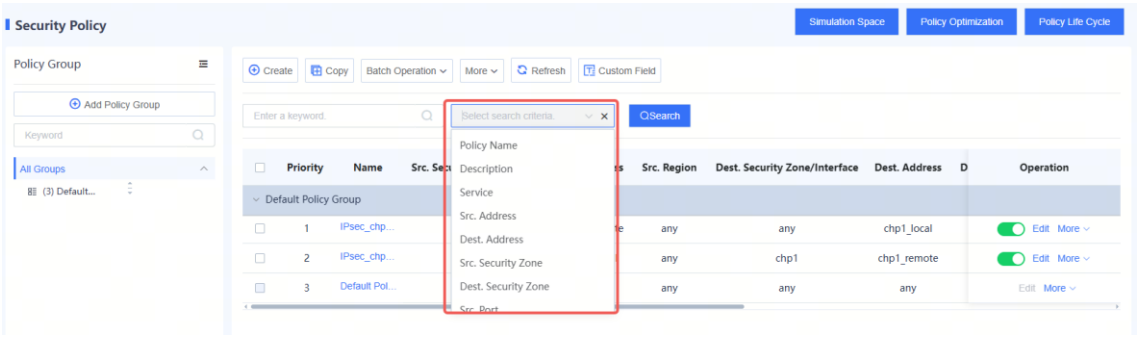


(3) To implement more accurate searches, click **+Advanced Search** and add a specific matching condition to search for security policies.

a Click **+Advanced Search** to add a search criterion.



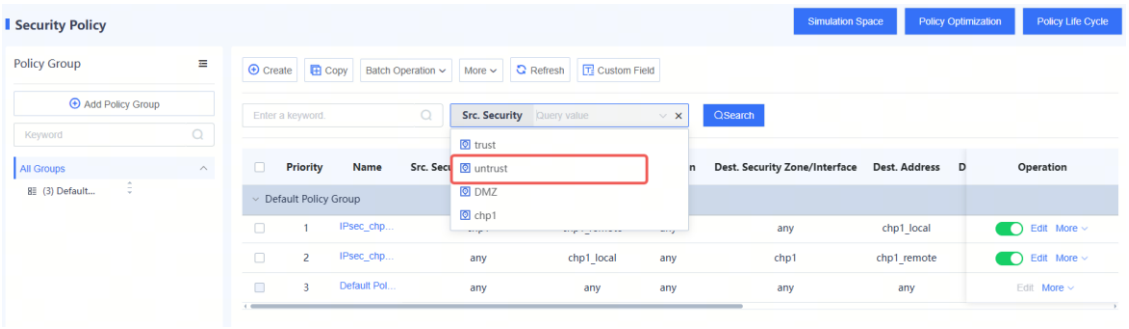
b Click the search criterion and set a search condition.



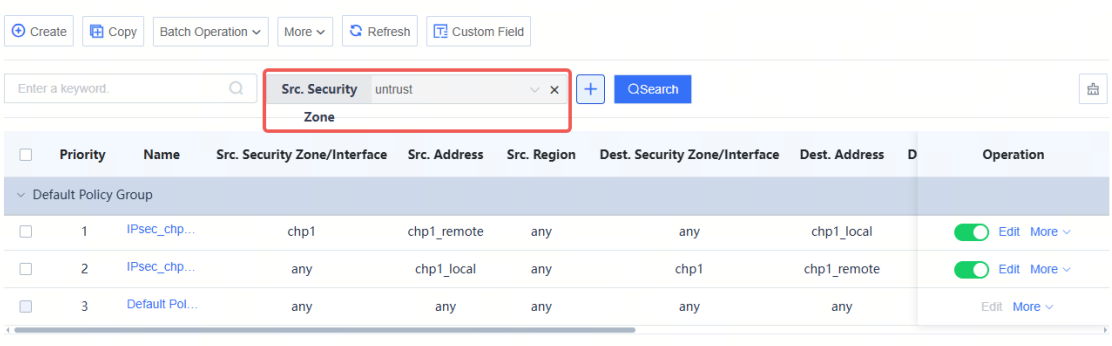
c Click the input box and set a search value (for example, set **Src. Security Zone** to **untrust**).

Note

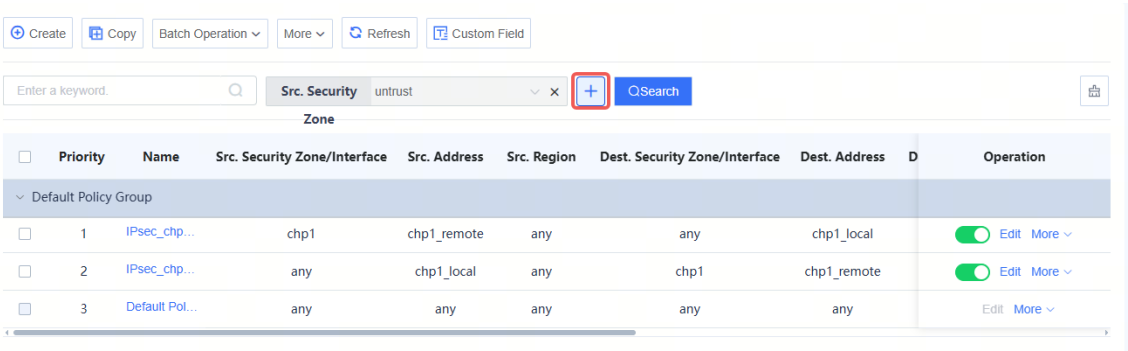
If matching conditions of security policies contain the current search condition, the security policies match the search criterion. For example, if **Src. Security Zone** is set to **trust** in the search condition, all security policies whose source zone is **trust** and **any** match the search condition.



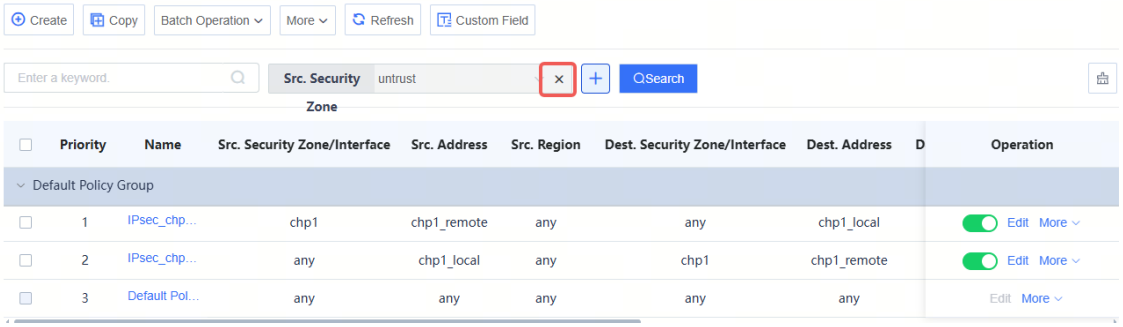
After setting parameters and values for a search criterion, you have added a search condition.



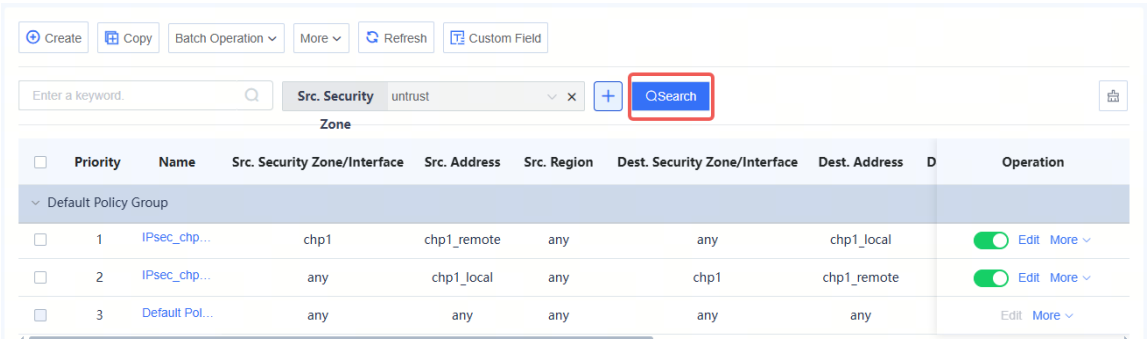
d (Optional) Click **+** to add more search conditions.



e (Optional) Click **X** next to a search criterion to delete the search condition.

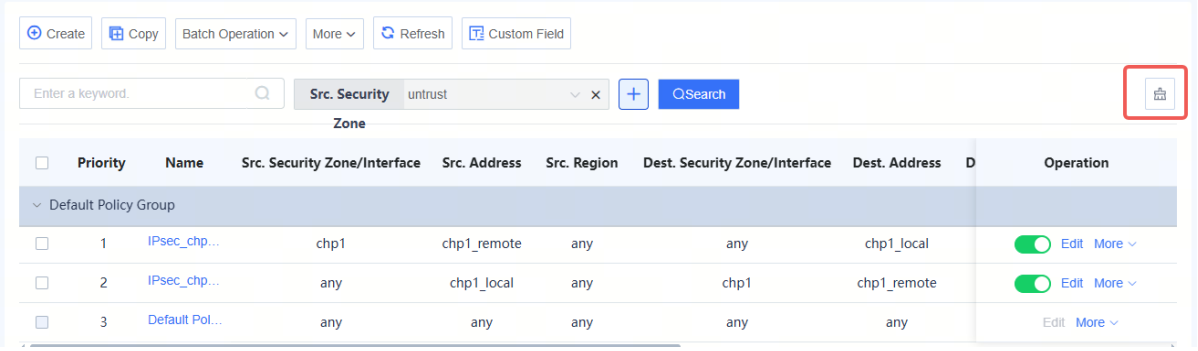


f After adding all the search conditions, click **Search**. Security policies that match the search conditions are displayed.



Follow-up Procedure

- Click the clear icon on the right to clear all search conditions.



4.1.8 Optimizing Security Policies

Application Scenario

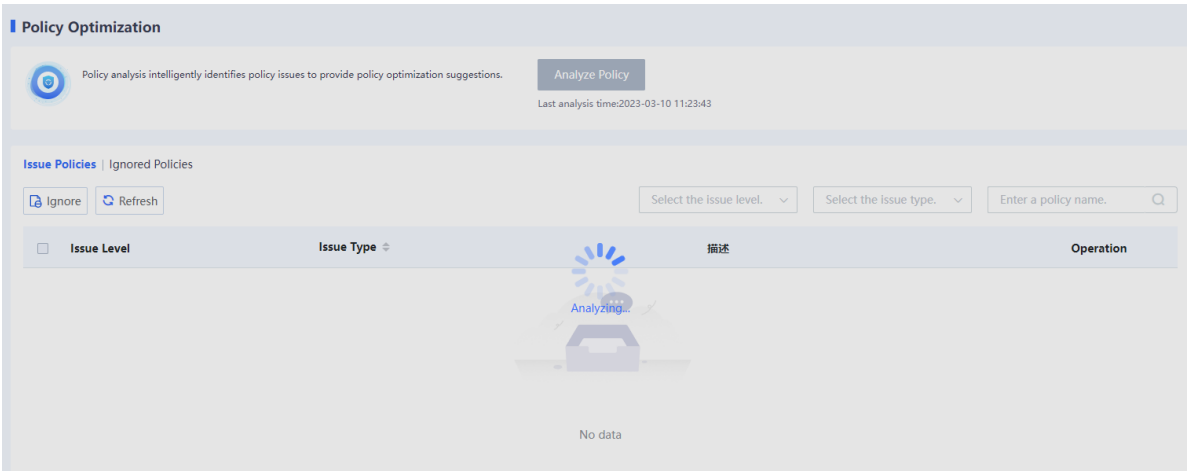
Affected by factors such as service accumulation and change of O&M personnel, the configuration complexity of security policies becomes increasingly high during the routine security policy O&M process. The policy optimization function of CF series firewalls can intelligently compare and analyze the filter conditions of the current security policies to identify redundant policies, which is convenient for O&M personnel to streamline and optimize policies, thus reducing O&M costs.

Procedure

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

(2) Click **Policy Optimization** in the upper right corner of the operation area.

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



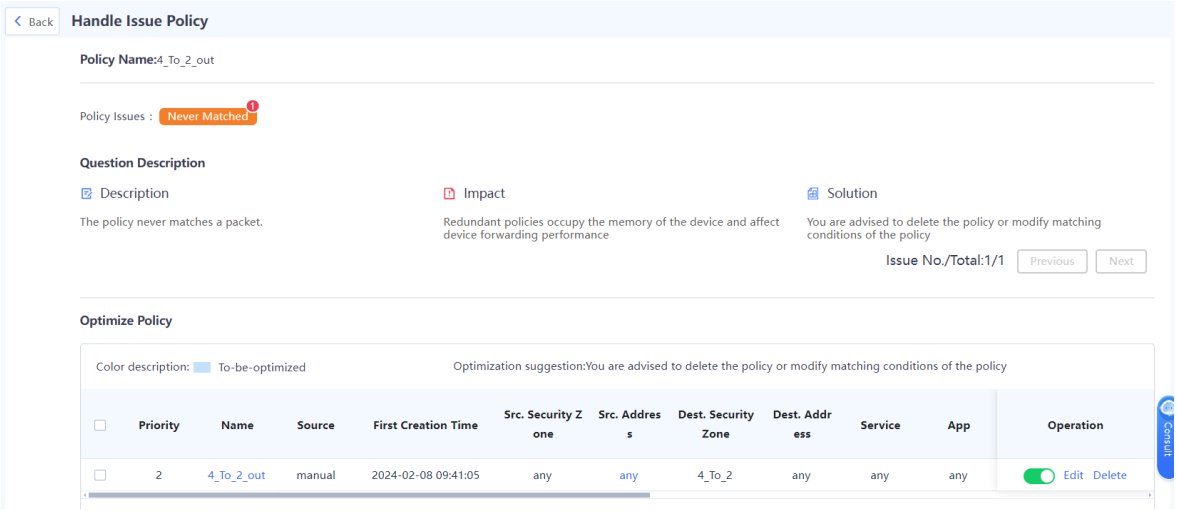
After analysis is completed, the system displays the issue policy list.



Note

After analyzing security policies using the policy optimization function, the system classifies the issues into three levels: major, minor, and to-be-optimized.

(4) Click **Handle** in the **Operation** column of the corresponding policy to view details about the policy.



The details about a specific issue and possible impact are displayed, and the solution is provided to O&M personnel as a reference.

4.1.9 Viewing Policy Life Cycle

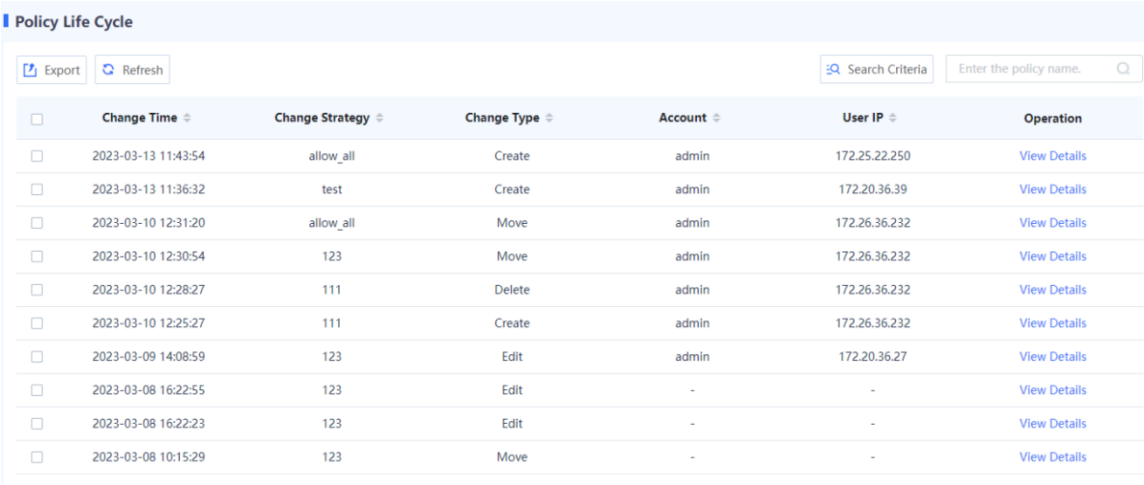
Application Scenario

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

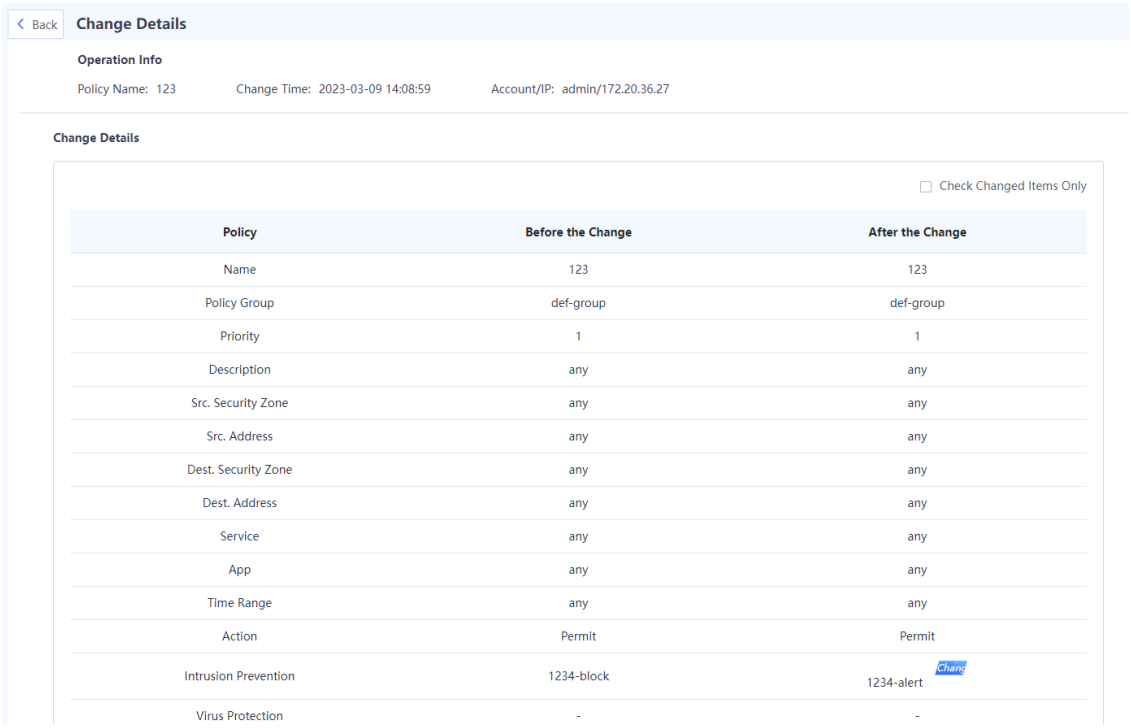
Procedure

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

(2) Click **Policy Life Cycle** in the upper right corner of the operation area.



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



4.1.10 Enabling Basic Protocol Packet Control

Application Scenario

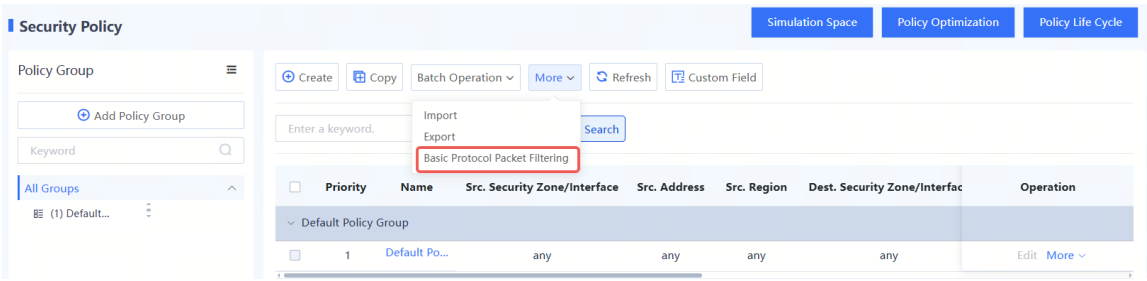
You can enable or disable the basic protocol packet control function of security policies.

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

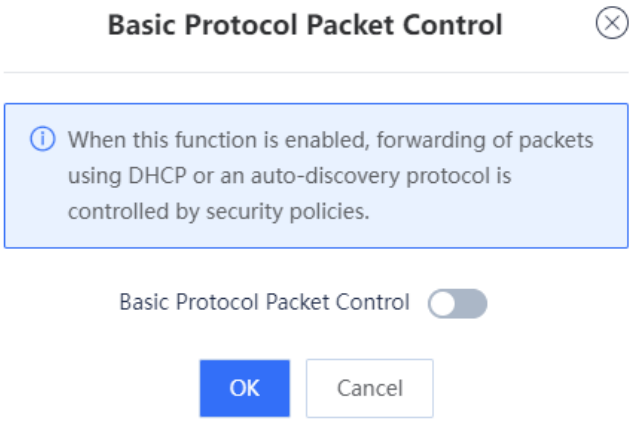
Procedure

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

(2) Click **More** and select **Basic Protocol Packet Filtering** from the drop-down list.



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



(4) Click **OK**.

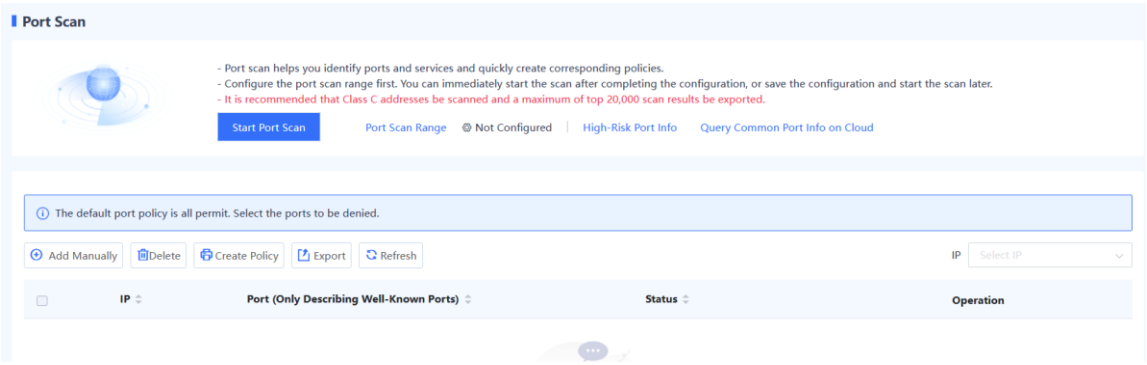
4.2 Enabling Port Scan

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

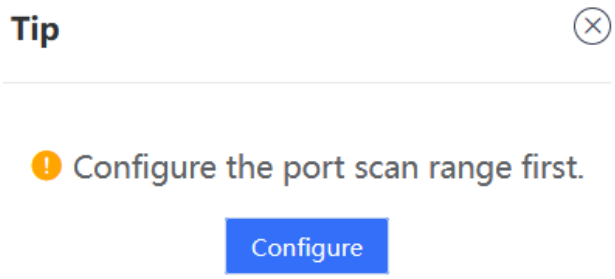
(1) Choose **Policy** > **Port Scan**.



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

a Click **Start Port Scan**.

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

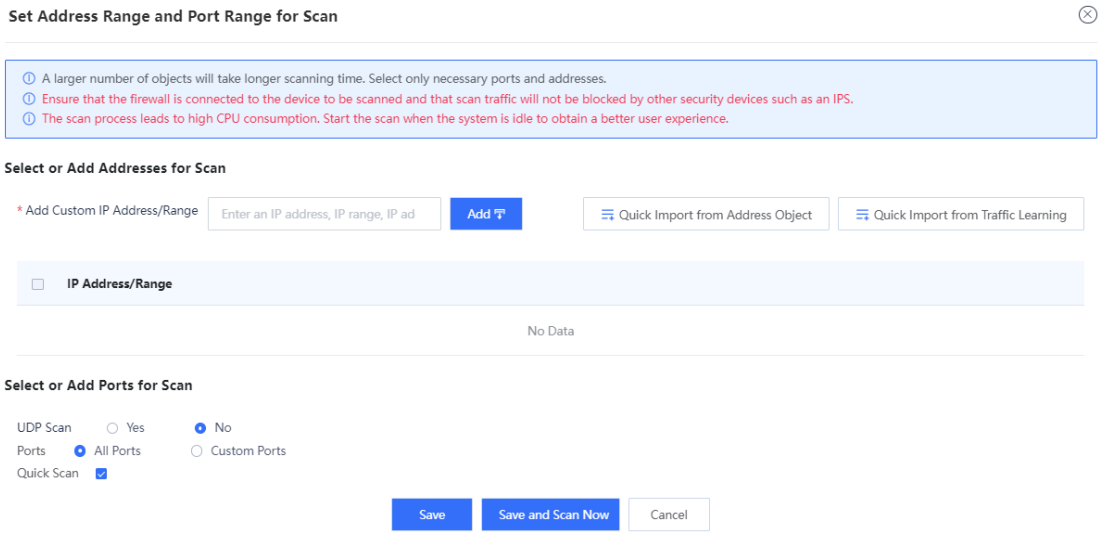


b Select or add the IP address to be scanned.

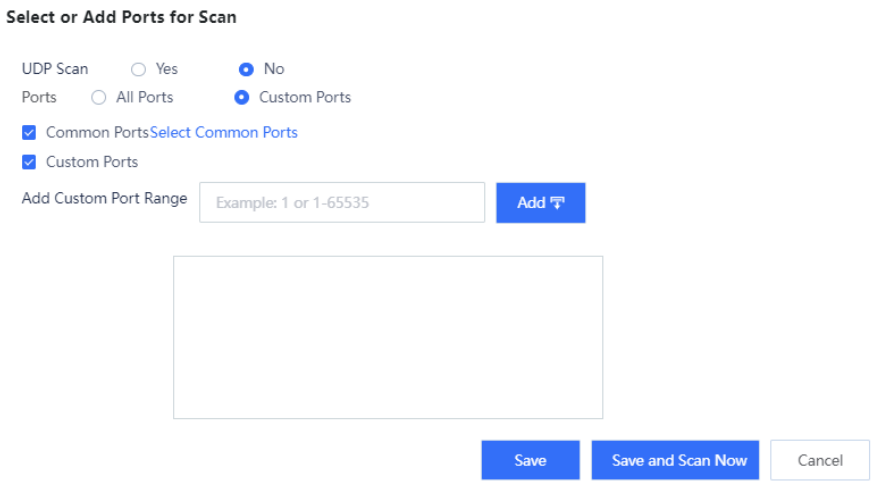
c Enter the IP address or range to be scanned in the **Add Custom IP Address/Range** input box, and click **Add** to add it to the **IP Address/Range** area.

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.



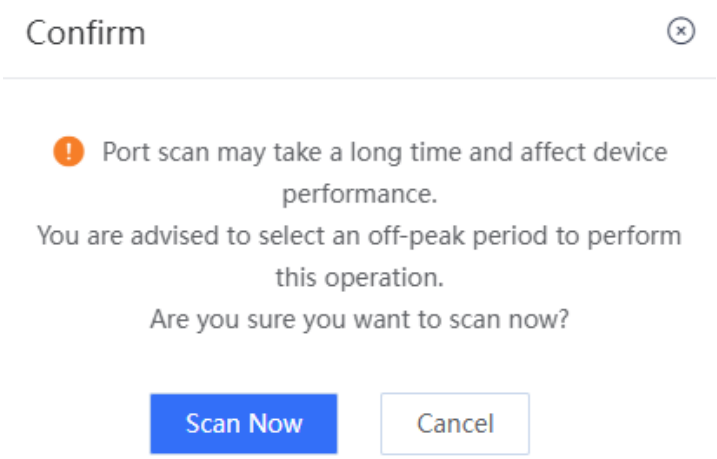
Item	Description	Remarks
UDP Scan	Whether to perform UDP scan.	[Example] Yes
Ports	Select the port to be scanned: ● **All Ports**: Scan all ports. o If **Quick Scan** is selected, a timeout period is set. When the scan starts, all ports other than well-known ports are scanned first. After the timeout period expires, only well-known ports are scanned, regardless of whether the other ports have been scanned. o If **Quick Scan** is not selected, no timeout period is set and all ports (including well-known ports) are scanned. ● **Custom Ports**: Customize the ports to be scanned. o Select **Common Ports** to add common service ports. You can click **Select Common Port**s to select common service ports. o 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.

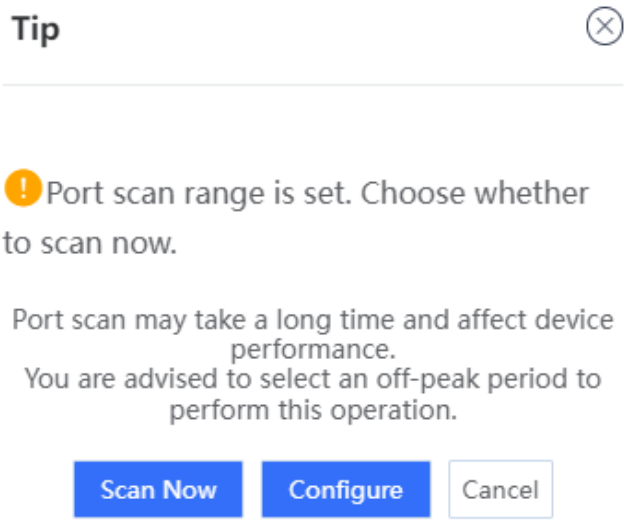
Confirm the system prompt and click **Scan Now.**



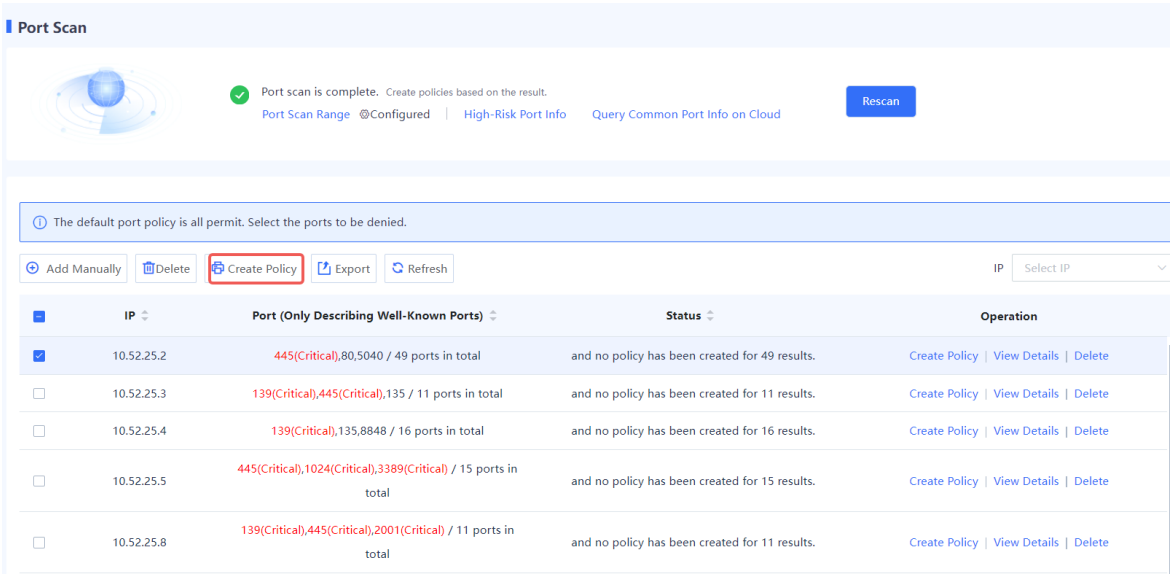
(3) (Optional) If port scan policy has been configured:

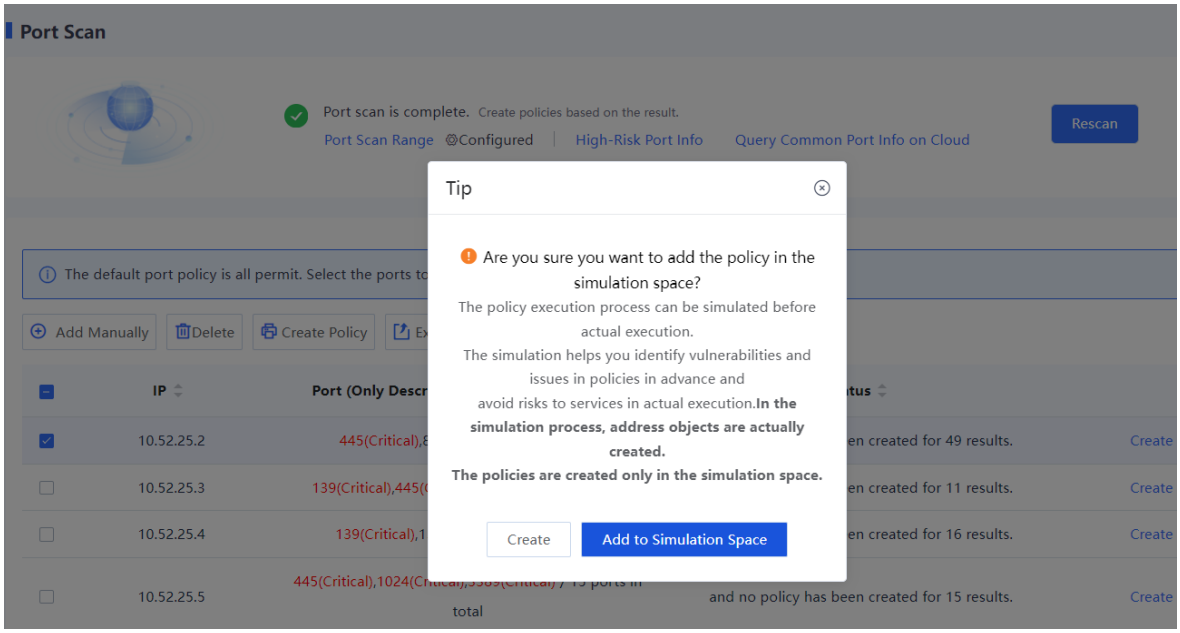
a Click **Start Port Scan**.

b Click **Scan Now** to start port scan.

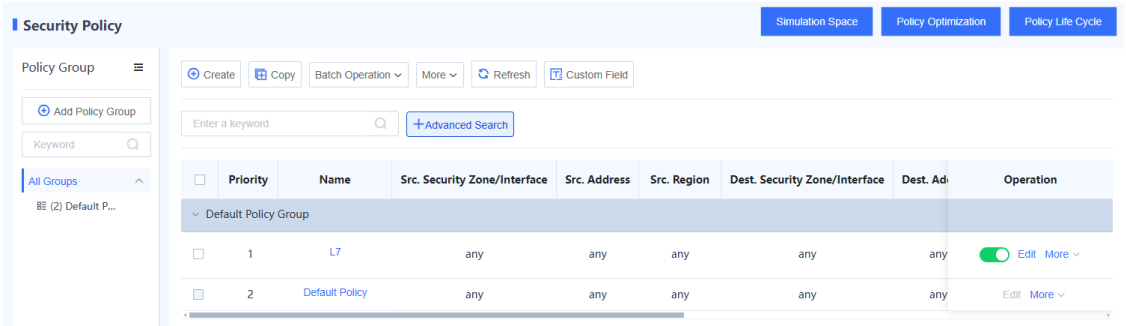


(4) When port scan is finished, select the scan result and click **Create Policy**.



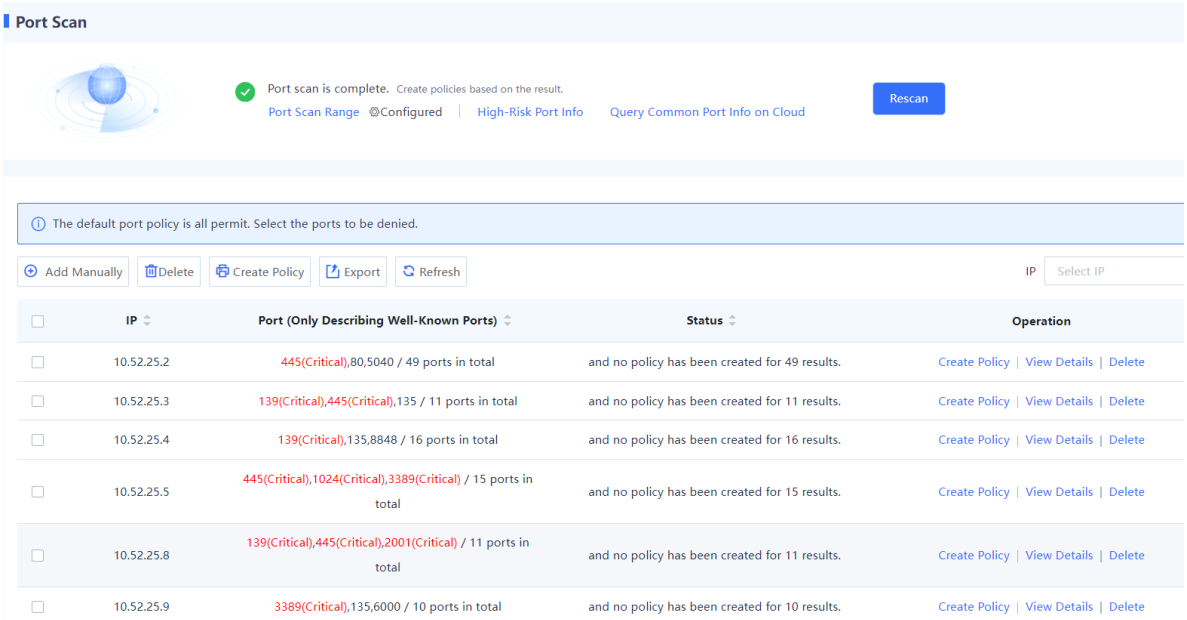


- Click **Create** to add the generated security policy to the security policy list.



- 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



- The device supports query of high-risk ports and common ports for you to check risk details and common port information. Click **High-Risk Port Info** to view the port numbers, service names, risk levels, and other information of all high-risk ports. Click **Query Common Port Info on Cloud** to view the port numbers, service names, and protocols of all common service ports on Ruijie Secure Cloud Platform.
- 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 **Delete** to delete the scan result.
- Click **Export** to generate and export a table that contains the contents of the three fields: IP address, port number, and protocol. A maximum of the top 20,000 scan results can be exported.

4.3 Enabling Traffic Learning

Application Scenario

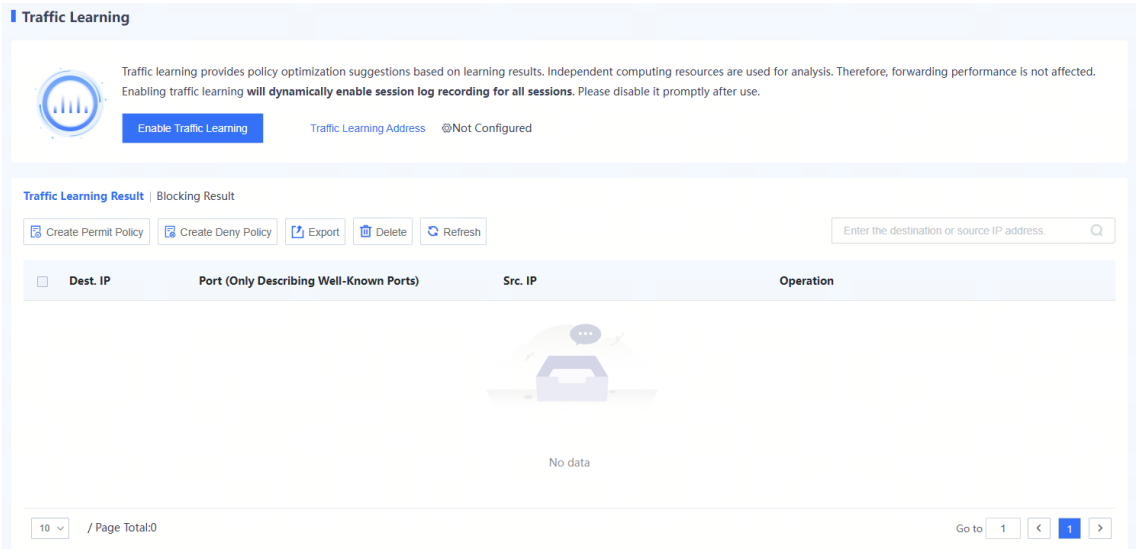
During device deployment, you can sort out the assets on the network only after analyzing the traffic logs in a certain period. The traffic learning function automatically analyzes traffic logs, and sorts out the asset IP addresses, open ports, and access relationships between assets on the network based on the configured asset IP addresses or IP address ranges.

Precautions

After a hard disk is installed on the device, if traffic learning is enabled, the session log recording function is also enabled for all security policies in the system background. (On the web UI, the associated switch is not toggled on.) Disable traffic learning in time after operations in this section are completed.

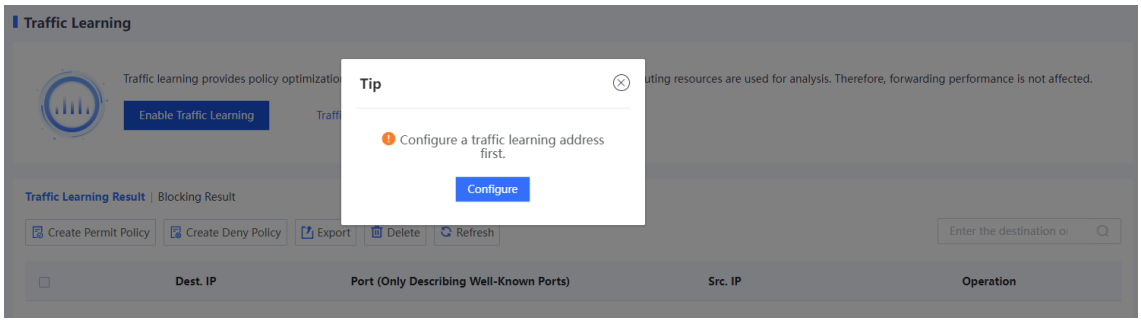
Procedure

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



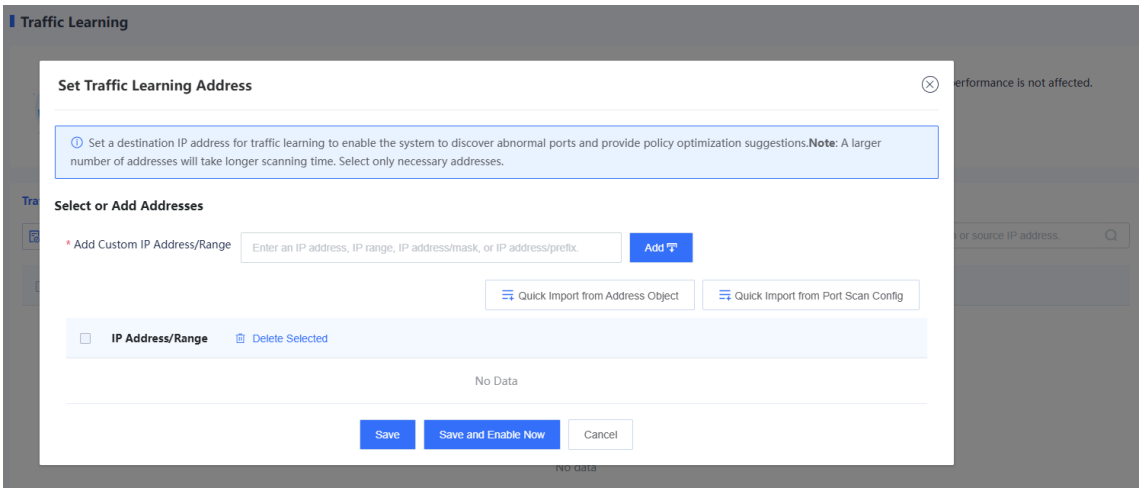
(2) (Optional) If the traffic learning address is not configured, configure it first.

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**.



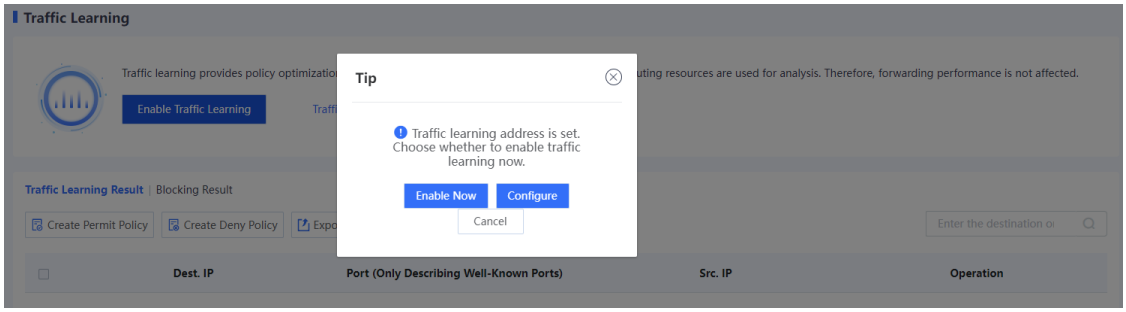
Note

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.

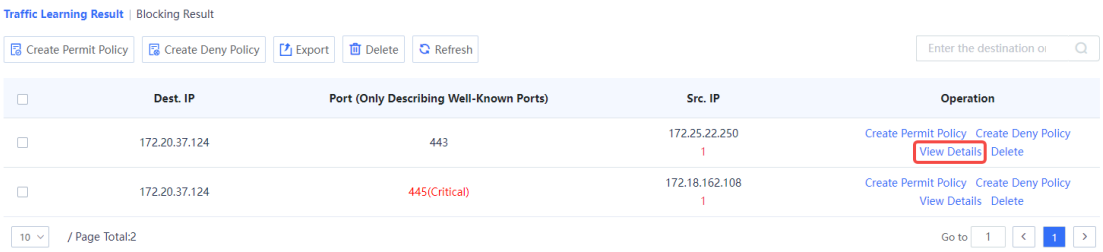
- When services are busy, click **Save** to save the traffic learning address configuration. You can enable traffic learning when services are idle.
- When services are idle, click **Save and Enable Now** to save the traffic learning address configuration and enable traffic learning immediately.

(3) (Optional) If the traffic learning address has been configured, click **Enable Traffic Learning** to modify the traffic learning address or enable traffic learning immediately.



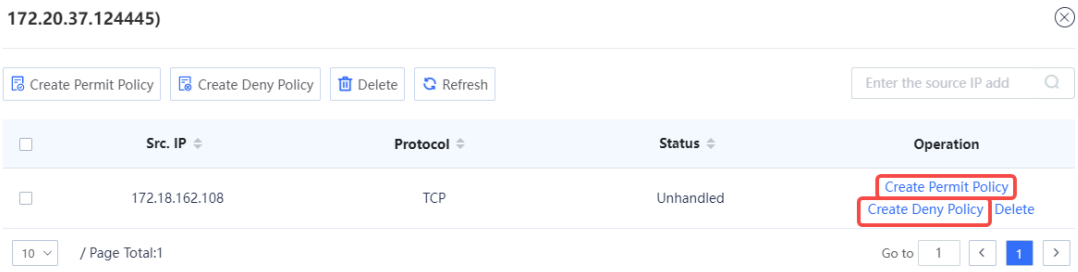
Verification

- 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**.

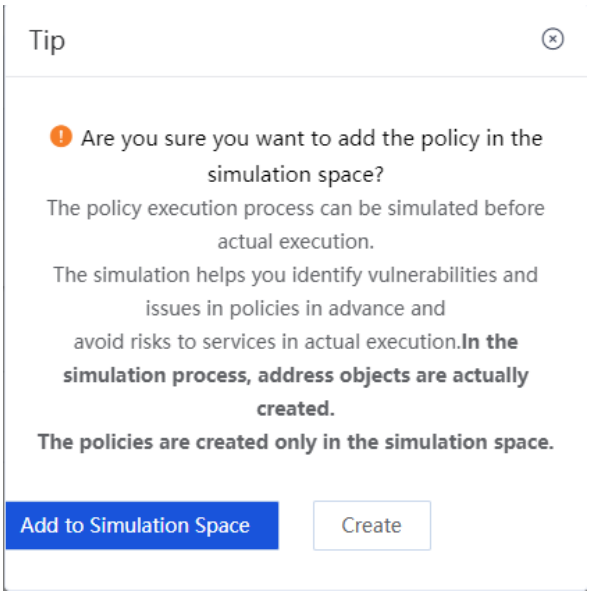


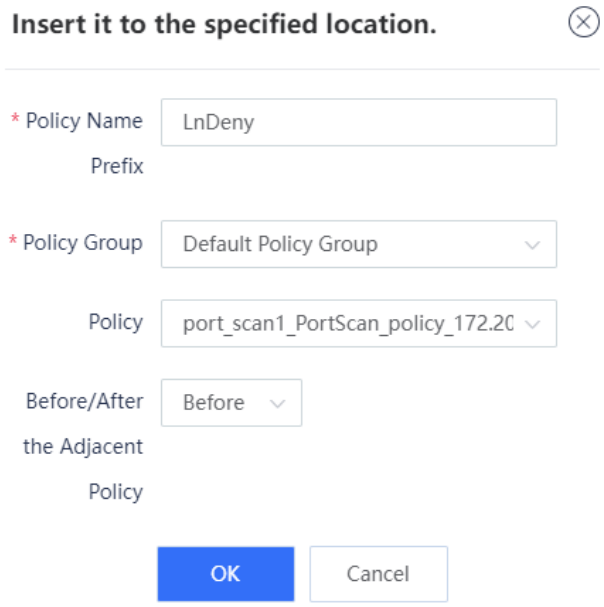
- You can choose to generate a deny policy or a permit policy for a specific traffic learning result.

  a On the traffic learning result page, click **Create Deny Policy** or **Create Permit Policy**.

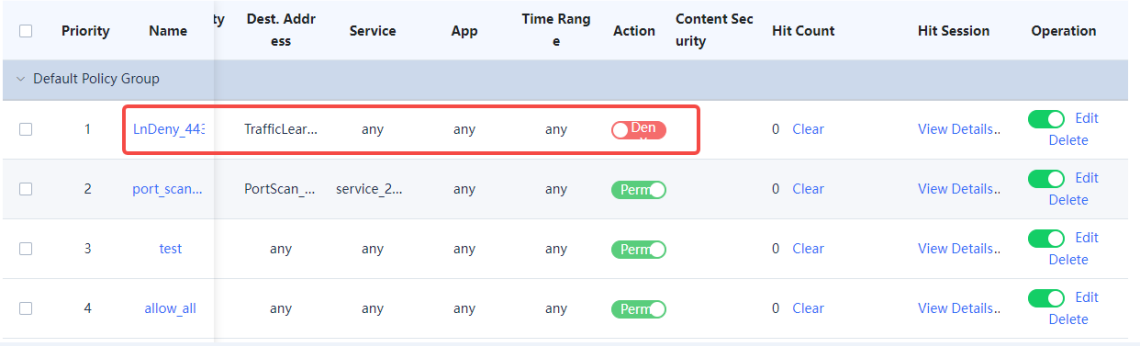


  b Add this policy to the simulation space or directly to the security policy list according to service requirements.

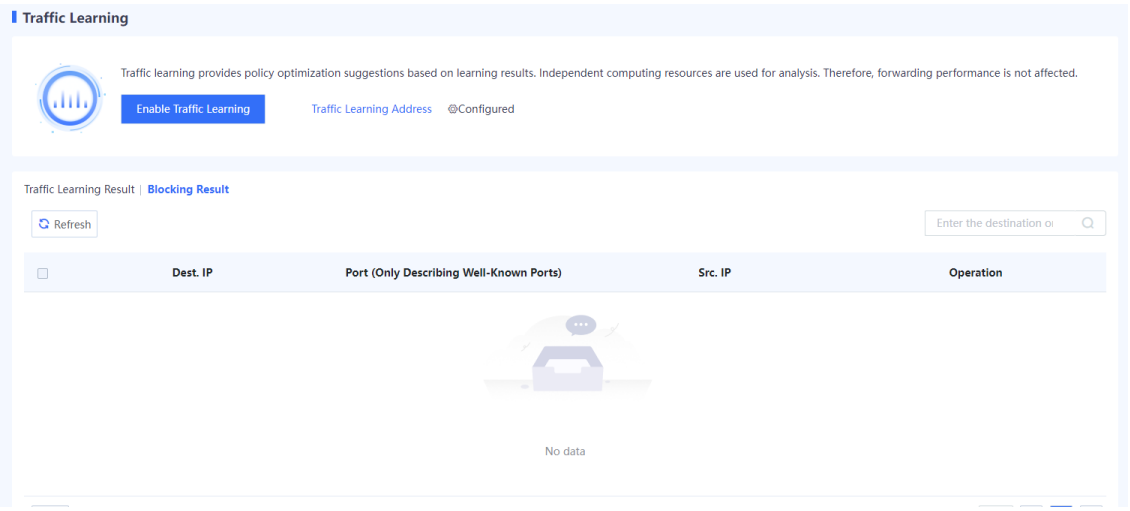




c After confirming that the policy is appropriate in the simulation space, add it to the security policy list.



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**.



4.4 Traffic Control Policy

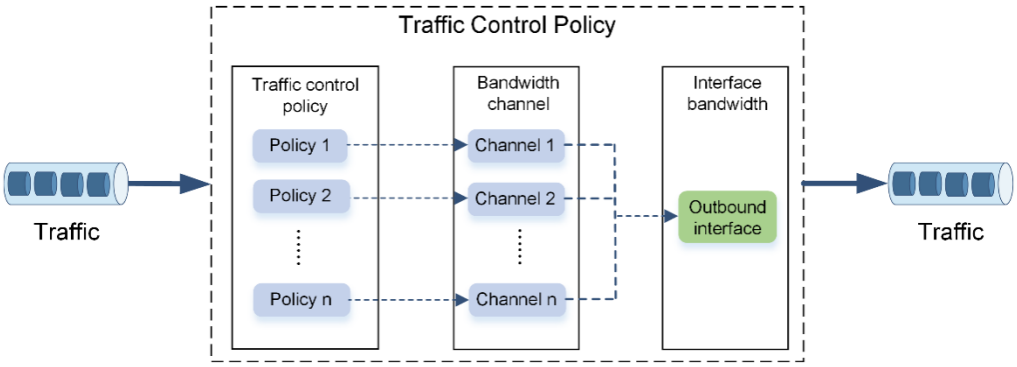
4.4.1 Overview

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: specifics the uplink and downlink bandwidth resources to be referenced by traffic control policies.
- Line bandwidth: specifics 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.

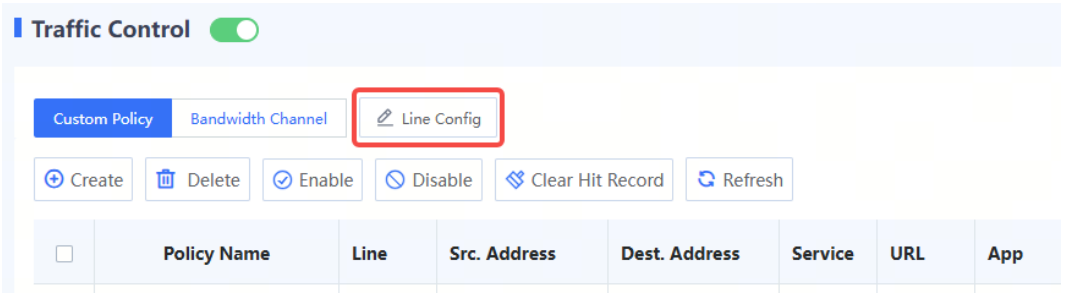
(4) When the traffic is sent out through the outbound interface, it is limited by the egress bandwidth. When traffic from multiple bandwidth channels is simultaneously forwarded by an interface and the actual traffic exceeds the interface bandwidth, the device forwards packets with higher priority first, 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.

4.4.2 Configuring Traffic Control Policies

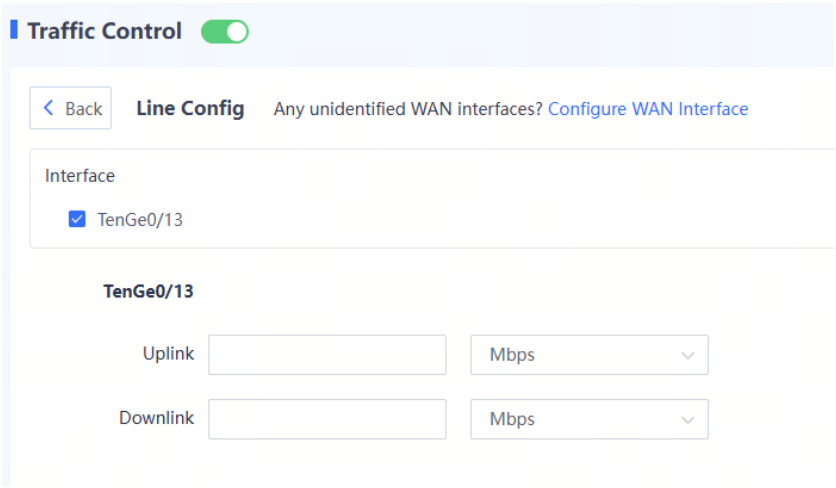
1. Configuring Egress Bandwidth

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

(2) Toggle on to enable traffic control.



(3) Click **Line Config**. Select an outbound interface and configure uplink and downlink bandwidth limits.



Note

The outbound interface must be a WAN interface.

(4) Click **Save**.

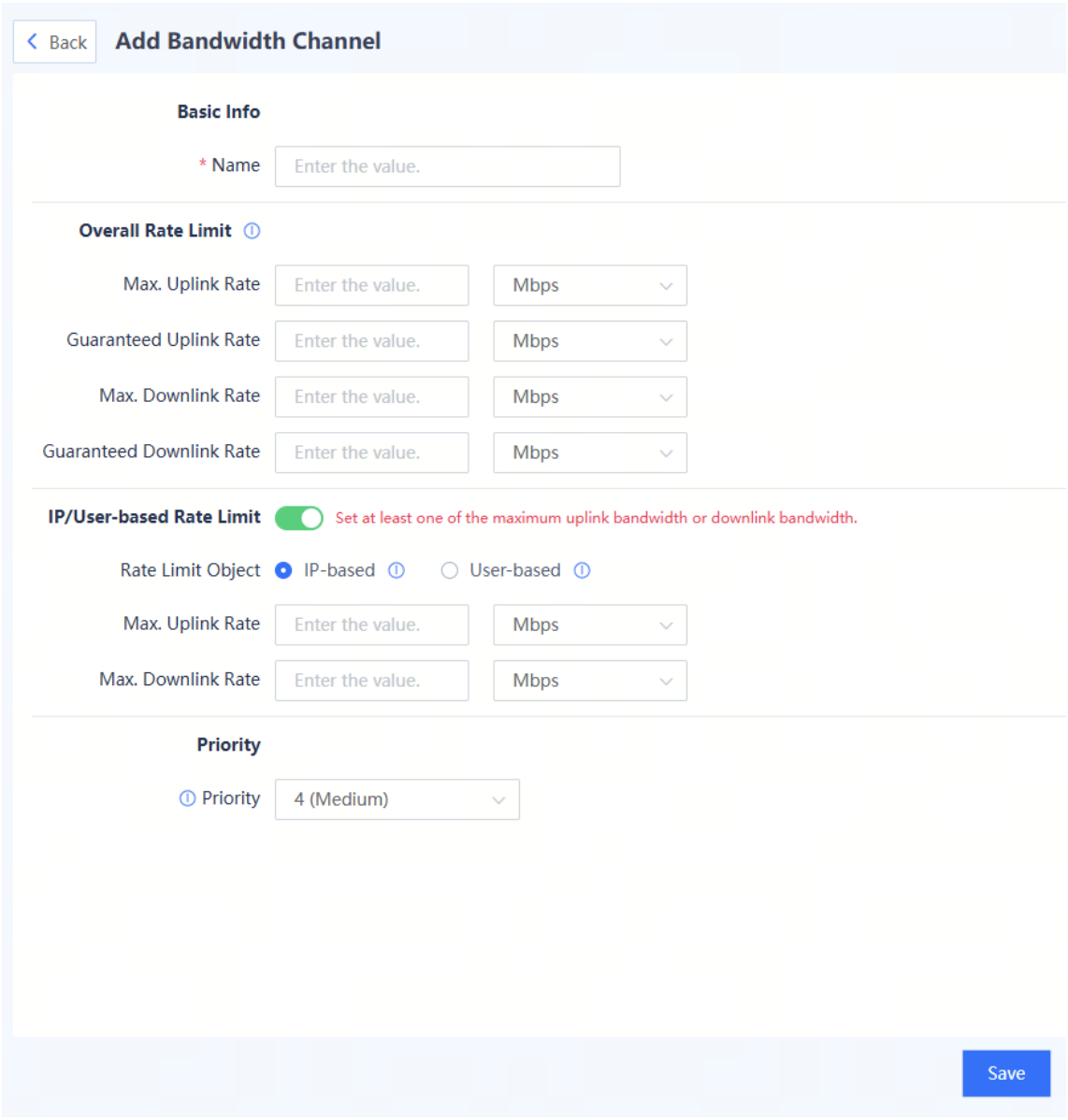
2. Configuring Bandwidth Channels

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

(2) Click the **Bandwidth Channel**. Click **Create**.



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



Item	Description	Remarks
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

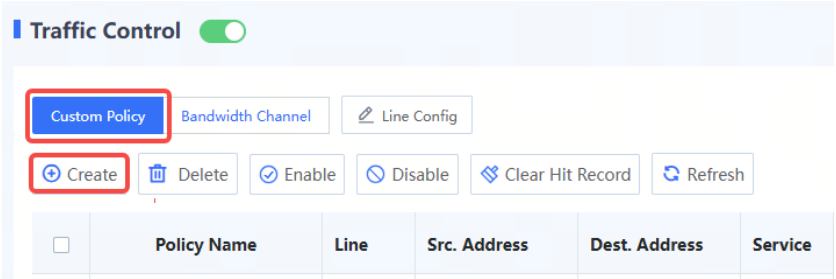
Item	Description	Remarks
Max. Downlink Rate	The maximum bandwidth resource available to the traffic transmitted over the channel. The excessive traffic is discarded. If the parameter is not specified, the traffic is not limited.	[Example] 10 Mbps
Guaranteed Downlink Rate	The minimum bandwidth resource available to the traffic transmitted over the channel. If the parameter is not specified, no bandwidth resource is guaranteed.	[Example] 10 Mbps
IP/User-based Rate Limit ● Toggle on **IP/User-based Rate Limit**. If it is disabled, rate limiting is not applied to each IP address or user. ● After enabling this feature, configure the maximum uplink rate or maximum downlink rate.		
Rate Limit Object	● IP-based: Limits the bandwidth of each IP address in a channel. ● User-based: Limits the bandwidth of each user in a channel. Traffic of unauthenticated users is limited based on the IP address.	[Example] IP-based
Max. Uplink Rate	The maximum bandwidth resource that can be obtained by traffic from a single IP address or user when it enters the channel. The traffic that exceeds the maximum uplink rate is discarded. If this parameter is not set, IP/user-based rate limiting is not performed.	[Example] 10 Mbps
Max. Downlink Rate	The maximum bandwidth resource that can be obtained by traffic from a single IP address or user when it enters the channel. The traffic that exceeds the maximum downlink rate is discarded. If this parameter is not set, IP/user-based rate limiting is not performed.	[Example] 10 Mbps
Priority	Bandwidth channel priority. When traffic from multiple bandwidth channels is simultaneously forwarded by an interface and traffic congestion occurs on the interface, the device forwards traffic from channels with higher priority first.	[Example] 1

(4) Click **Save**.

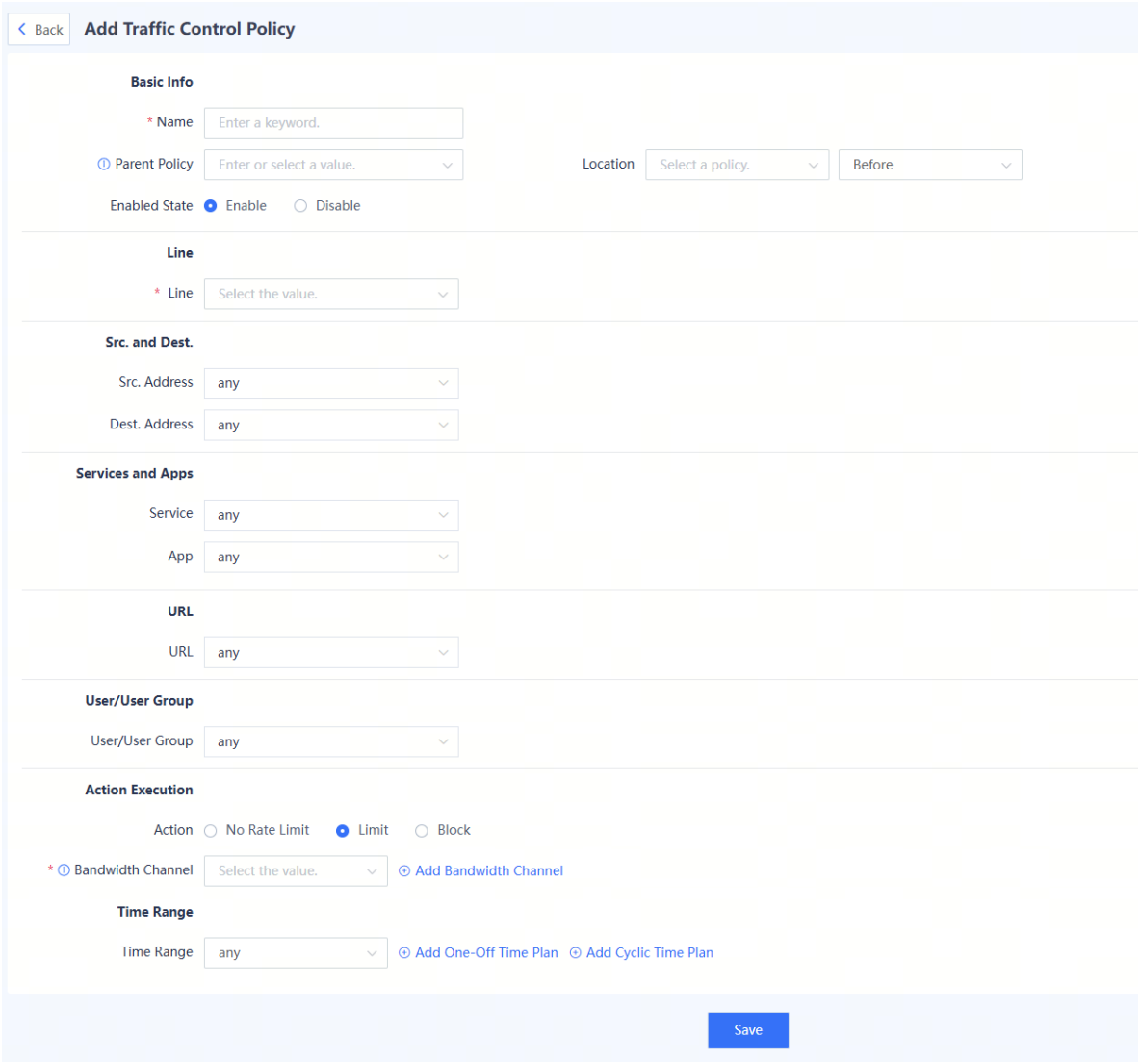
3. Configuring Traffic Control Policies

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

(2) Click **Custom Policy**. Click **Create**.



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



Item	Description	Remarks
Basic Info		
Name	Name of the traffic control policy	[Example] Policy_1

Item	Description	Remarks
Parent Policy	When creating a traffic control policy, you can configure another traffic control policy as its parent policy. In this case, the current policy is a child policy. Traffic is preferentially matched against the parent policy and then the child policy until the lowest level of the child policy is matched. If traffic matches both the parent policy and the child policy, traffic control is performed based on the child policy. If traffic matches only the parent policy but not the child policy, traffic control is performed based on the parent policy. Up to three levels of parent-child policies are supported. For overall rate limiting, note that the maximum uplink or downlink bandwidth of a parent policy must be larger than or equal to that of its child policy, and the maximum uplink or downlink guaranteed bandwidth of a parent policy must be larger than or equal to that of its child policy. The bandwidth channels of the parent policy and its child policy cannot be the same.	Select an existing traffic control policy from the drop-down list.
Location	Move the new policy above or below the specified policy. The closer a policy is to the front, the higher its priority in matching.	Select a policy from the drop-down list.
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
Src. and Dest.		
Src. Address	The traffic with specified source IP addresses matches the policy.	[Example] any
Dest. Address	The traffic destined for the specified IP address or domain name matches 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
Indicates the URL.		
Indicates the URL.	The traffic of specified URLs matches the policy.	[Example] any

Item	Description	Remarks
User/User Group		
User/User Group	The traffic of specified users or user groups matches the policy.	[Example] UserGroup_1
Action Execution		
Action	The action the device performs for the traffic matching the policy. 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.	-
Bandwidth Channel	Define the specific uplink and downlink bandwidth resources.	Select an existing bandwidth channel from the drop-down list box or click **Add Bandwidth Channel** to create a bandwidth channel. For details about the bandwidth channel, see 2. Configuring Bandwidth Channels.
Time Range		
Time Range	Effective time range.	[Example] any

(4) Click **Save**.

4.5 NAT Policy

4.5.1 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).

4.5.2 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.
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.	• 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.

SNAT Type	NAT Content	Application Scenario
PAT (NAPT)	Both IP addresses and port numbers at the transport layer are translated.	● 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.

4.5.3 Working Principle

1. NAT64 Prefix

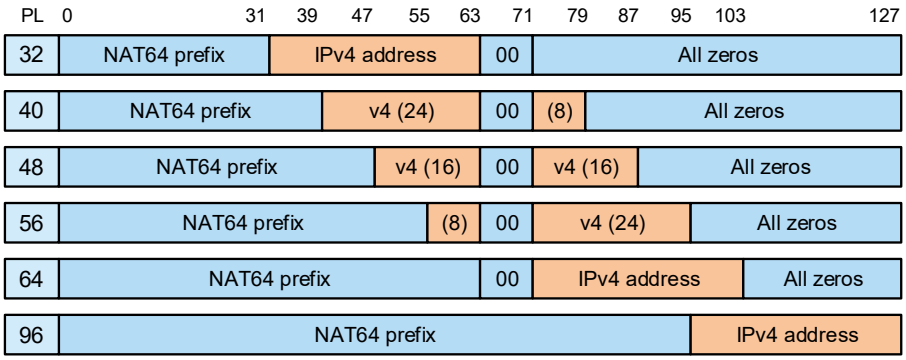
The NAT64 prefix is an IPv6 address prefix with a length of 32, 40, 48, 56, 64 or 96 bits. It is used to construct an IPv6 address of an IPv4 node on an IPv6 network in NAT46/NAT64, thereby enabling communication between IPv4 and IPv6 networks. When an IPv4 host initiates an access request packet, the 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 4-1, 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 4-1 IPv6 Address Formats for Different NAT64 Prefix Lengths



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

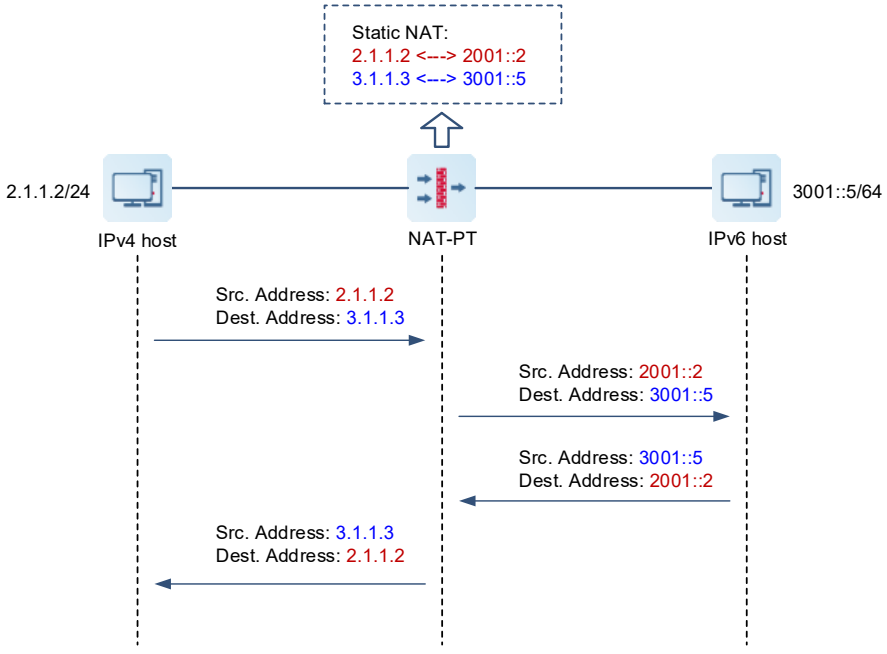
Network Address Translation-Protocol Translation (NAT-PT) enables communication between IPv6 and IPv4 networks. It integrates and evolves from Stateless IP/ICMP Translation (SIIT) and Network Address Translation (NAT). SIIT provides 1:1 mapping for translation between IPv4 and IPv6 addresses. Based on 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 4-2 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

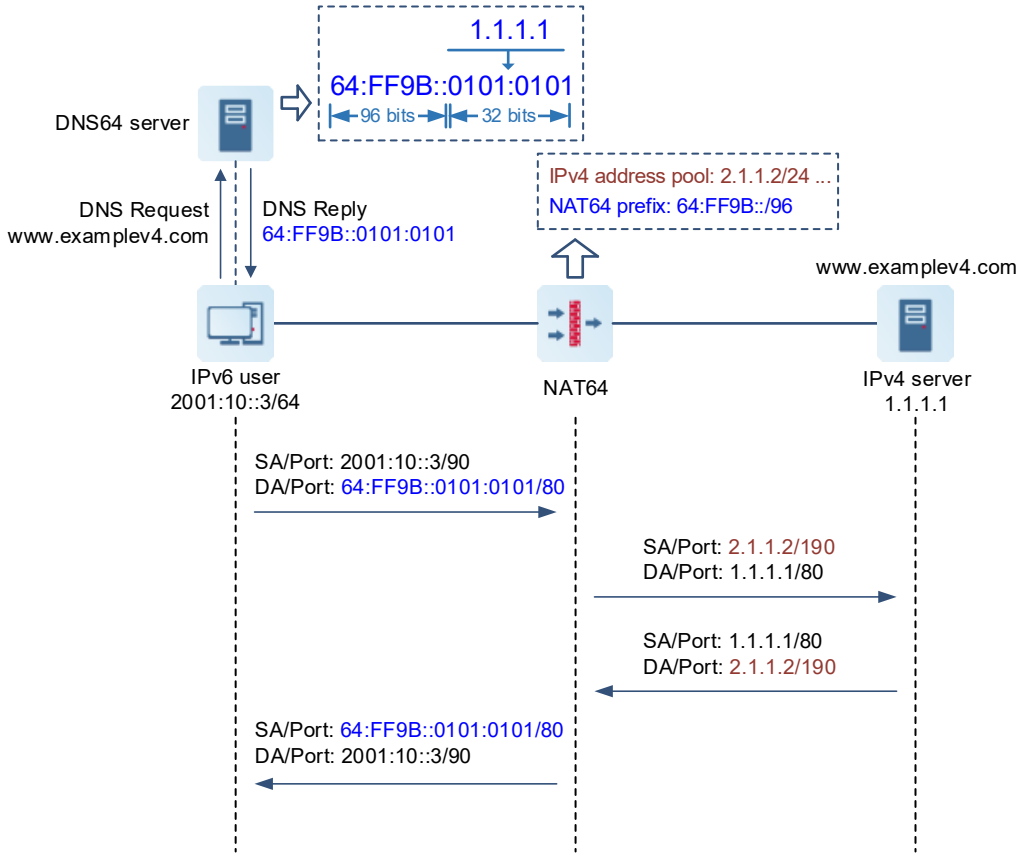
NAT-PT enables communication between IPv6 and IPv4 networks through network address and protocol translation. However, NAT-PT has many limitations. For example, it cannot translate the option in the IPv4 header or provide end-to-end security. To eliminate the limitations in NAT-PT, the Internet Engineering 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 4-3 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.

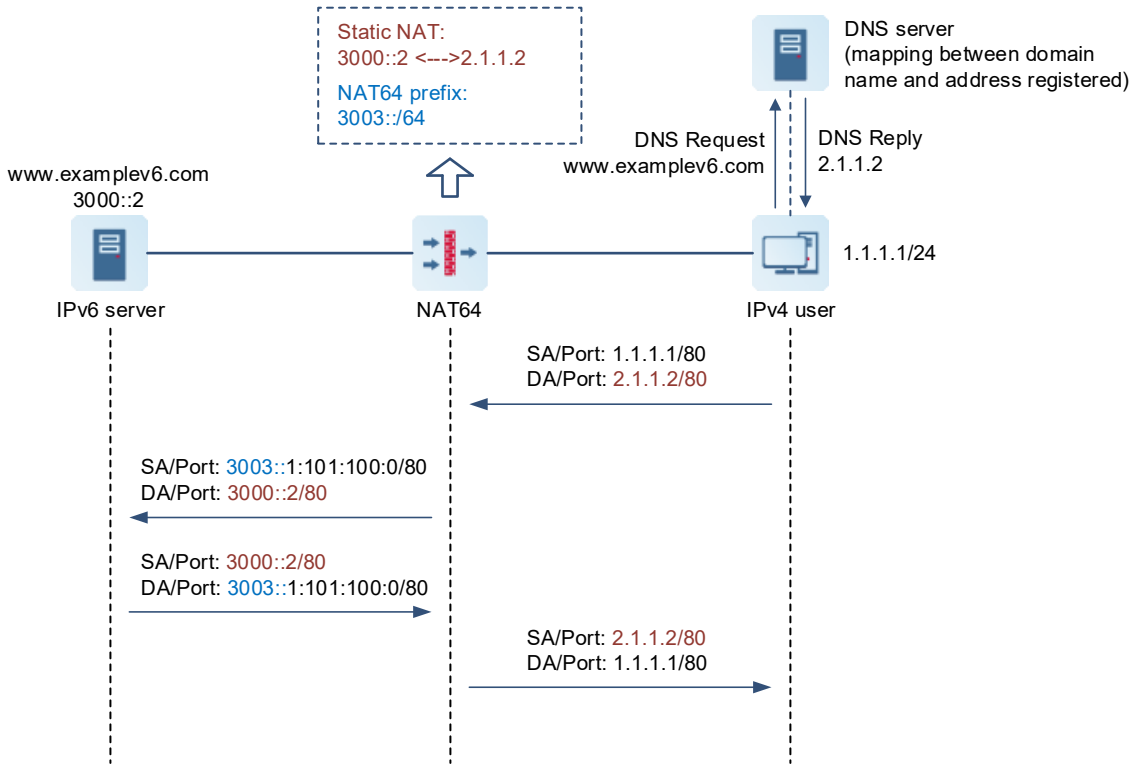
(5) The NAT64 device sends the IPv4 packet to the IPv4 server and creates a session table for storing the mappings between the IPv6 and IPv4 addresses.

(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 4-4 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 external networks.
- Destination NPTv6: translates destination IPv6 addresses for external networks to access services provided by intranet hosts.

4.5.4 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 external networks.

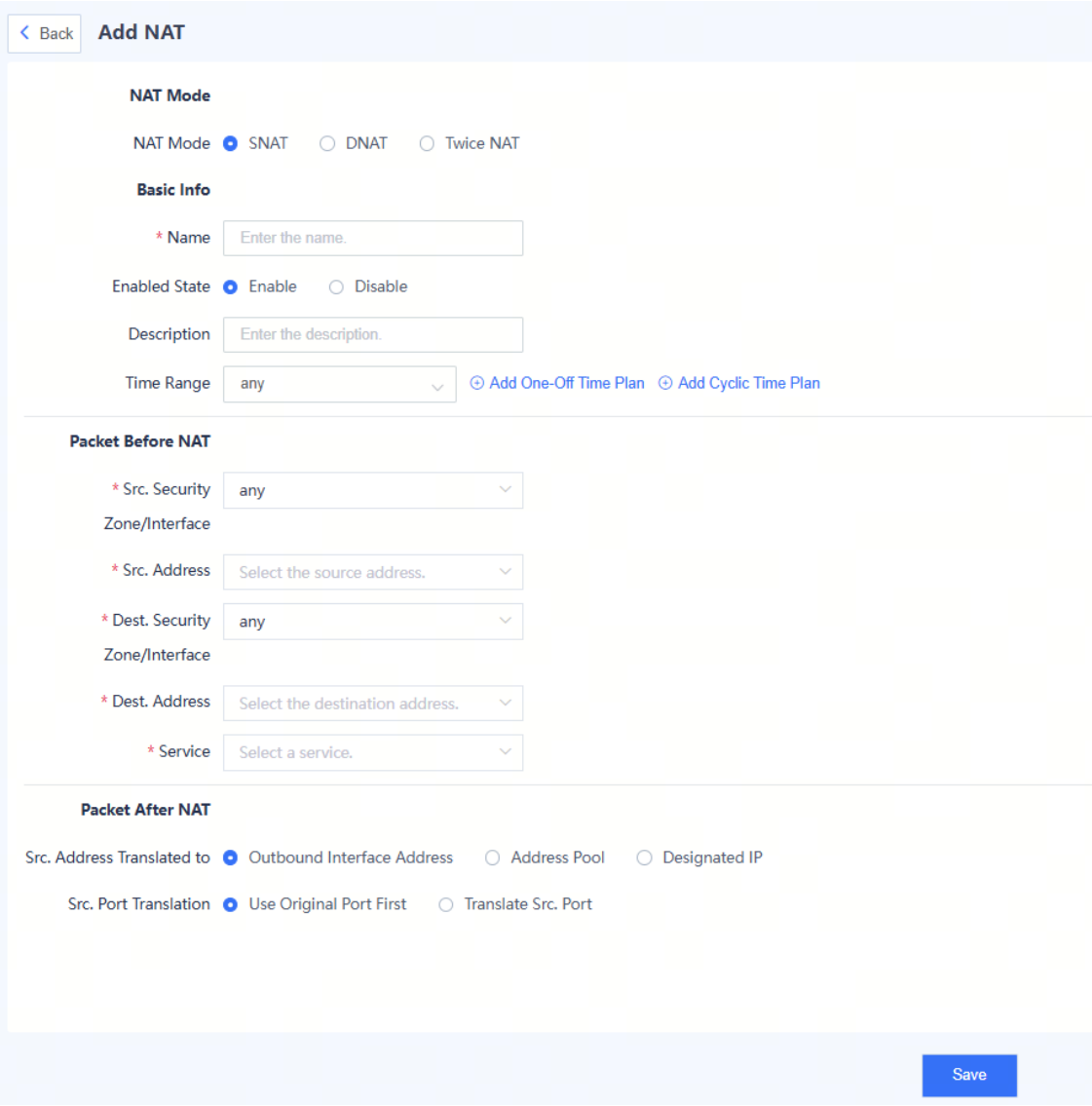
SNAT translates private network IP addresses into public network IP addresses so that private network users can use public network addresses to access the Internet.

Procedure

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

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

On the **Add NAT** page that is displayed, set **NAT Mode** to **SNAT**.



(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. ● **SNAT**: source address translation ● **DNAT**: destination address translation ● **Twice NAT**: source and destination address translation	[Example] SNAT
Basic Info		
Name	Name of the NAT policy.	[Example] NAT_policy_1

Item	Description	Remarks
Enabled State	Whether to enable the NAT policy immediately after configuration is completed.	[Example] Enable
Description	Description of the NAT policy.	[Example] NAT policy_1
Time Range	Time range in which the NAT policy is effective.	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/Interface	NAT is performed for packets from these security zones or interfaces.	**Any** indicates all interfaces. [Example] any
Src. Address	NAT is performed for packets from these addresses.	[Example] any
Dest. Security Zone/Interface	NAT is performed for packets sent to these security zones or interfaces.	**Any** indicates all interfaces. [Example] any
Dest. Address	NAT is performed for packets sent to these addresses.	[Example] any
Service	NAT is performed for packets of these services.	● 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. ● Click **Add Service** to create a custom service. [Example] any
Packet After NAT		

Item	Description	Remarks
Src. Address Translated to	Select the translated source address type based on the scenario. Valid values: ● Address Pool Set an address pool. ● Designated IP You need to specify an IP address and the source port translation mode. If **Use Original Port First** is selected, the device preferentially uses the original port for traffic forwarding. If the original port is occupied, the source port is randomly translated into an unused port. If **Translate Src. Port** is selected, the source port is randomly translated into an unused port, regardless of whether the original port is occupied. ● Outbound Interface Address You need to configure the source port translation mode, which can be **Use Original Port First** or **Translate Src. Port**.	[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

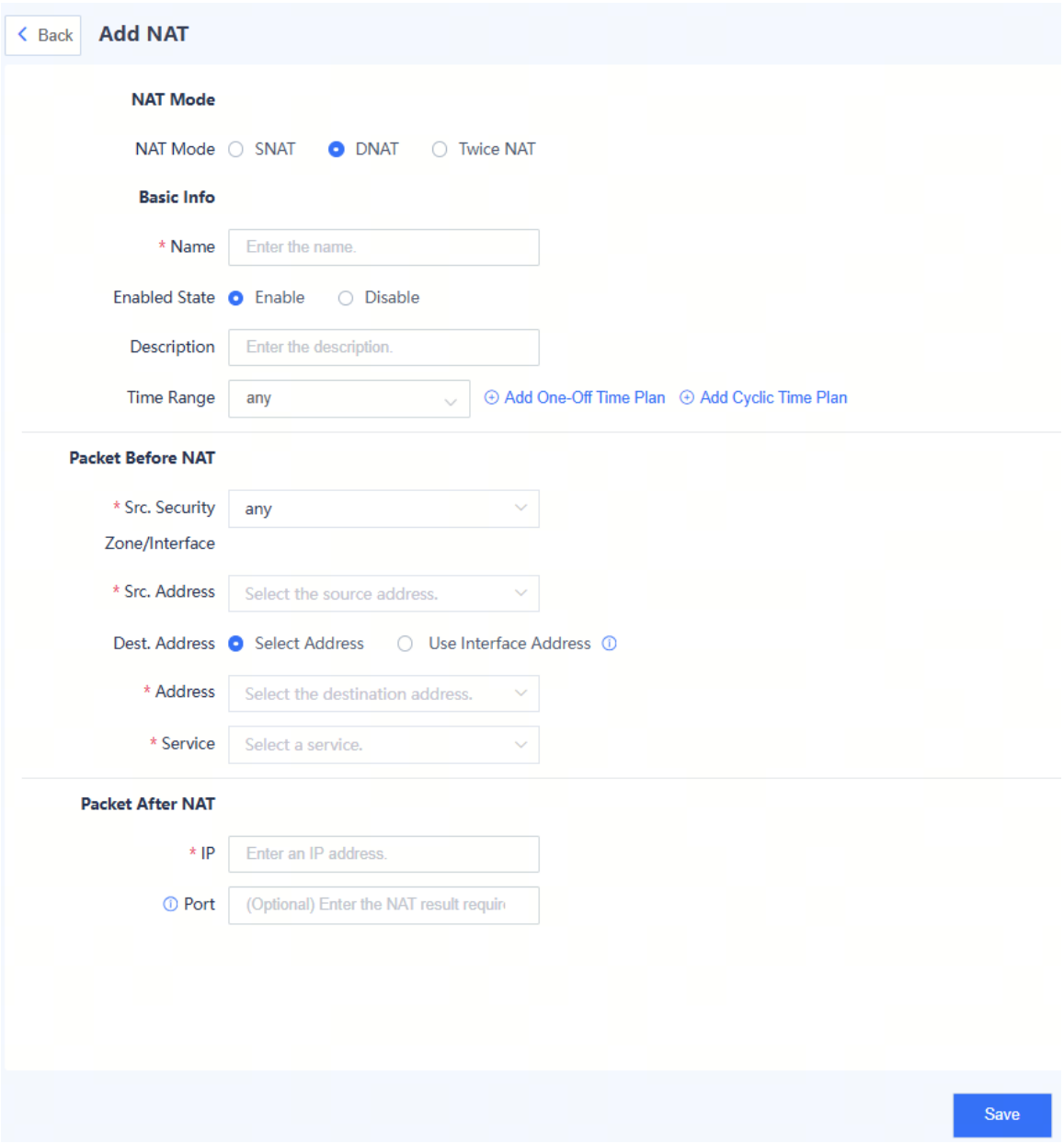
DNAT refers to the translation of the destination address and port number in a packet, which is typically used to map intranet servers for external networks. DNAT translates public network IP addresses into private network IP addresses so that public network users can use public network addresses to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

Procedure

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

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

On the **Add NAT** page that is displayed, set **NAT Mode** to **DNAT**.



(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. ● **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.	[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.	[Example] NAT policy_1
Time Range	Time range in which the NAT policy is effective.	● 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/Interface	NAT is performed for packets from these security zones or interfaces.	**Any** indicates all interfaces. [Example] any
Src. Address	NAT is performed for packets from these addresses.	[Example] any
Dest. Address	NAT is performed for packets sent to such addresses or interfaces.	[Example] Select an address.
Address	NAT is performed for packets sent to these addresses.	[Example] any

Item	Description	Remarks
Interface	NAT is performed for packets sent to such interfaces. It applies to the scenario where a device does not have a fixed external IP address for a service interface (for example, PPPoE dial-up or DHCP connection) and DDNS must also be used: (1) Configure DDNS mapping on an interface and bind a domain name. (2) Select **Use Interface Address** and select the corresponding interface. (3) Access the mapped service based on the dynamically bound domain name of DDNS to implement fixed-domain name access (IP address is variable).	Select an interface from the drop-down list box. Only the interface assigned with an IP address takes effect.
Service	NAT is performed for packets of these services.	● 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. ● Click **Add Service** to create a custom service. [Example] any
Packet After NAT		
IP address	Translated destination IP address.	[Example] 192.168.10.30
Port	Translated destination port number.	[Example] 80

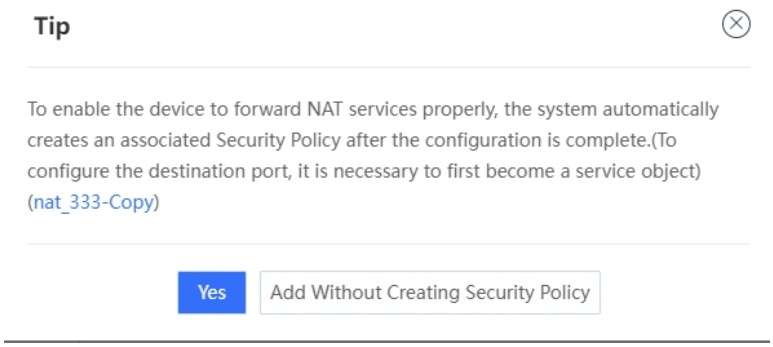
(4) Click **Save**. A dialog box is displayed, prompting you to determine whether to add a corresponding security policy.

Click **Yes**. A security policy is automatically associated and added on the security policy page to permit NAT traffic.

Click **Add Without Creating Security Policy** to add a NAT policy without adding an associated security policy.

Caution

If a security policy is not automatically associated or added, you need to manually configure a security policy to permit NAT traffic. Otherwise, NAT fails.



Follow-up Procedure

- If the destination address fails to be translated using NAT, you can use the port mapping fault diagnosis tool to troubleshoot the fault. For details, see 8.6.1 2. Port Mapping Exception Diagnostics.
- 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.

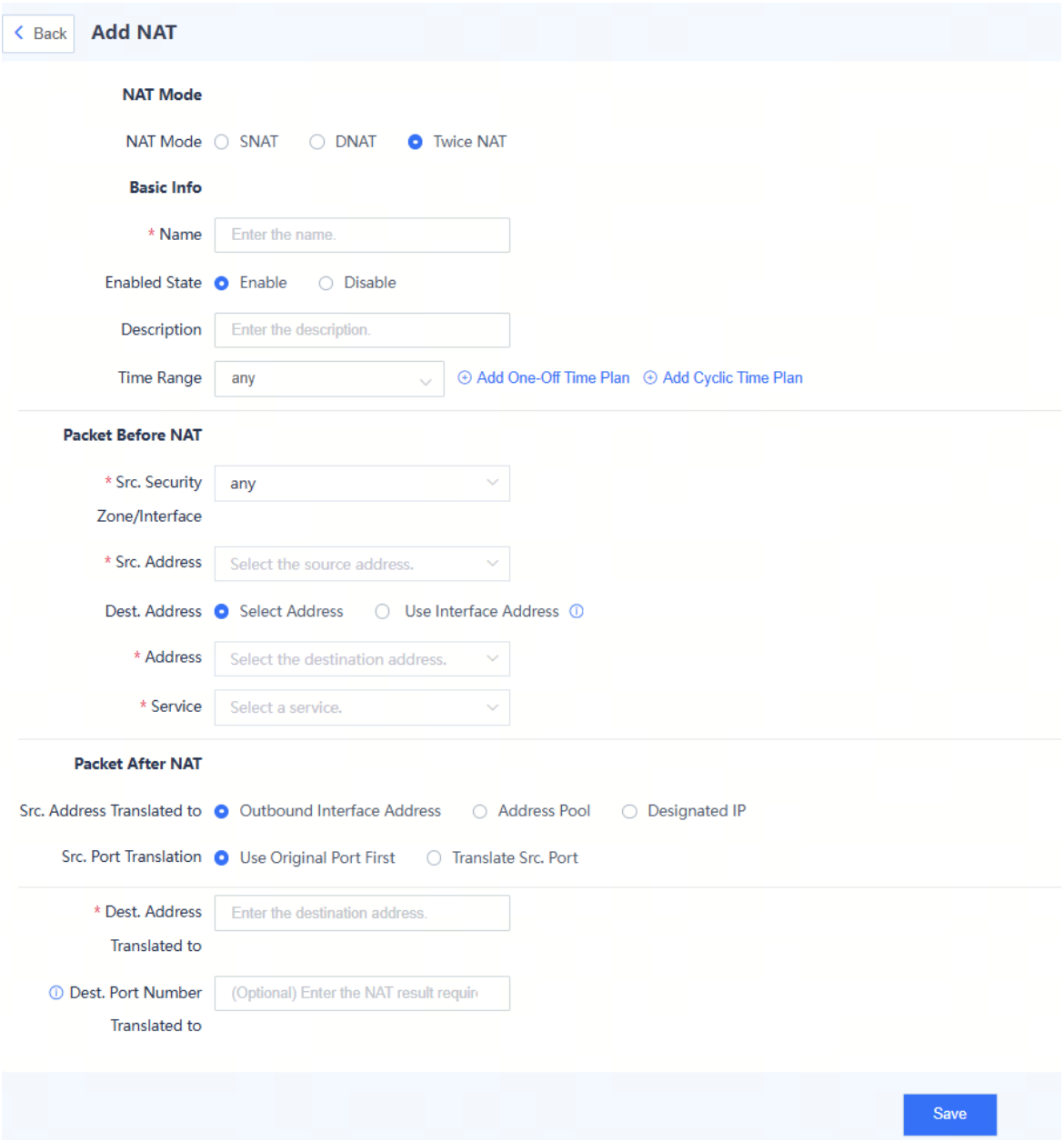
It applies to a scenario where intranet PCs need to use public network addresses to access intranet servers.

Procedure

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

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

On the **Add NAT** page that is displayed, set **NAT Mode** to **Twice NAT**.



(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. ● **SNAT**: source address translation ● **DNAT**: destination address translation ● **Twice NAT**: source and destination address translation	[Example] Twice NAT

Item	Description	Remarks
Basic Info		
Name	Name of the NAT policy.	[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.	[Example] NAT policy_1
Time Range	Time range in which the NAT policy is effective.	● 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/Interface	NAT is performed for packets from these security zones or interfaces.	**Any** indicates all interfaces. [Example] any
Src. Address	NAT is performed for packets from these addresses.	[Example] any
Dest. Address	NAT is performed for packets sent to such addresses or interfaces.	[Example] Select an address.
Address	NAT is performed for packets sent to these addresses.	[Example] any

Item	Description	Remarks
Interface	NAT is performed for packets sent to such interfaces. It applies to the scenario where a device does not have a fixed external IP address for a service interface (for example, PPPoE dial-up or DHCP connection) and DDNS must also be used: (1) Configure DDNS mapping on an interface and bind a domain name. (2) Select **Use Interface Address** and select the corresponding interface. (3) Access the mapped service based on the dynamically bound domain name of DDNS to implement fixed-domain name access (IP address is variable).	Select an interface from the drop-down list box. Only the interface assigned with an IP address takes effect.
Service	NAT is performed for packets of these services.	● 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. ● Click **Add Service** to create a custom service. [Example] any
Packet After NAT		

Item	Description	Remarks
Src. Address Translated to	Select the translated source address type based on the scenario. Valid values: ● Address Pool Set an address pool. ● Designated IP You need to specify an IP address and the source port translation mode. If **Use Original Port First** is selected, the device preferentially uses the original port for traffic forwarding. If the original port is occupied, the source port is randomly translated into an unused port. If **Translate Src. Port** is selected, the source port is randomly translated into an unused port, regardless of whether the original port is occupied. ● Outbound Interface Address You need to configure the source port translation mode, which can be **Use Original Port First** or **Translate Src. Port**.	[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

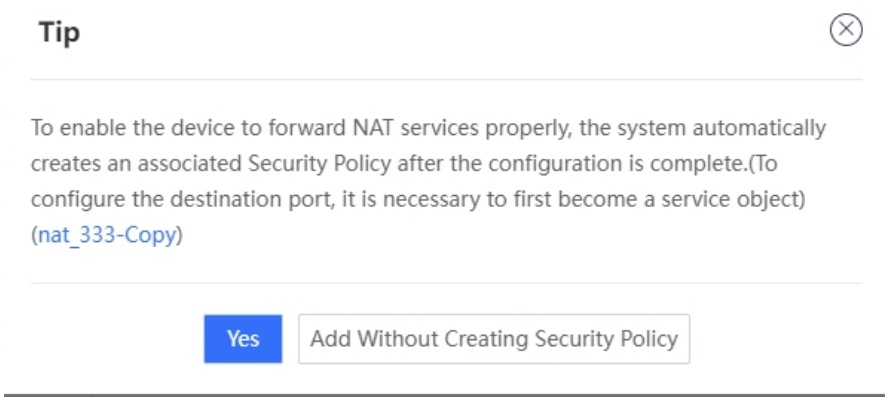
(4) Click **Save**. A dialog box is displayed, prompting you to determine whether to add a corresponding security policy.

Click **Yes**. A security policy is automatically associated and added on the security policy page to permit NAT traffic.

Click **Add Without Creating Security Policy** to add a NAT policy without adding an associated security policy.

Caution

If a security policy is not automatically associated or added, you need to manually configure a security policy to permit NAT traffic. Otherwise, NAT fails.



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

CF series firewalls support fast generation of NAT 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 CF series firewall, you can configure the policy migration tool to obtain the corresponding configuration file.

Note

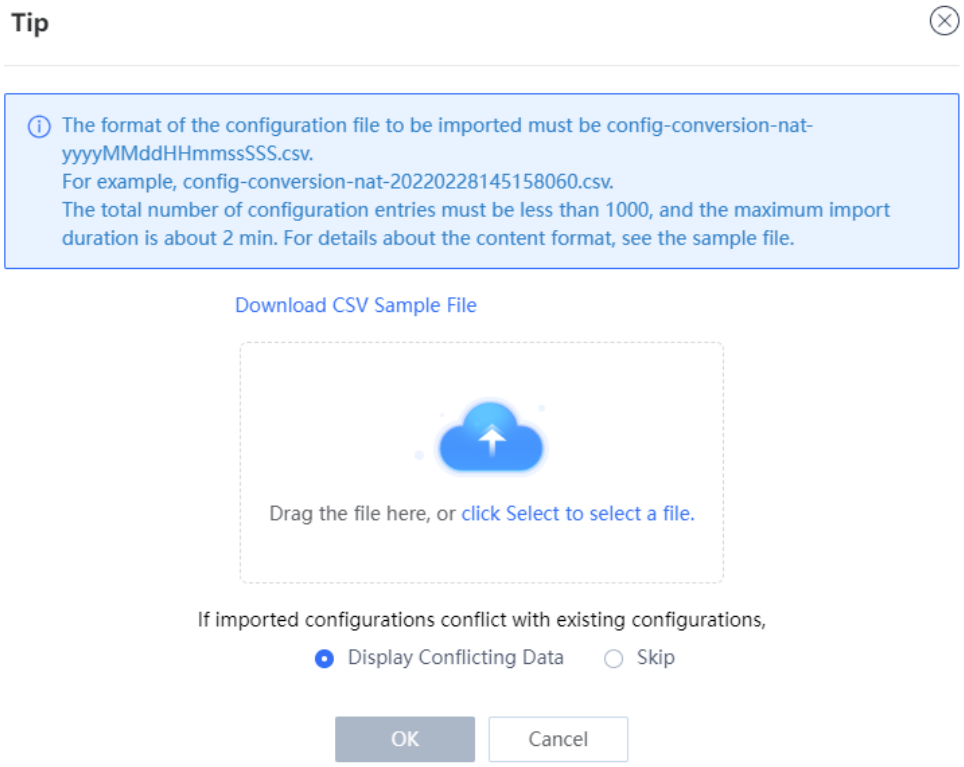
For the usage of the policy migration tool, contact technical support engineers.

Procedure

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

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

A tip dialog box is displayed.



(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.

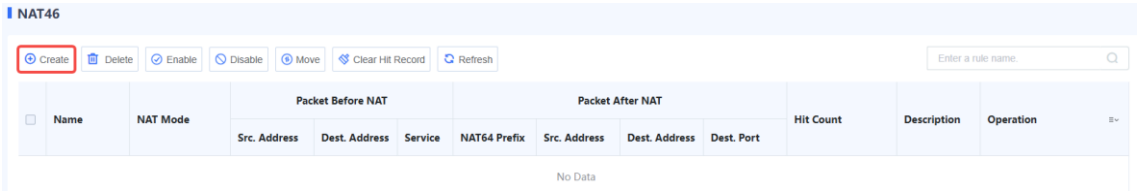
4.5.5 Configuring NAT46

Application Scenario

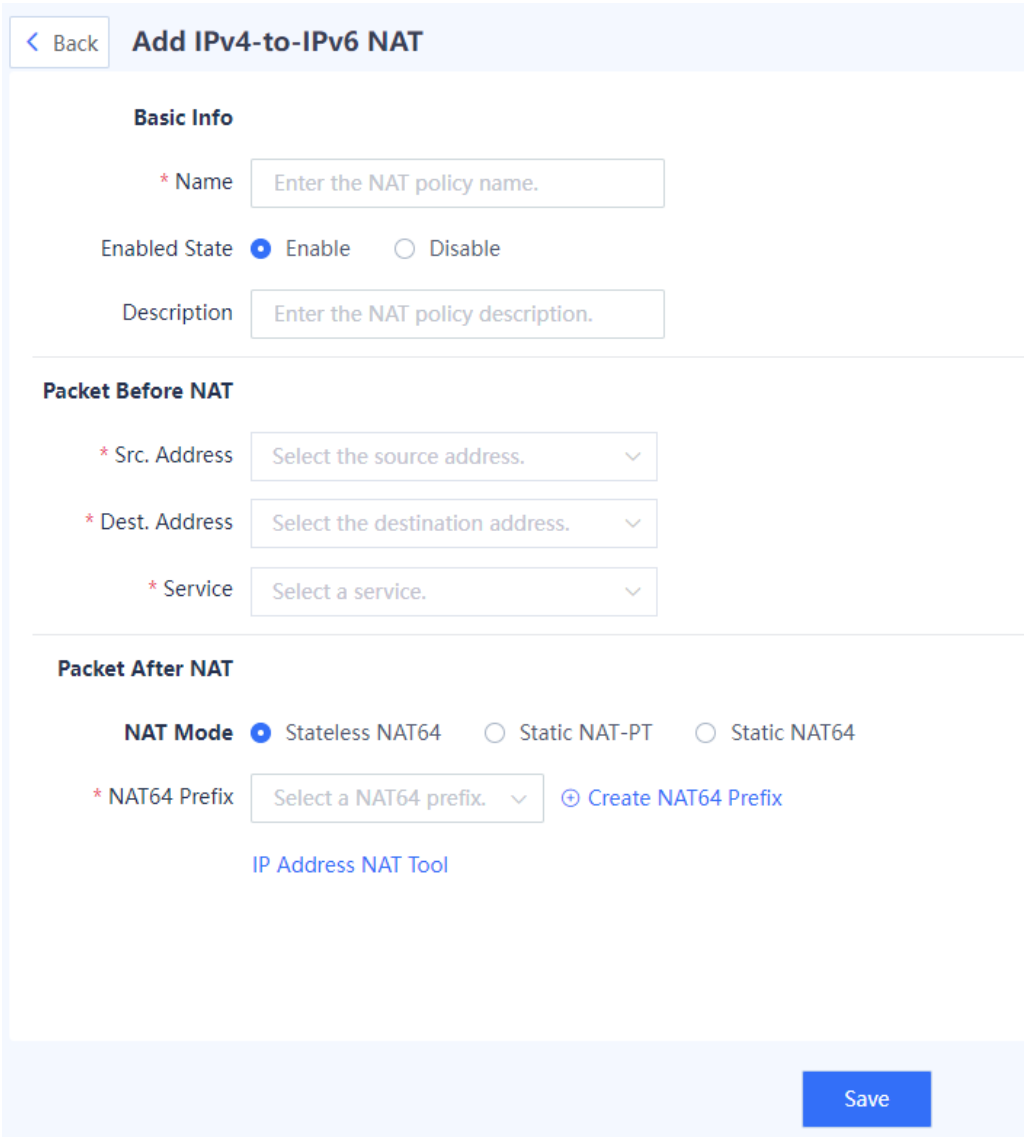
Configure a NAT46 policy to translate source and destination addresses in IPv4 packets to IPv6 addresses, thereby enabling IPv4 hosts to access IPv6 networks.

Procedure

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



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



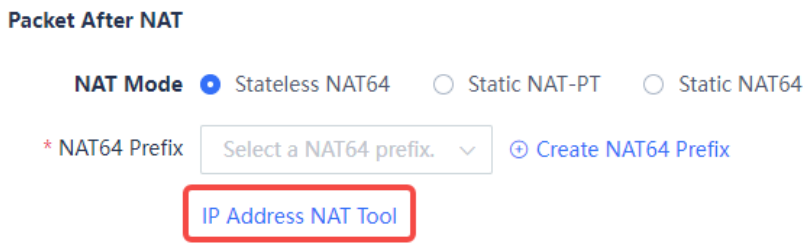
(3) Configure a NAT46 policy. The following table lists the configuration parameters.

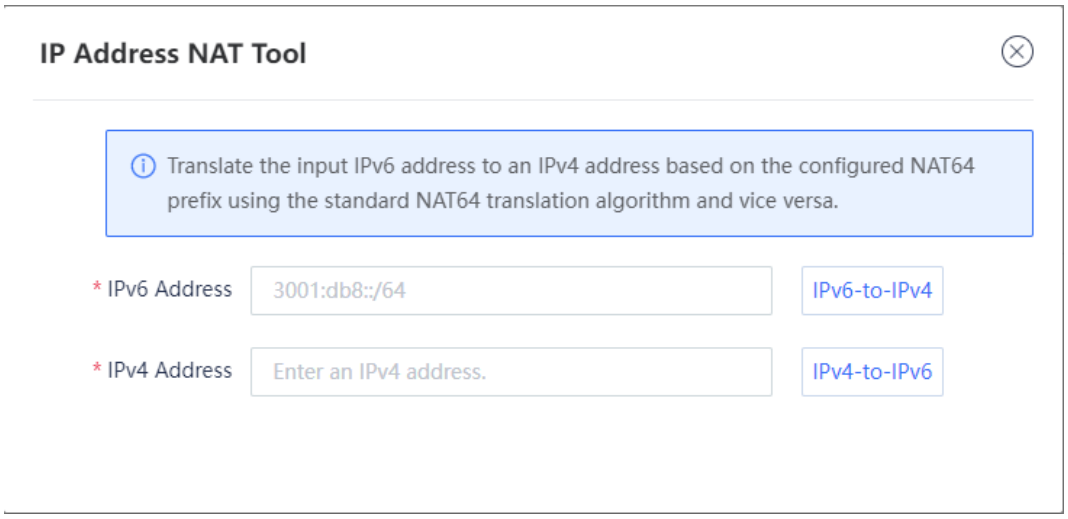
Item	Description	Remarks
Basic Info		
Name	Name of the NAT46 policy.	[Example] NAT46_policy_1
Enabled State	Whether to enable the NAT46 policy immediately after configuration is completed.	[Example] Enable
Description	Description of the NAT46 policy.	[Example] NAT46 policy_1
Packet Before NAT		
Src. Address	NAT is performed for packets from these addresses.	● 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.	● 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.	● 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: ● Stateless NAT64 ● Static NAT-PT ● Static NAT64	For different implementation modes, you need to configure different parameters. [Example] Stateless NAT64

Item	Description	Remarks
NAT Mode: Stateless NAT64.		
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.	● 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.	● 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.	● 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.	● 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.





(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.

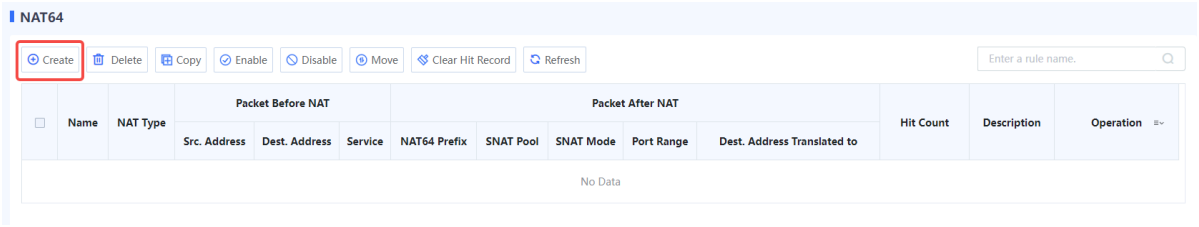
4.5.6 Configuring NAT64

Application Scenario

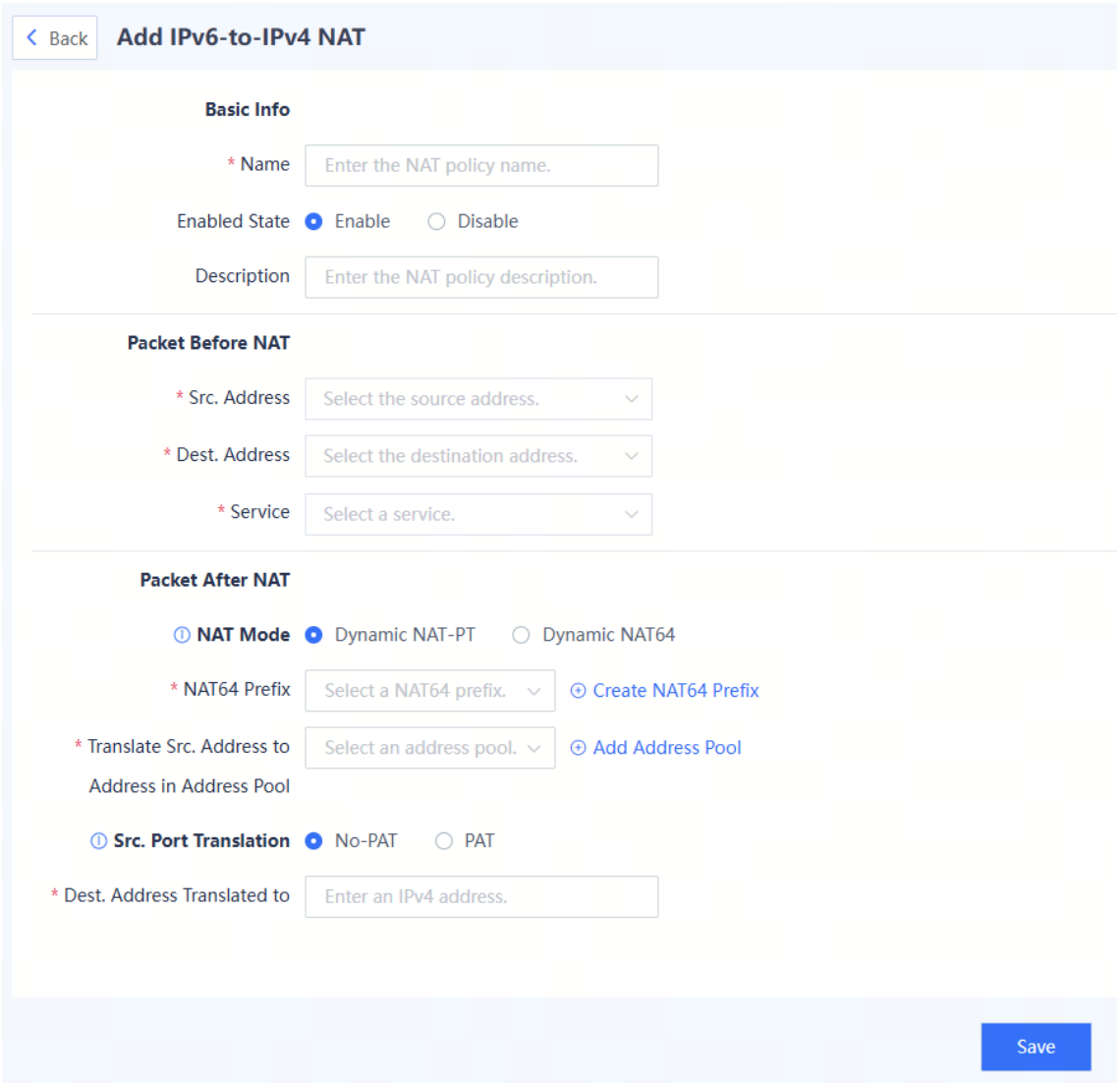
Configure a NAT64 policy to translate source and destination addresses in IPv6 packets to IPv4 addresses, thereby enabling IPv6 hosts to access IPv4 networks.

Procedure

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



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



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

Item	Description	Remarks
Basic Info		
Name	Name of the NAT64 policy.	[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.	[Example] NAT64 policy_1
Packet Before NAT		

Item	Description	Remarks
Src. Address	NAT is performed for packets from these addresses.	• 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. 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. 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.	• 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.	• 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	NAT64 implementation mode. Valid values: Dynamic NAT-PT Dynamic NAT64	For different implementation modes, you need to configure different parameters. [Example] Dynamic NAT64
NAT Mode: Dynamic 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.	• 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.	● 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: **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 to 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.	● 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.	● Click the drop-down list, and select an address pool. ● Click **Add Address Pool** to create a custom address pool. [Example] nat_pool_1

Item	Description	Remarks
SNAT Mode	Whether to translate the transport-layer source port numbers in packets: ● **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 to 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.

4.5.7 Configuring NAT66

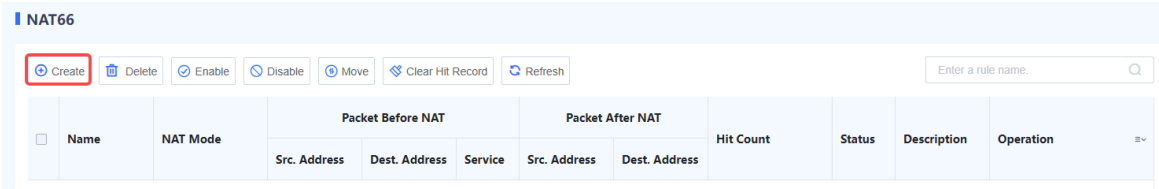
1. Configuring SNAT

Application Scenario

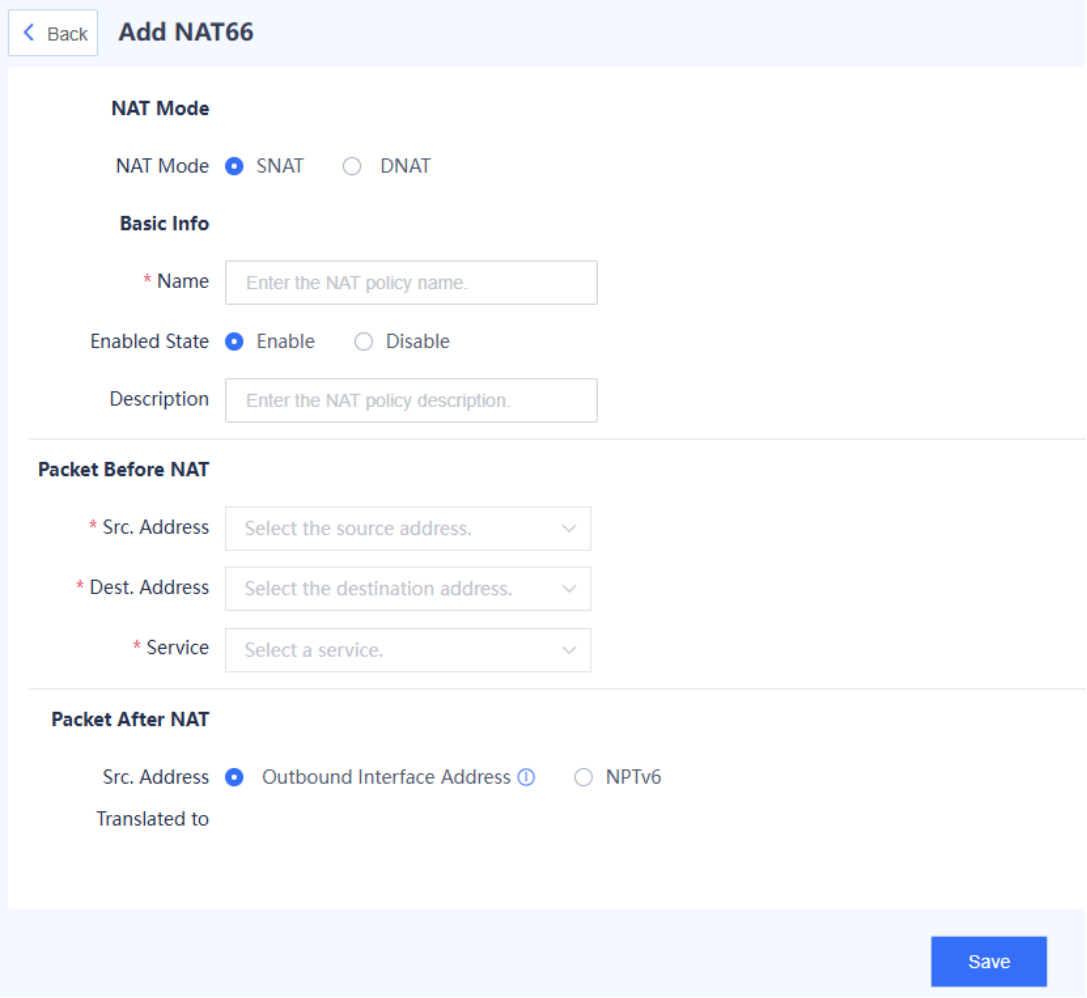
Source NPT66 translates source IPv6 addresses in IPv6 packets for intranet hosts to access external networks.

Procedure

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



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



(3) Set **NAT Type** to **SNAT** to configure a source NPT66 policy. The following table lists the configuration parameters.

Item	Description	Remarks
NAT Type		
NAT Type	NAT66 translation mode.	[Example] SNAT
Basic Info		
Name	Name of the NAT66 policy.	[Example] NPTv6_policy_1
Enabled State	Whether to enable the policy immediately after configuration is completed.	[Example] Enable

Item	Description	Remarks
Description	Policy description.	[Example] NPTv6 policy1
Packet Before NAT		
Src. Address	NAT is performed for packets from these addresses.	● 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.	● 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.	● 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		
Src. Address Translated to	Two options are supported: ● **Outbound Interface Address**: Translates the source address of a packet into the IPv6 address of the outbound interface. ● **NPTv6**: Translates the source address of a packet into an IPv6 address with a specified prefix.	[Example] Outbound Interface Address

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.	● This parameter needs to be configured only when **Src. Address Translated to** is set to **NPTv6**. ● Enter a valid IPv6 address prefix and prefix length. The following values are not allowed: o Loopback address: 0:0:0:0:0:0:0:1 or ::1 o Link-local address: addresses with a prefix of FE80:: o Multicast address: IPv6 addresses in the range of FF00::/8ollowing values are not allowed: is replaced w o 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. [Example] 3003::/64

(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.

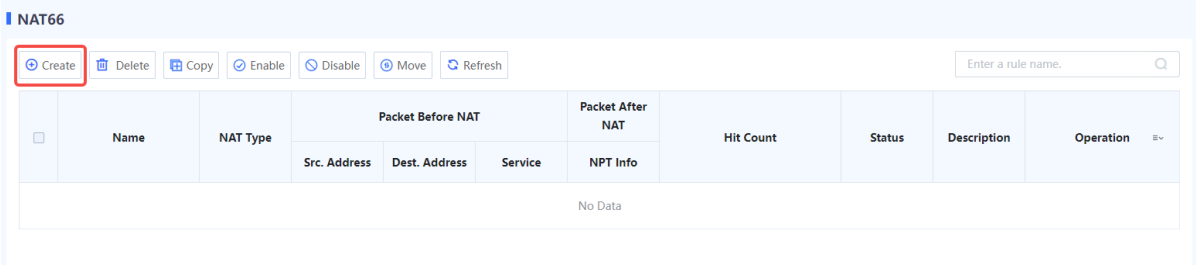
2. Configuring DNAT

Application Scenario

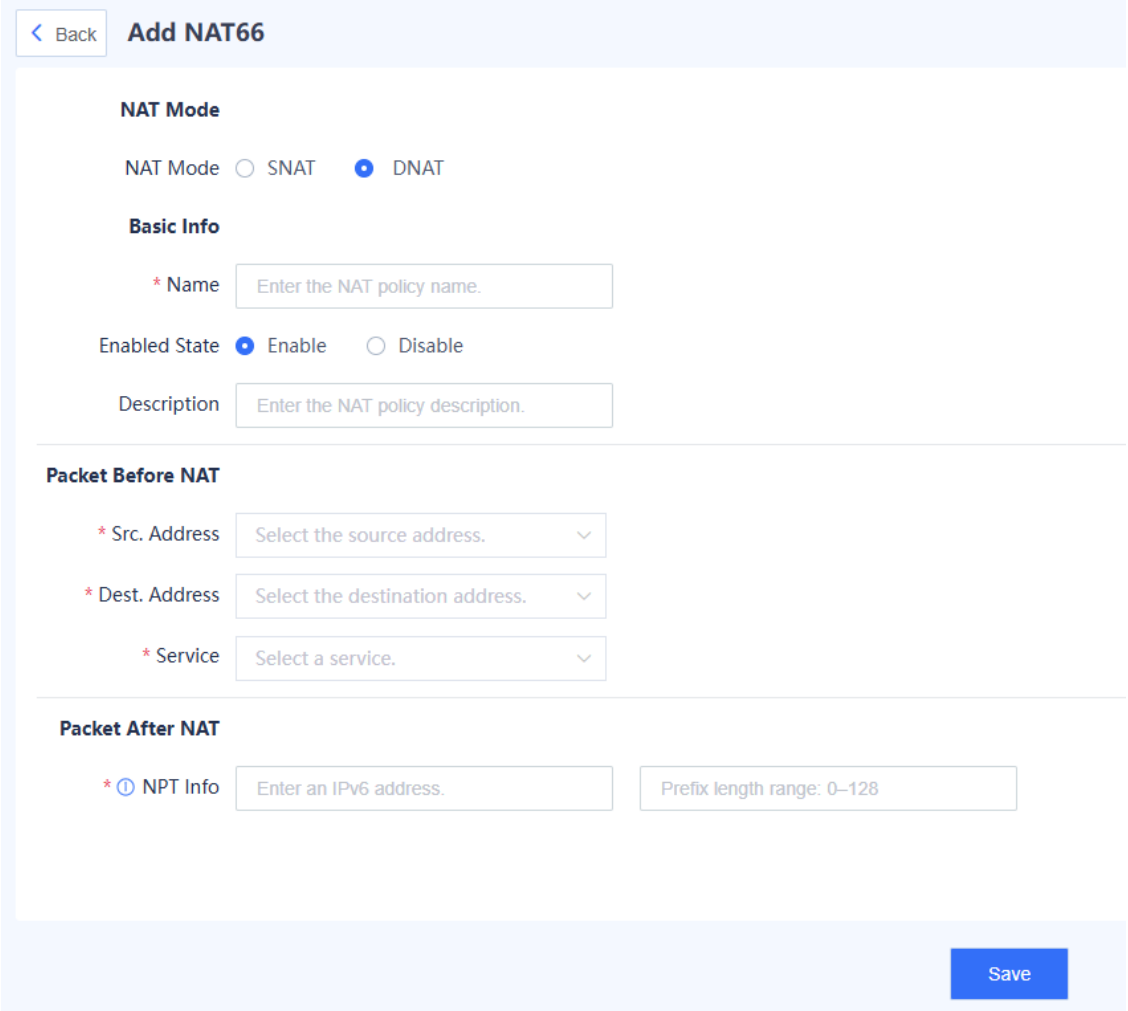
Destination NPTv6 translates destination IPv6 addresses in IPv6 packets for external networks to access services provided by intranet hosts.

Procedure

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



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



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

Item	Description	Remarks
NAT Type		
NAT Type	NAT66 translation mode.	[Example] DNAT
Basic Info		
Name	Name of the NAT66 policy.	[Example] NPTv6_policy_1
Enabled State	Whether to enable the policy immediately after configuration is completed.	[Example] Enable

Item	Description	Remarks
Description	Policy description.	[Example] NPTv6 policy1
Packet Before NAT		
Src. Address	NAT is performed for packets from these addresses.	● 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.	● 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.	● 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		
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.	● Enter a valid IPv6 address prefix and prefix length. The following values are not allowed: ○ Loopback address: 0:0:0:0:0:0:0:1 or ::1 ○ Link-local address: addresses with a prefix of FE80:: ○ Multicast address: IPv6 addresses in the range of FF00::/8 to FFFF::/8, that is, an address 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. [Example] 3003::/64

(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.

4.5.8 Enabling the ALG Function

Application Scenario

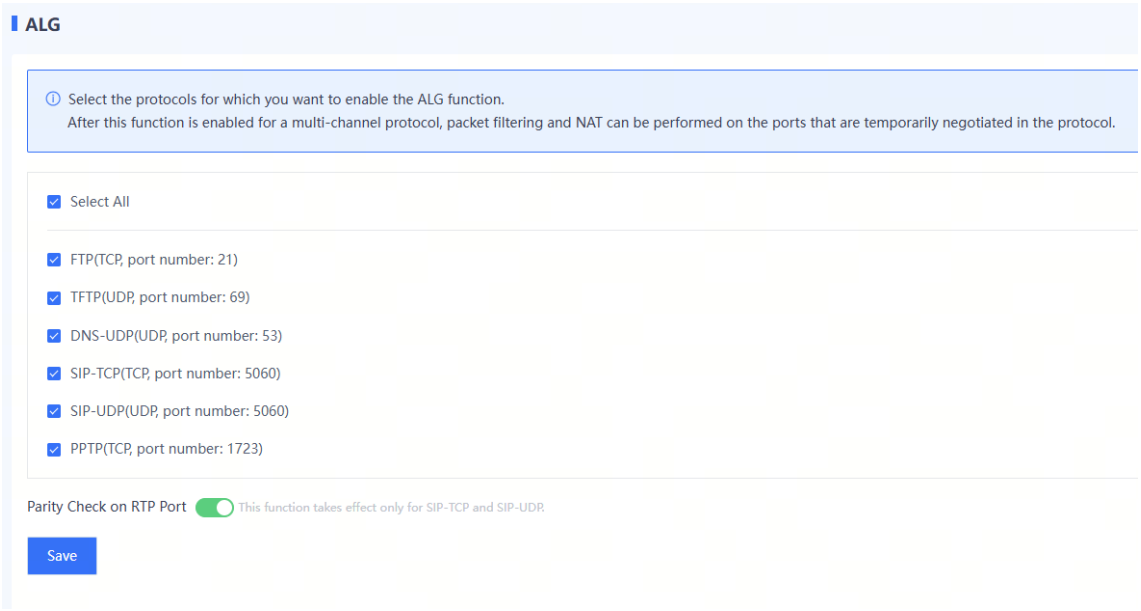
The application-level gateway (ALG) function is used to automatically detect application layer information for certain packets in a NAT scenario. Corresponding access rules are enabled (a server-map table is generated) based on the application layer information, and IP address and port information in 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, enable **Parity Check on RTP Port**, and click **Save**.

- After the ALG function is enabled, information in the packets of these protocols can be translated by NAT.
- After parity check of an RTP interface is enabled, the device checks parity of the RTP interface in SIP messages. If an RTP port number in a SIP message is odd, the source port number for the expected session will be automatically converted to an even number; otherwise, the RTP port number is not converted.

Note

An expected session refers to a session that is established on the device, no packet passes through the device, and packets may pass through the device in the near future.

4.5.9 Configuring an Address Pool

Application Scenario

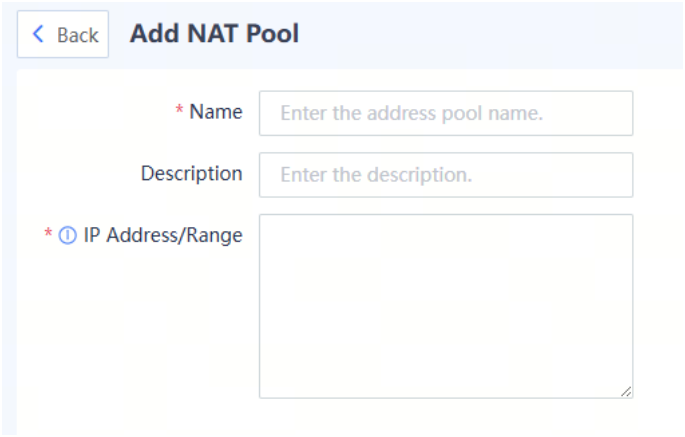
After an address pool is configured, the addresses in the pool can be selected when you set parameters of **Packet After NAT** for a NAT policy.

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**.

4.5.10 Configuring NAT64 Prefixes

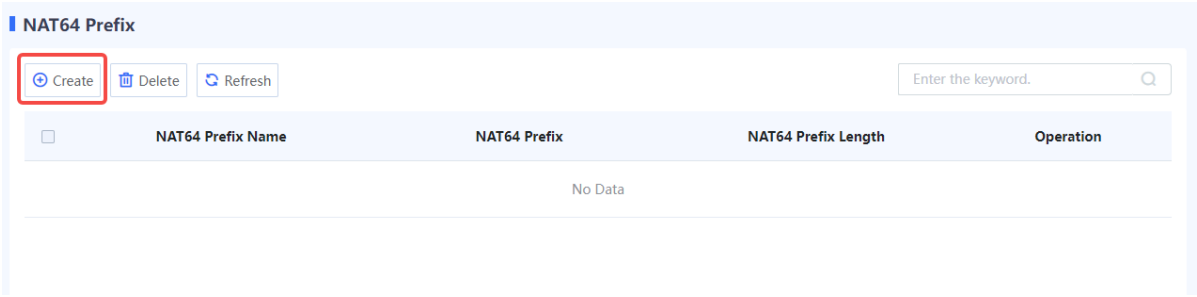
Application Scenario

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.

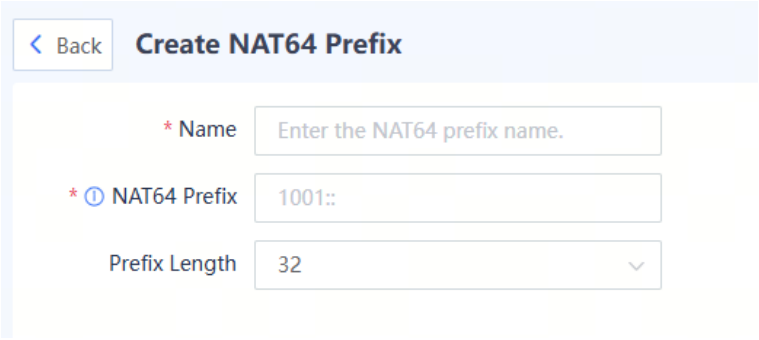
When configuring a NAT64 or NAT46 policy, you can reference the configured NAT64 prefix as the NAT64 prefix for NAT.

Procedure

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



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



(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**.

4.6 Port Mapping Policy

4.6.1 Overview

The port mapping function maps a specific port of an external IP address to a specific port on an internal server. In this way, requests from external networks can be forwarded to a specific device on the intranet based on external IP addresses and port numbers. As a result, external users can access intranet servers, such as a DNS server, web server, and FTP server.

4.6.2 Configuring a Port Mapping Policy

Application Scenario

Typically, port mapping is used for external users to access intranet servers, for intranet users to access intranet servers using external IP addresses, and for mutual access between two intranets.

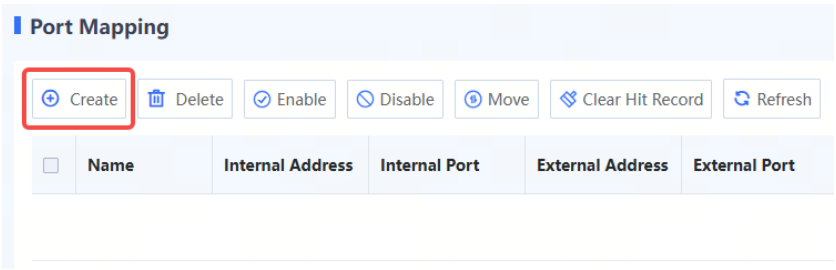
Precautions

A port mapping policy takes precedence over a NAT policy. That is, if traffic matches a port mapping policy, NAT policies will not be matched.

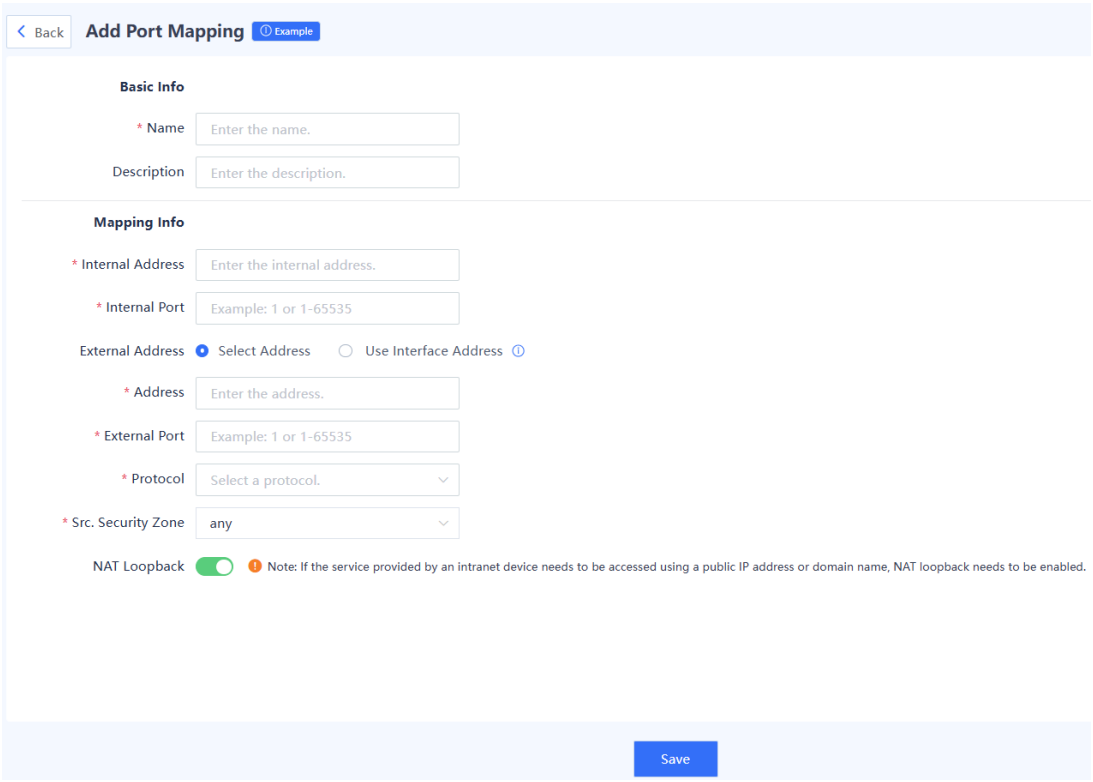
Procedure

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

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



(3) Configure port mapping.



Item	Description	Remarks
Basic Info		
Name	Name of a port mapping policy.	[Example] port_map
Description	Description of a port mapping policy.	-
Mapping Info		
Internal Address	Internal IP address to be mapped to, which is the IP address of the destination intranet server. This address indicates the destination to which a request is forwarded.	[Example] 192.168.1.2
Internal Port	Internal port number to be mapped to, which is the port number of the destination intranet server.	Enter a single port number or port number range. The number of configured internal ports must be the same as that of the configured external ports. [Example] 80 or 2-80

Item	Description	Remarks
External Address	External IP address used to receive requests from an external network. In a port mapping scenario where a device does not have a fixed external IP address (for example, PPPoE dial-up), **External Address** must be set to **Use Interface Address** and DDNS must be configured: (1) Configure an interface with DDNS to enable dynamic domain name binding. (2) Select **Use Interface Address** for port mapping and select the corresponding interface. (3) Access the mapped service based on the dynamically bound domain name of DDNS to implement access through a fixed domain name (IP address is variable).	You can manually set an IPv4 address or use the interface address. [Example] 200.10.10.10
External Port	External port number used to receive requests from an external network.	Enter a single port number or port number range. The number of configured external ports must be the same as that of the configured internal ports. [Example] 80 or 2-80
Protocol	Protocol used by traffic accessing the server. Select **TCP**, **UDP**, or **TCP+UDP**.	[Example] TCP
Src. Security Zone	Traffic from this security zone is allowed to hit a port mapping policy. If security requirements are high, set the source security zone to the security zone to which the WAN interface belongs. Otherwise, set this parameter to **any**.	Any indicates all interfaces. [Example] any
NAT Loopback	If intranet users need to access intranet services using external IP addresses or domain names, NAT loopback needs to be enabled.	[Example] Enabled

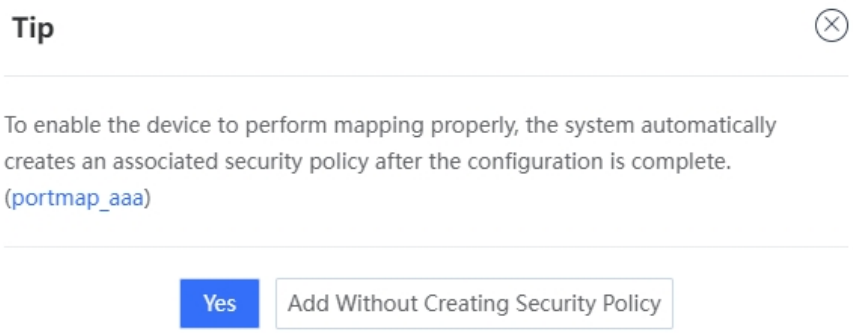
(4) Click **Save**. A dialog box is displayed, prompting you to determine whether to add a corresponding security policy.

Click **Yes**. A security policy is automatically associated and added on the security policy page to permit port mapping traffic.

Click **Add Without Creating Security Policy** to add a port mapping policy without adding an associated security policy.

Caution

If a security policy is not automatically associated or added, you need to manually configure a security policy to permit port mapping traffic. Otherwise, port mapping fails.



Follow-up Procedure

- When port mapping fails, you can use the port mapping fault diagnosis tool to troubleshoot the fault. For details, see 8.6.1 2. Port Mapping Exception Diagnostics.
- To modify a port mapping policy, click **Edit**. To delete a port mapping policy, click **Delete**. To enable or disable a port mapping policy, click the switch.
- To delete multiple port mapping policies in a batch, select the policies that you want to delete and click **Delete**.
- To add a new port mapping policy based on existing policy configuration, select a port mapping policy and click **Copy**.
- To enable multiple port mapping policies in a batch, select the policies that you want to enable and click **Enable**.
- To disable multiple port mapping policies in a batch, select the policies that you want to enable and click **Disable**.
- To move a port mapping policy, select the policy and click **Move**. The closer a policy is to the front, the higher its priority is in matching.
- Select a port mapping policy and click **Clear Hit Record** to clear the hit count of the policy and start counting again.
- Enter the full or part of a port mapping policy name in the search bar to search for policies. Fuzzy search is supported.

4.7 Security Defense

4.7.1 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 CF 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, ARP rate limit, and anti-ARP spoofing functions on the intranet.
- IP-MAC binding: strictly verifies the validity of source devices to improve network security.
- Session control: properly allocates session resources to prevent a large number of attacks.
- DNS protection: protects DNS services against attacks and abuse, ensuring security and reliability of domain name resolution.

4.7.2 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.

4.7.3 Configuring DoS/DDoS Attack Defense

1. Configuring Source Defense Against DoS/DDoS

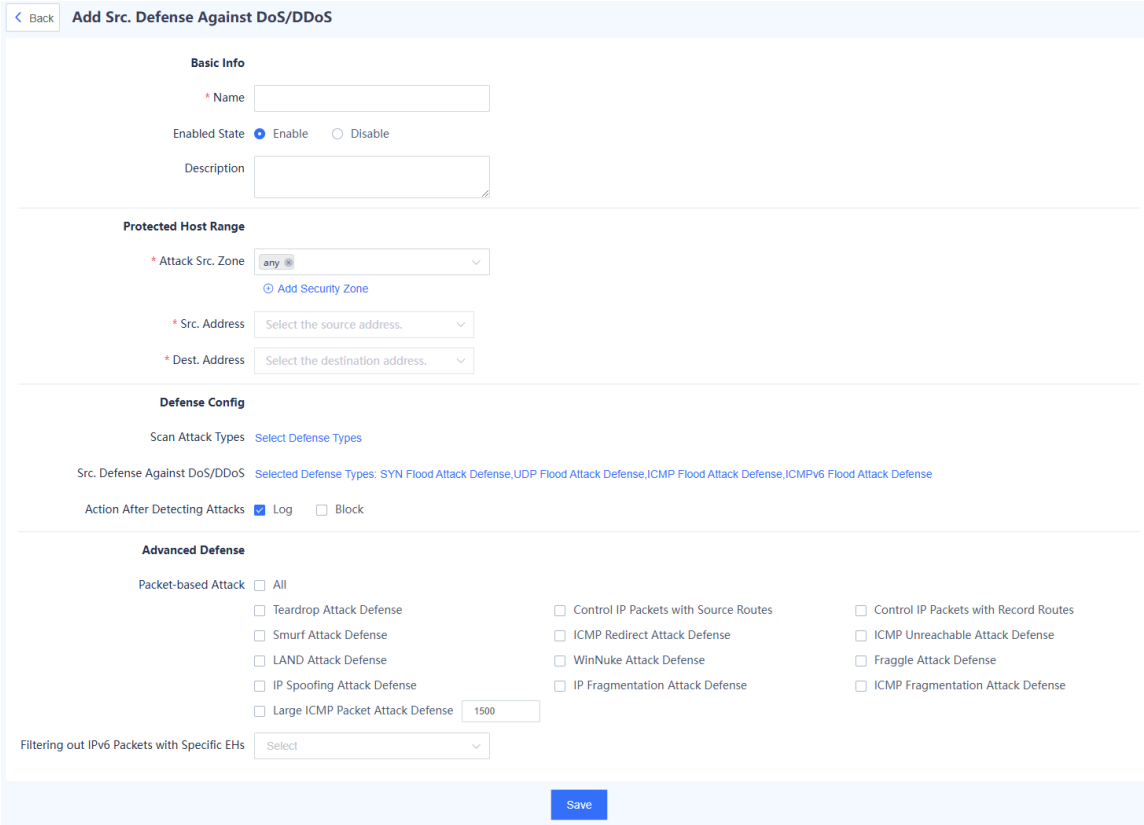
Procedure

(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.



(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.	[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.	[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.	Any indicates all interfaces. [Example] any
Src. Address	After this policy is delivered, the device checks the traffic from this address set.	**any** indicates all addresses. [Example] any

Item	Description	Remarks
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] 100
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] 100
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
Blocking Duration (s)	Duration of traffic blocking after an attack is detected.	[Example] 300s
Action After Detecting Attacks	Action taken after the system detects an attack, including: ● **Log**: Only record a security log, but not block traffic. ● **Block**: Only block traffic, but not record a security log.	[Example] Log + Block

Item	Description	Remarks
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**.
- Click **Basic Protocol Packet Control**. In the dialog box that is displayed, toggle on **Basic Protocol Packet Control** to enable DDoS policies for UDP-based Quick UDP Internet Connections (QUIC) packet forwarding.
- 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

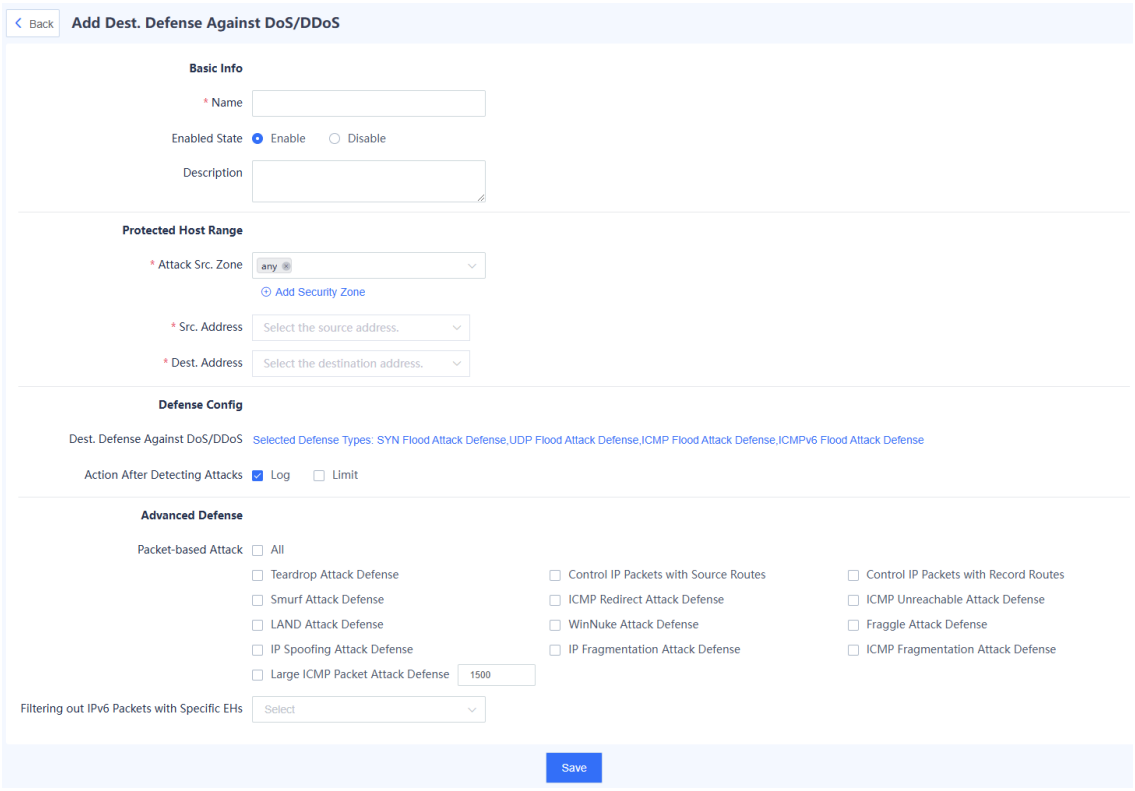
Procedure

(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.



(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.	[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.	[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.	Any indicates all interfaces. [Example] any
Src. Address	After this policy is delivered, the device checks the traffic from this address set.	**any** indicates all addresses. [Example] any

Item	Description	Remarks
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
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	Different types of attack defense based on packets.	[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**.
- Click **Basic Protocol Packet Control**. In the dialog box that is displayed, toggle on **Basic Protocol Packet**

Control to enable DDoS policies for UDP-based QUIC packet forwarding.

- 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.

4.7.4 Configuring ARP Attack Defense

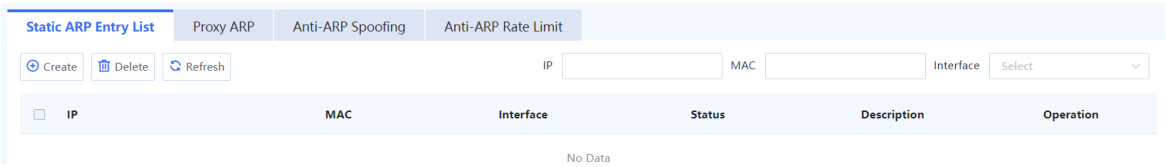
1. Configuring Static ARP

Application Scenario

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

Procedure

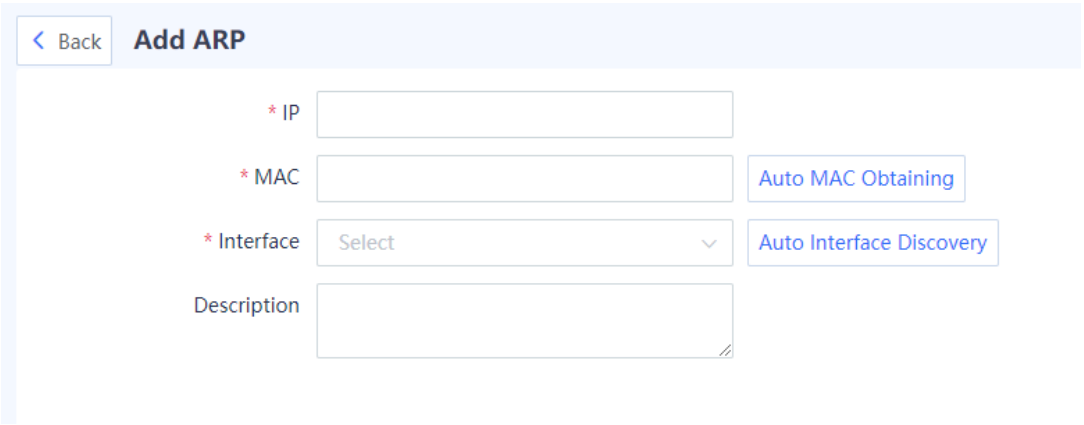
(1) Choose **Policy** > **Security Defense** > **ARP Attack Defense** > **Static ARP Entry List**.



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 address	IP address to be bound to the static ARP entry.	[Example] 192.168.10.3

Item	Description	Remarks
MAC address	MAC address to be bound to the static ARP entry.	Two configuration methods are supported: ● Fill in the information manually. ● Click **Auto MAC Obtaining**. The device will search for the MAC address matching the IP address according to the available ARP entry information. If no address is found, the system displays "No address is matched." [Example] 11:22:33:44:55:66
Interface	Physical interface to be bound.	Two configuration methods are supported: ● Fill in the information manually. ● Click **Auto Interface Discovery**. The device will configure the interface that may match the IP address according to the related information. If no interface is found, the system displays "No interface is matched." [Example] Ge0/1

(4) Click **Save**.

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.

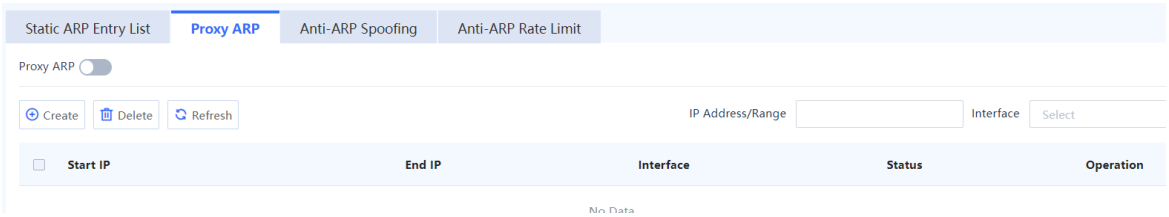
2. Configuring Proxy ARP

Application Scenario

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

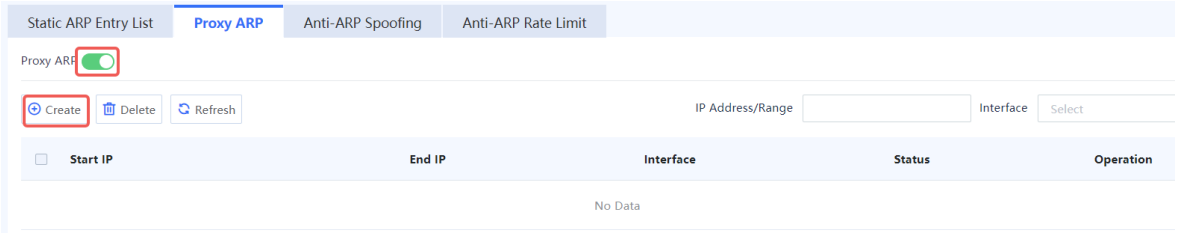
Procedure

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



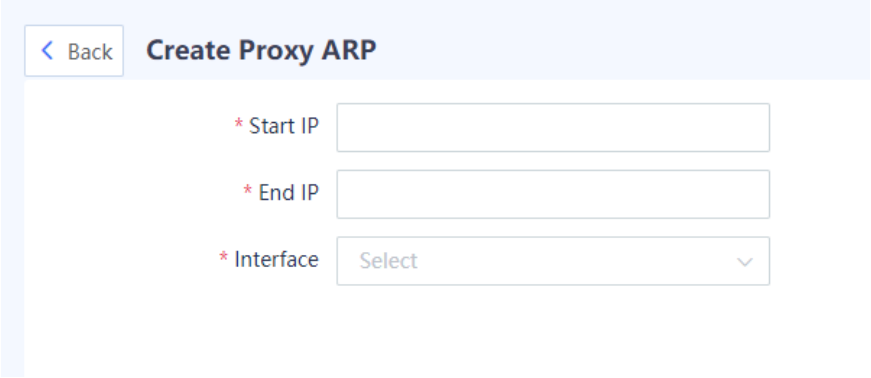
The proxy ARP network segments configured on the device are displayed. The **Status** column shows whether the interfaces bound to the entries are valid or invalid.

(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**.

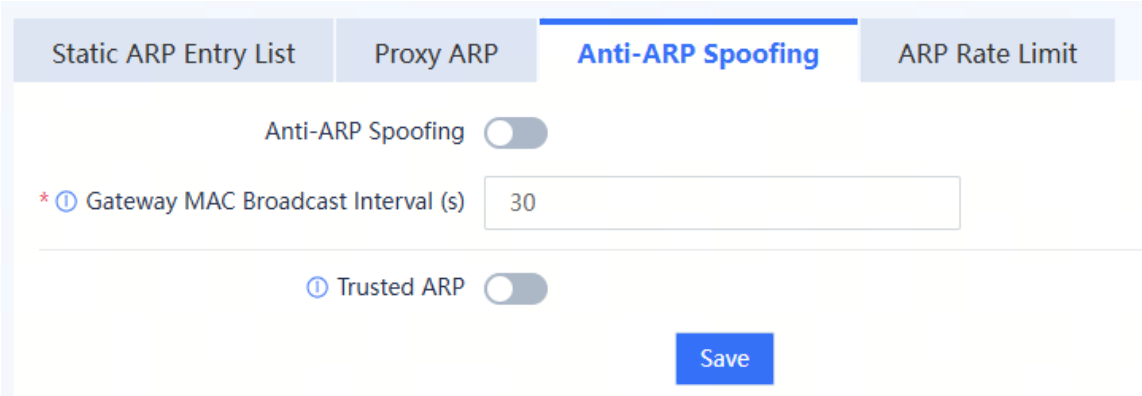
3. Configuring Anti-ARP Spoofing

Application Scenario

On a network where the gateway needs to be highly reliable and devices frequently access the network or change dynamically (for example, new devices access the LAN; NICs are updated or replaced, or IP addresses are modified for existing devices), enabling anti-ARP spoofing and trusted ARP probing can filter out fake ARP entries. This ensures the reliability of ARP entries on the local device and maintains correct communication links between terminals and the gateway.

Procedure

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



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

After anti-ARP spoofing is enabled, the device periodically sends gratuitous ARP broadcast packets to advertise its own MAC address. In this way, terminals on the same network can obtain the correct MAC address of the gateway. This ensures normal packet forwarding from users to the gateway and prevents interception by malicious attackers.

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

(4) Toggle on **Trusted ARP**.

After trusted ARP is enabled, the device sends unicast requests to verify the authenticity of new or updated dynamic ARP entries, improving the reliability of dynamic ARP entries.

(5) Click **Save**.

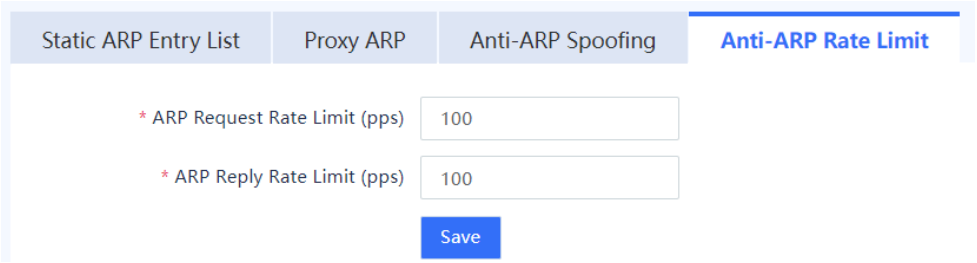
4. Configuring ARP Rate Limiting

Application Scenario

ARP rate limiting can be configured for networks with heavy ARP traffic. When a global rate limit is configured for ARP request/response packets, the system monitors the number of ARP packets sent to the local device. If the overall ARP packet rate exceeds the configured global threshold and the ARP packet rate from a specific IP address exceeds 5 pps, the system discards ARP packets from that IP address. Otherwise, ARP packets are permitted. This function prevents a single IP address from exceeding the threshold with a large number of ARP attack packets, thereby avoiding ARP packets from other IP addresses from being discarded.

Procedure

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



(2) Modify the global rate limit of ARP request or reply packets.

The default values of both parameters are 100, in pps.

(3) Click **Save**.

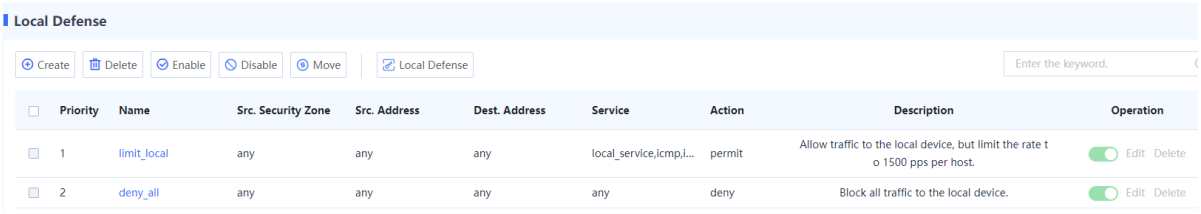
4.7.5 Configuring Local Defense

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**.

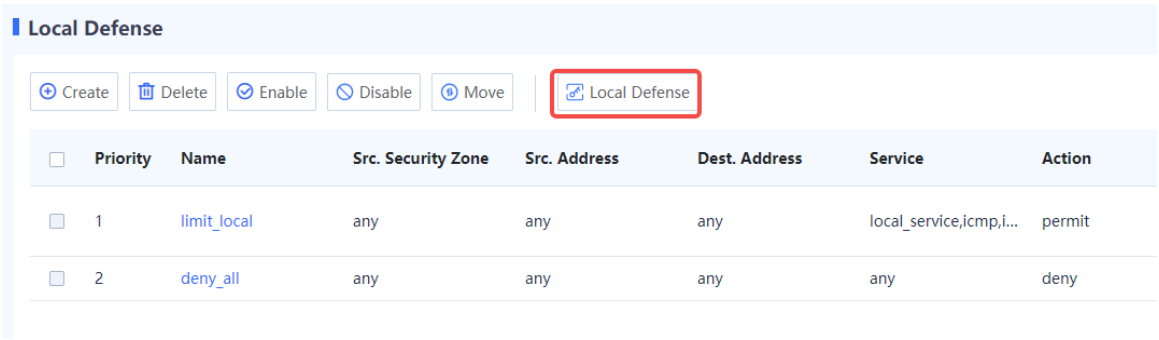


Note

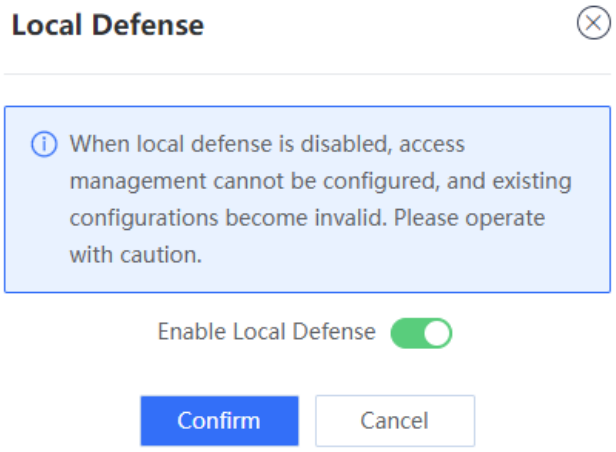
The local defense function has two default policies that cannot be modified to ensure that the device is protected from traffic attacks after it is delivered.

(2) Enable Local Defense.

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

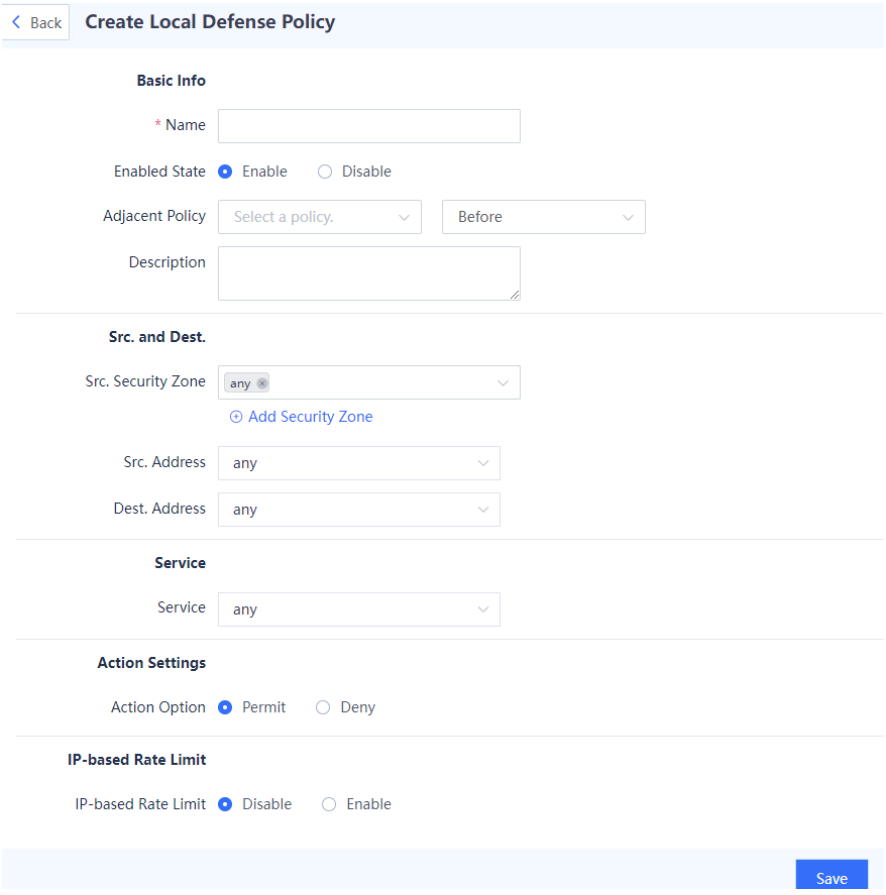


b Toggle on **Local Defense** and click **Confirm**.



(3) Create a local defense policy.

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



b Set the parameters for the local defense policy.

Item	Description	Remarks
Basic Info		

Item	Description	Remarks
Name	Name of the local defense policy.	[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.	-
Src. and Dest. Associate the policy with source security zone, source address object, destination address object, and service object. The policy takes effect when all the four items are hit.		
Src. Security Zone	After this policy is delivered, the device checks the traffic from this zone.	Any indicates all interfaces. [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	Whether to restrict the number of packets that can pass per second in the traffic matching the policy. ● **Disable**: not restricted ● **Enable**: restricted. The **Packets Allowed to Pass Through Each Host (pps)** field needs to be set.	[Example] Disable

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.

4.7.6 DNS Protection

Application Scenario

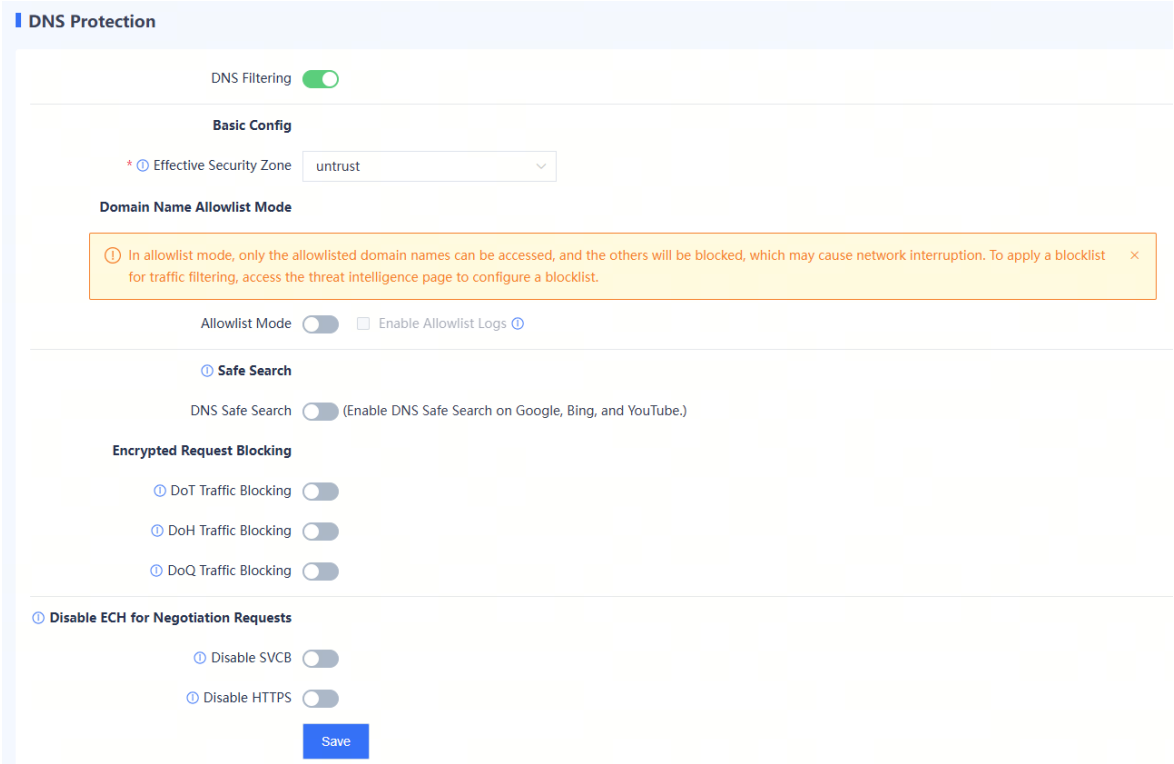
After DNS filtering is configured, the device performs access control based on domain names in DNS request packets. DNS filtering allows the device to block access to invalid domain names and permits access to valid domain names by matching a DNS allowlist.

This function applies only to DNS traffic from an intranet to an external network.

Procedure

(1) Choose **Policy** > **Security Defense** > **DNS Protection**.

(2) Click  to enable DNS filtering.



(3) Configure DNS filtering.

Item	Description	Remarks
Basic Config		
Effective Security Zone	DNS filtering takes effect only for DNS request packets whose outbound interface belongs to the security zone. For example, if the security zone is untrust, DNS protection needs to be implemented for outgoing packets from the interfaces of the untrust zone.	● Select one or more security zones from the drop-down list box. ● Any indicates all interfaces. [Example] untrust
Domain Name Allowlist Mode		
Domain Name Allowlist Mode	After the allowlist mode is enabled, only allowlisted domain names can be accessed, and other domain names are blocked.	[Example] Enabled

Item	Description	Remarks
Enable Allowlist Logs	Whether to enable allowlist filtering for security logs. ● After this function is enabled, only blocking logs about domain names that are not in the allowlist will be recorded. ● After this function is enabled, a large number of logs will be generated, occupying a large number of disk resources. You are advised to disable this function.	It is available only when the allowlist mode is enabled. [Example] Disabled
Domain Name Allowlist	After a domain name is added to the allowlist, the device permits the traffic destined for this domain name.	● Enter one record per line, separating records with carriage returns. ● A maximum of 1000 static domain names can be added to the allowlist. ● Complete domain name matching and prefix wildcard matching are supported. The wildcard (*) represents any string. ● It is available only when the allowlist mode is enabled. [Example] www.example.com *.example.com
Safe Search DNS Safe Search is a network safety protection measure. It filters and manages network access at the DNS layer to intercept user access to unauthorized content or high-risk content (such as adult content and malicious websites). This feature helps manage user online behavior. DNS Safe Search takes effect during domain name resolution and works together with URL Safe Search (based on web addresses) to provide more comprehensive security filtering. You are advised to enable both features. For details about the URL Safe Search configuration, see 5.10.3 1. Custom URL Filtering Template.		
DNS Safe Search	After this function is enabled, search engines such as Google Chrome, Bing, and YouTube work in safe search mode to ensure safety and compliance of the accessed content.	[Example] Enable
Restrict Access to YouTube	Whether to restrict access to YouTube.	[Example] Disable

Item	Description	Remarks
Mode	Restriction mode for YouTube access. In strict mode, an automated system is used to filter out a large number of videos while leaving some videos available for users to watch. Compared with the strict mode, the number of videos available for users to watch is significantly increased in moderate mode.	This parameter is available only after **Restrict Access to YouTube** is set to **Enable**. [Example] Strict
Encrypted Request Blocking When **DoT Traffic Blocking**, **DoH Traffic Blocking**, and **DoQ Traffic Blocking** are enabled at the same time, the client browser can send DNS packets in plaintext to ensure normal URL filtering.		
DoT Traffic Blocking	The device blocks DNS over TLS (DoT) packets and generates security logs.	[Example] Enabled
DoH Traffic Blocking	The device blocks DNS over HTTPS (DoH) packets and generates security logs.	[Example] Enabled
DoQ Traffic Blocking	The device blocks DNS over QUIC (DoQ) packets and generates security logs.	[Example] Enabled
Disable ECH for Negotiation Requests When a client browser uses DNS queries to retrieve the Encrypted Client Hello (ECH) configuration, the Server Name Indication (SNI) information in subsequent HTTPS packets is encrypted. As a result, URL filtering fails. To ensure normal URL filtering, you are advised to disable ECH. When **DoT Traffic Blocking**, **DoH Traffic Blocking**, and **DoQ Traffic Blocking** are enabled at the same time and both SVCB negotiation and HTTPS negotiation are disabled, the client cannot retrieve the ECH configuration information.		
Disable SVCB	The device blocks DNS packets of RR type 64 (SVCB) and generates a security log.	SVCB negotiation is disabled by default. [Example] Disabled
Disable HTTPS	The device blocks DNS packets of RR type 65 (HTTPS) and generates a security log.	HTTPS negotiation is disabled by default. [Example] Disabled

(4) Click **Save**.

4.7.7 IP-MAC Binding

1. Overview

Manually configure the IP-MAC address binding function to verify the IP and MAC address binding relationship of inbound packets. If a specified IP address is bound with a MAC address, the device receives only the IP packets containing the matched IP address and MAC address. The other packets are discarded. This function applies to defense against host spoofing attacks and can filter out forged IP packets sent to the device by attackers that spoof the IP or MAC addresses of authorized hosts.

2. Manually Configuring IP-MAC Binding

Precautions

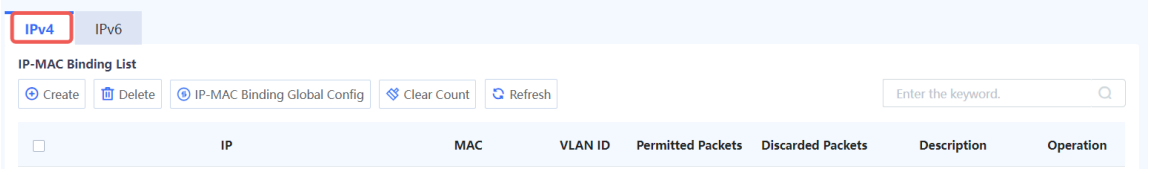
One IP address can be bound with only one MAC address, and up to 1,000 IP-MAC binding policies can be added.

Procedure

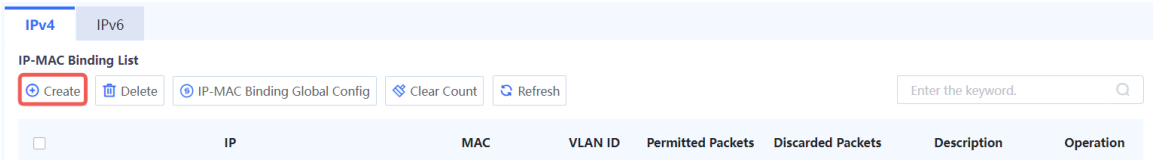
(1) Add an IP-MAC binding entry.

a Choose **Policy** > **Security Defense** > **IP-MAC Binding**.

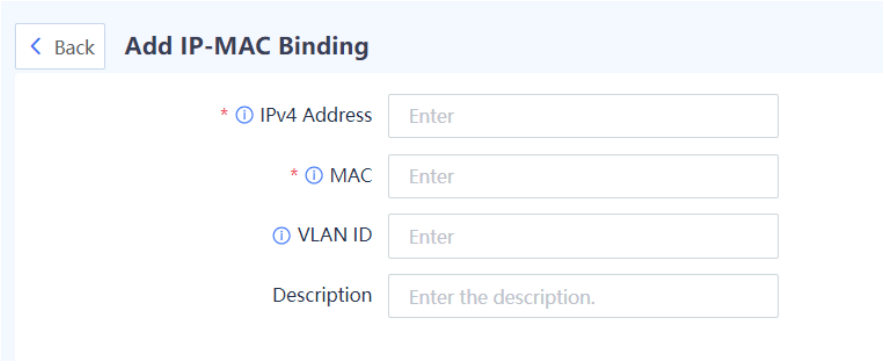
b Click the **IPv4** or **IPv6** tab based on the type of the IP address to be configured.



c Click **Create** in the **IP-MAC Binding List** area.



d Configure the IP-MAC binding entry.

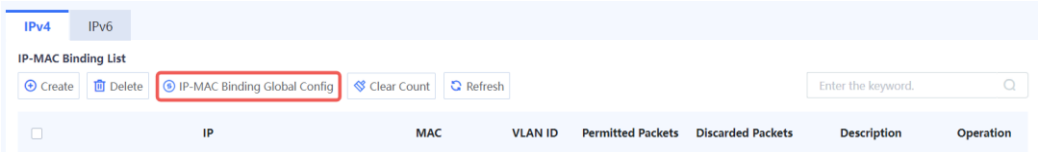


Item	Description	Remarks
IPv4 Address	IPv4 address to be bound.	[Example] 192.168.1.1
MAC address	MAC address to be bound.	[Example] 1a:2b:3c:4d:5e:64
VLAN ID	ID of the VLAN to which the binding entry belongs.	[Example] 192
Description	Description of the binding entry.	N/A

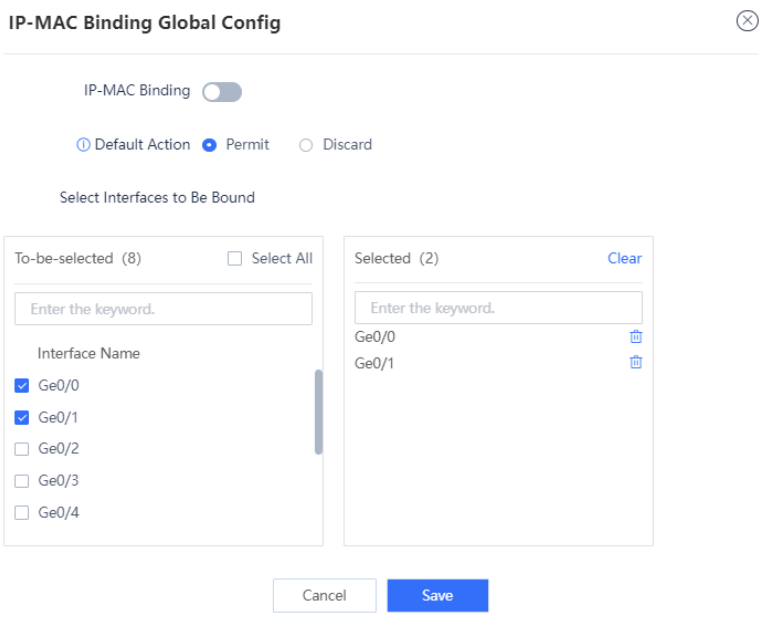
e Click **Save**.

(2) Set global configuration for the IP-MAC binding entry.

a Click **IP-MAC Binding Global Config**.



b Set global configuration for the IP-MAC binding entry.



Item	Description	Remarks
IP-MAC Binding	Toggle on the switch to enable the IP-MAC binding function. If it is not enabled, the IP-MAC binding entry does not take effect.	[Example] Disabled
Default Action	Action on traffic that does not match the binding rule. You can select **Permit** or **Discard**.	[Example] Permit
Select Interfaces to Be Bound	Interfaces on which the IP-MAC binding entry needs to take effect. A maximum of 150 interfaces can be bound.	Select interfaces in the **To-be-selected** area. The selected interfaces are automatically added to the **Selected** area. [Example] Ge0/0

c Click **Save**.

3. Configuring IP-MAC Binding for Dynamic ARP Entries

Application Scenario

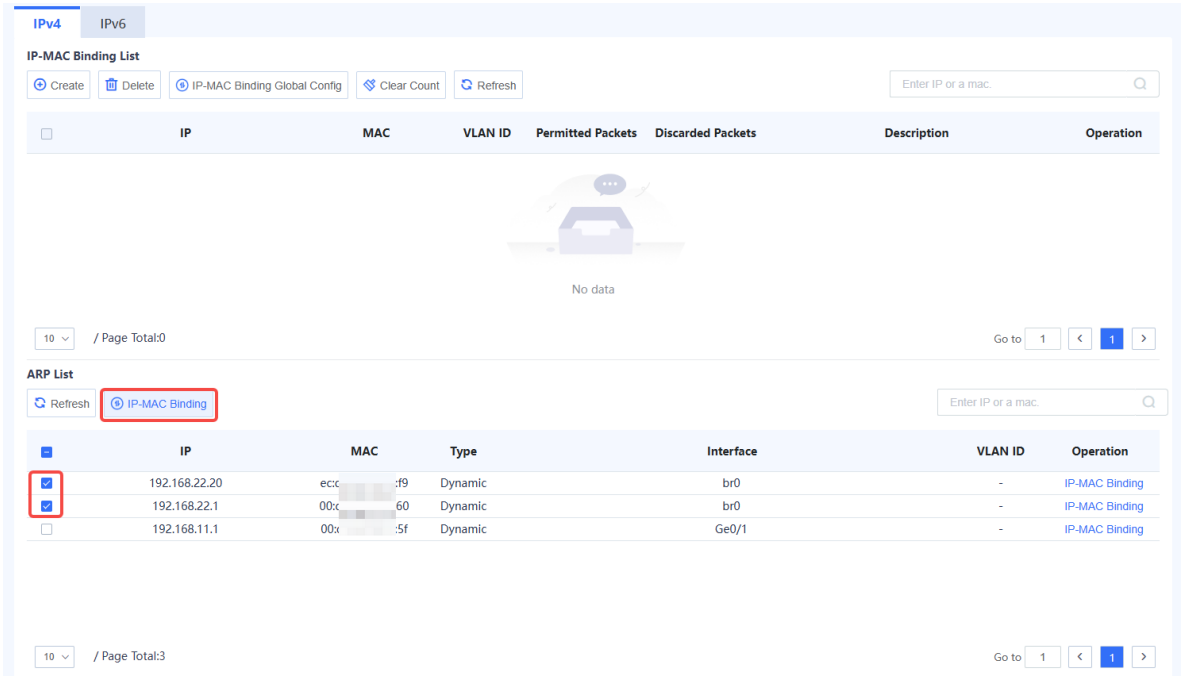
Dynamic ARP entries are automatically learned, generated, and updated by the ARP protocol based on ARP message exchange. These entries can be aged out and overwritten by new dynamic ARP entries. This function can quickly bind IP and MAC addresses.

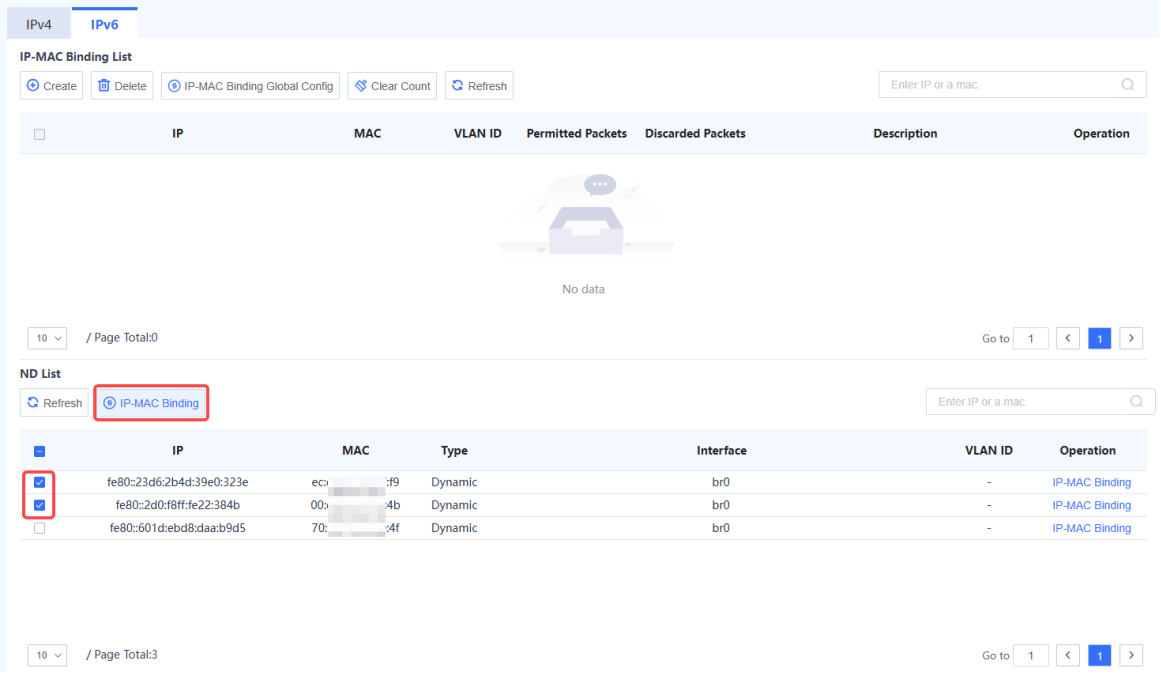
If dynamic ARP entries are updated after IP-MAC binding, you must manually delete the original bindings and rebind them. Otherwise, the terminal traffic may be mistakenly blocked.

Procedure

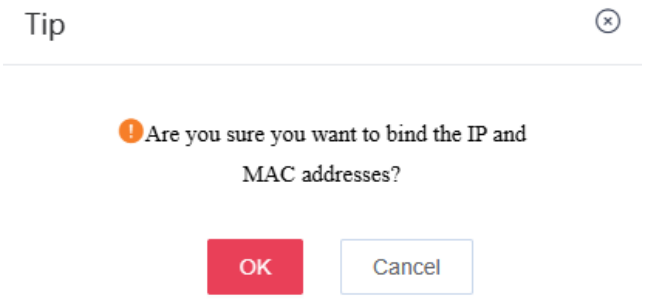
(1) Choose **Policy** > **Security Defense** > **IP-MAC Binding**.

(2) In the **ARP List** area, select at least one entry and click **IP-MAC Binding**.

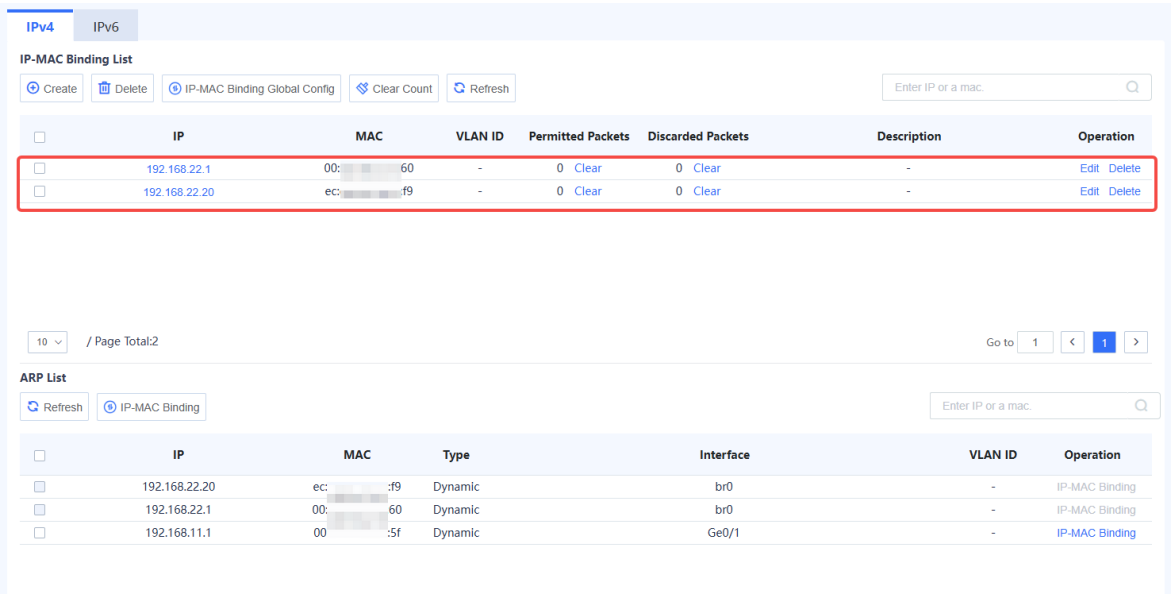

IPv4
IPv6
IP-MAC Binding List
Create
Delete
IP-MAC Binding Global Config
Clear Count
Refresh
Enter IP or a mac.
IP
MAC
VLAN ID
Permitted Packets
Discarded Packets
Description
Operation
No data
10
/ Page Total:0
Go to 1
1
ARP List
Refresh
IP-MAC Binding
Enter IP or a mac.
IP
MAC
Type
Interface
VLAN ID
Operation
192.168.22.20
Dynamic
br0
IP-MAC Binding
192.168.22.1
Dynamic
br0
IP-MAC Binding
192.168.11.1
Dynamic
Ge0/1
IP-MAC Binding
10
/ Page Total:3
Go to 1
1

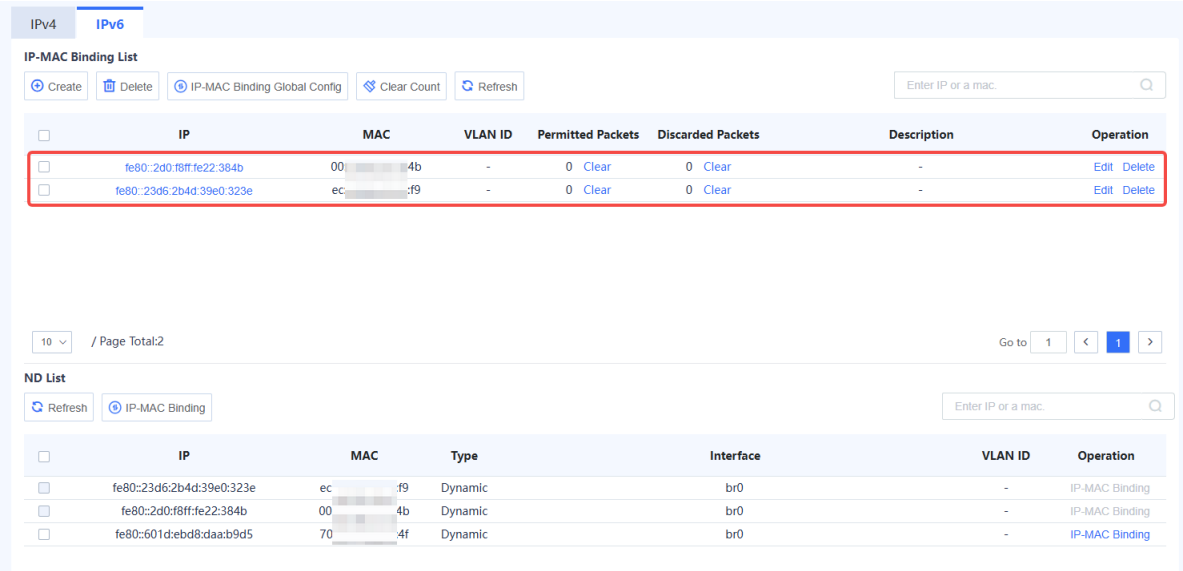

IPv4
IPv6
IP-MAC Binding List
Create
Delete
IP-MAC Binding Global Config
Clear Count
Refresh
Enter IP or a mac.
IP
MAC
VLAN ID
Permitted Packets
Discarded Packets
Description
Operation
No data
10
/ Page Total:0
Go to 1
1
ND List
Refresh
IP-MAC Binding
Enter IP or a mac.
IP
MAC
Type
Interface
VLAN ID
Operation
fe80::23d6:2b4d:39e0:323e
Dynamic
br0
IP-MAC Binding
fe80::2d0:f8ff:fe22:384b
Dynamic
br0
IP-MAC Binding
fe80::601d:ebd8:daa:b9d5
Dynamic
br0
IP-MAC Binding
10
/ Page Total:3
Go to 1
1

(3) Click **OK**.



(4) After static IP-MAC binding is applied to entries, the ARP entries selected in the previous step are automatically included in **IP-MAC Binding List**. That is, the dynamic ARP entries are translated into static ARP entries.





4.8 Threat Intelligence

4.8.1 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 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 threats, attacks, and malicious access.

4.8.2 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

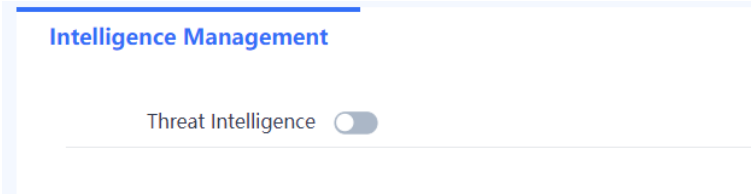
You have obtained and activated the TI capability license. For details about license activation, see 7.2.4 Activating the License.

Note

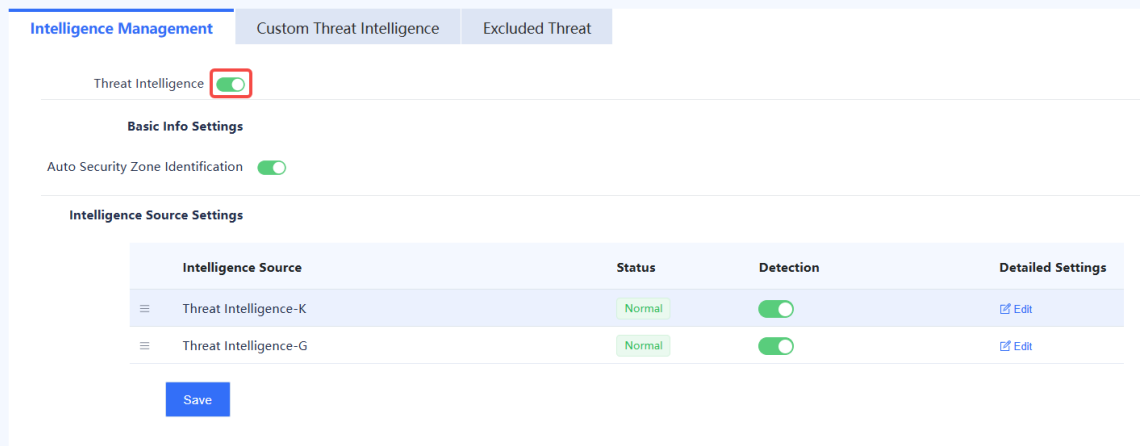
If the TI function is not authorized or authorization expires, the detection based on TI signature library is unavailable, and only the custom TI configured manually can be used. In this case, the TI signature library cannot be upgraded.

Procedure

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



(2) Click to enable the TI function.



(3) Set the parameters of TI.

Item	Description	Remarks
Basic Config		
Auto Security Zone Identification	Whether to identify the traffic inbound and outbound security zones automatically. ● After this function is enabled, the device automatically identifies the inbound and outbound security zones of traffic, and determines whether to perform threat signature matching for the traffic. ● If this function is disabled, you can manually specify the effective security zones for TI.	Any indicates all interfaces. [Example] Enable
Effective Security Zone	Specify the security zone where TI takes effect. The system performs TI matching and processing (block or alarm) for the traffic of the specified zone. The device can detect LAN-to-WAN and WAN-to-LAN traffic to identify malicious traffic.	When **Auto Security Zone Identification** is disabled, this parameter needs to be configured. [Example] untrust
Intelligence Source Settings		
Intelligence Source	Source of the TI data. After you enable **Threat Intelligence**, the device detects the data based on the corresponding TI signature library. Click ≡ to sort items in this column in descending order from top down.	The Threat Intelligence-K (Kaspersky) source can be enabled only when the Threat Intelligence-K license is activated on the device. The Threat Intelligence-G (Google) source can be enabled only when the Threat Intelligence-G license is activated on the device.

Item	Description	Remarks
Status	Current status of the TI function ● **Unauthorized**: The TI function license is not activated for the device, or the device cannot communicate with Ruijie Secure Cloud Platform. ● **No signature database**: Authorization is performed and threat intelligence is activated, but the local device does not have a signature database. ● **Normal**: The TI function license is activated. The function is available and the library can be updated. ● **Off**: The threat intelligence function is available, but detection is disabled. ● **Upgrading**: The threat information database is being updated. ● **Expired**: The threat intelligence license has expired. ● **Insufficient memory**: The TI function does not work because the system memory is insufficient. (You can enable the TI function again when the memory is sufficient.)	The status is displayed automatically according to the current TI function status. [Example] Normal
Detection	Whether to enable the current intelligence source for detection.	[Example] Enable
Click **Edit** in the **Detailed Settings** column to configure the intelligence source in details.		
Type	Select the TI type to defend against.	Select to enable defense. [Example] All Types
Action	Action to be taken on the traffic matching the TI: ● **Deny**: Block traffic and record a security log. ● **Alarm**: Not block traffic, but record a security log.	When multi-intelligence source detection is enabled, the most strict action applies if the traffic matches multiple intelligence sources. [Example] Deny

(4) Click **Save**.

4.8.3 Customizing Threat Intelligence

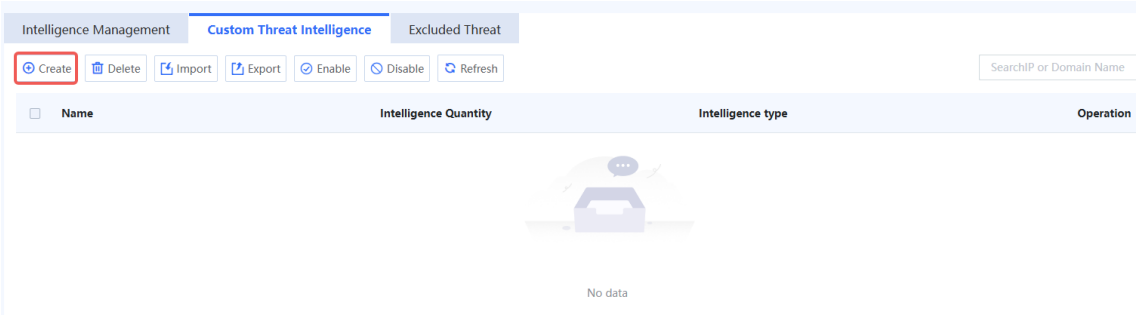
Application Scenario

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.

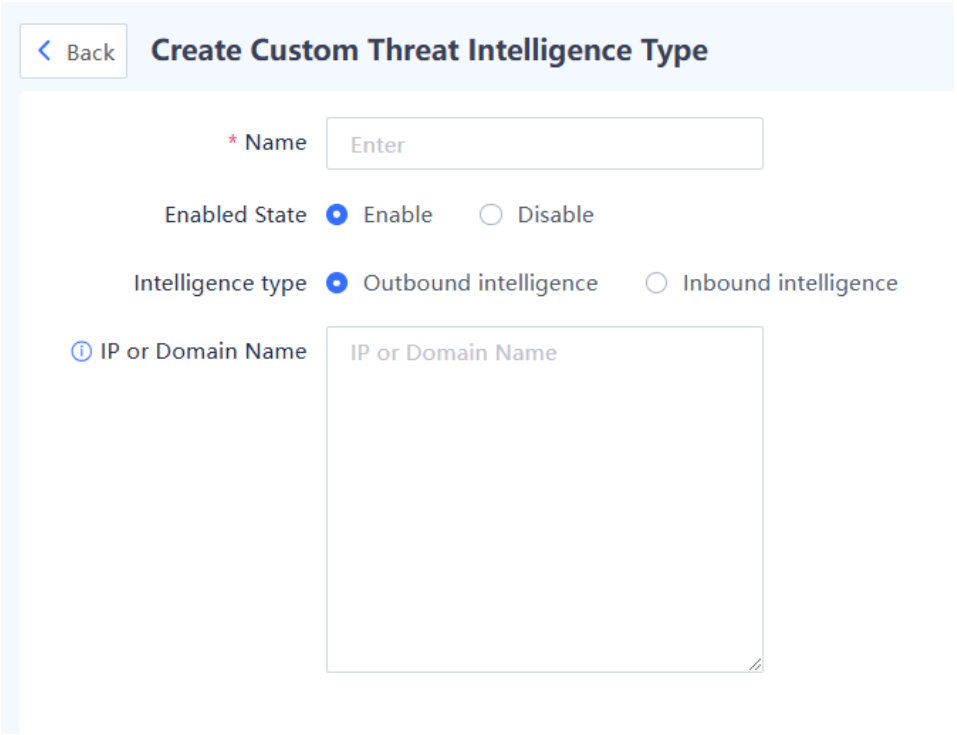
In the unauthorized state, custom TI can still be used for matching.

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 State	Whether to enable the TI. The disabled TI will not be matched.	[Example] Enable

Item	Description	Remarks
Intelligence type	● **Outbound intelligence**: Detect the destination IP addresses and domain names in DNS requests for outbound traffic. ● **Inbound intelligence**: Detect the source IP addresses of inbound traffic.	[Example] Outbound Intelligence
Outbound Intelligence		
IP or Domain Name	Destination IP address or DNS name to be checked and blocked.	● If multiple IPv4 addresses or domain names need to be configured, enter one IPv4 address or domain name per line, and press Enter to separate lines. ● The device supports full match or suffix match for the domain name: ○ Full match: Enter the complete domain name, such as www.ruijie.com. ○ Suffix match: Enter an incomplete domain name with the header replaced by an asterisk (*), for example, *.ruijie.com.
Inbound Intelligence		
IP	Source IP address to be checked and blocked.	If multiple IPv4 addresses need to be configured, enter one IPv4 address per line, and press Enter to separate lines. [Example] 157.148.69.74 157.148.69.75

(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.

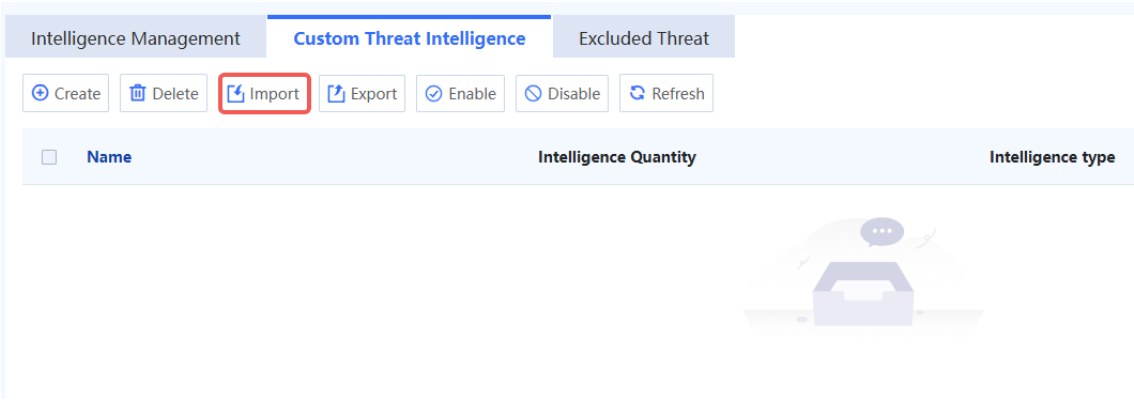
2. Importing Custom TI

Application Scenario

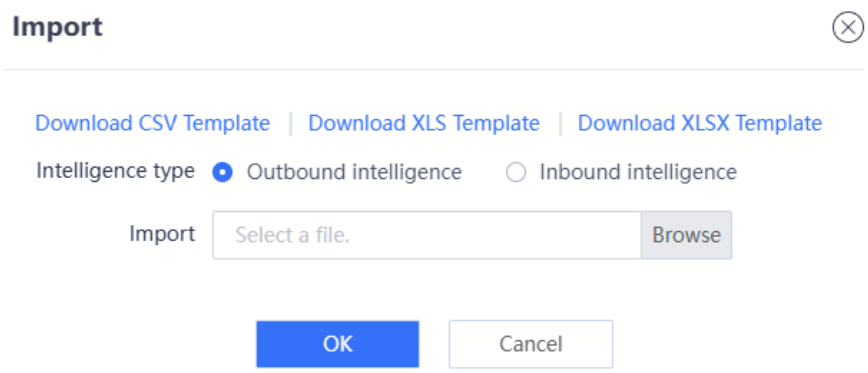
When you need to add a large number of TI types, you can fill in TI information in a template, and import them in a batch with one click.

Procedure

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

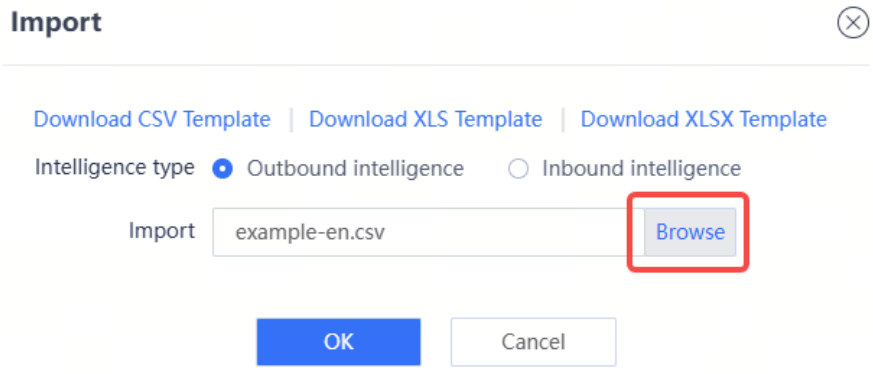


(2) Click **Import**. The **Import** dialog box is displayed.



(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.

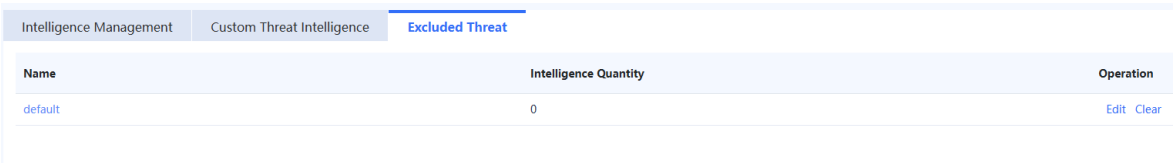
4.8.4 Configuring an Excluded Threat

Application Scenario

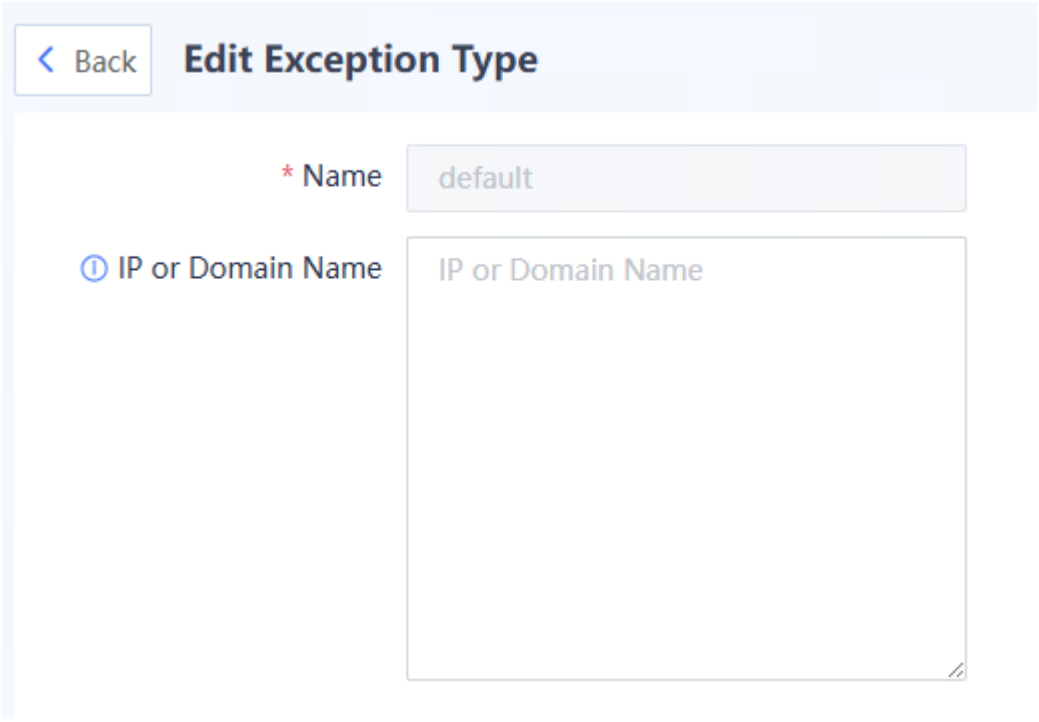
If the user's normal data is intercepted by mistake due to the not-updated TI content or other reasons, or if an IP address or domain name is not malicious, you can add the IP address or domain name to the excluded threat list. The traffic matching the excluded threat list will be permitted by the TI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

4.8.5 Viewing Threat Intelligence Logs

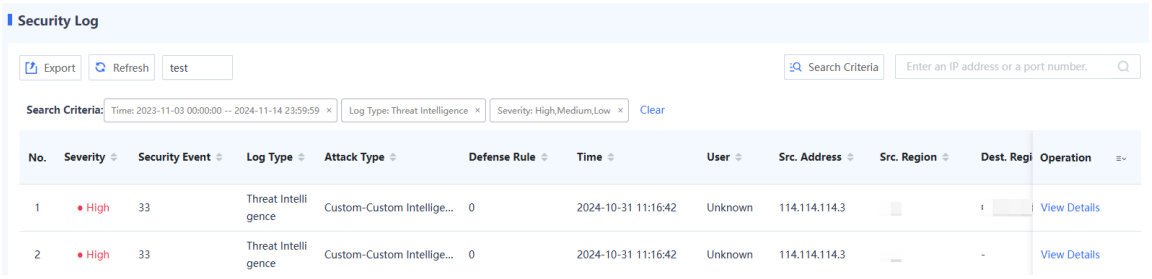
Application Scenario

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.

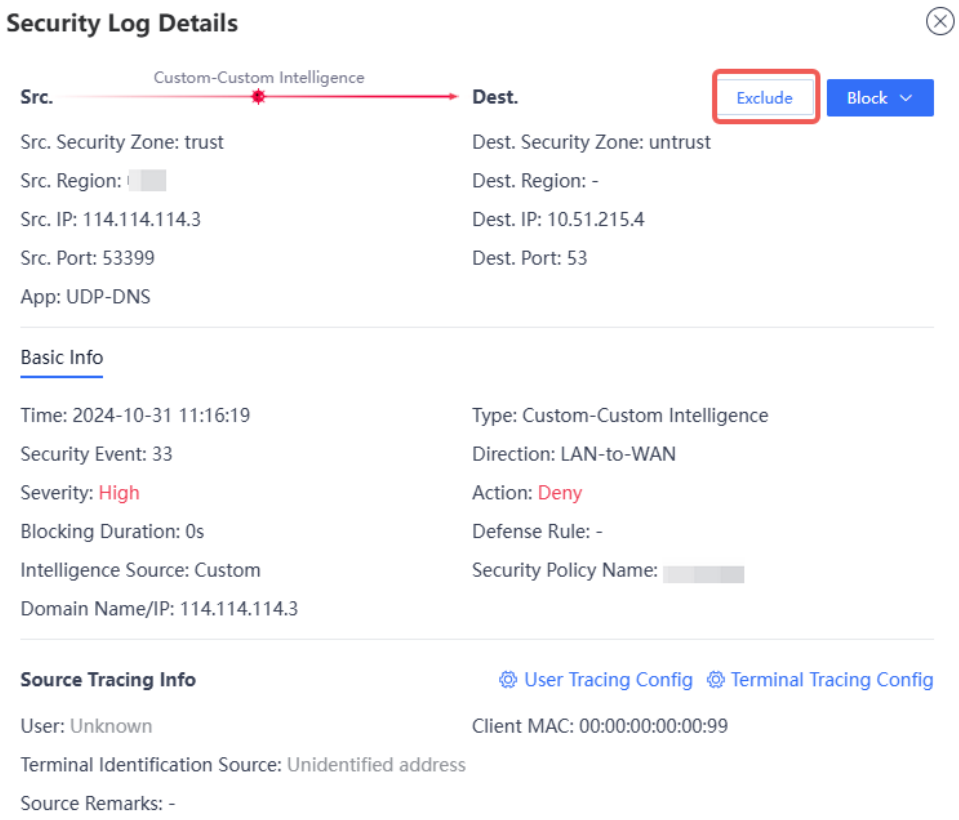
Procedure

(1) Choose **O&M** > **Logs** > **Security Log**.

(2) The TI log information is displayed on the web UI.



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



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 8.3.2 2. Querying Security Logs.

4.8.6 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 7.5 Signature Library Upgrade.

4.9 Session Control

4.9.1 Configuring the Uplink Packet Rate Limit

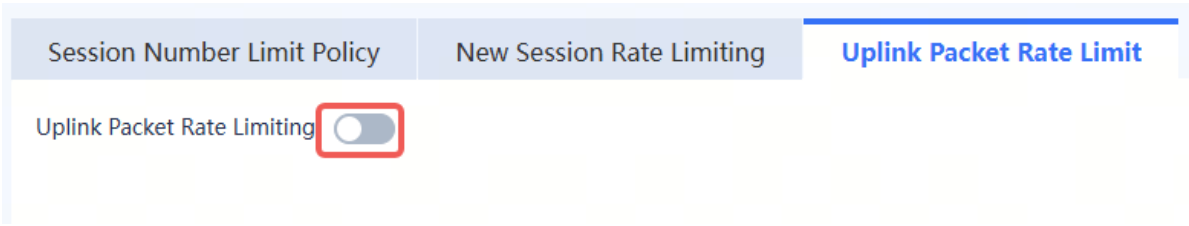
Application Scenario

Configure global per-IP rate limiting or rate limiting on designated IP addresses for uplink packets. The priority of rate limiting on designated IP addresses is higher than that of global per-IP rate limiting. In scenarios where network traffic is heavy, you can limit the rate of uplink packets to ensure proper network bandwidth allocation and prevent network congestion.

Procedure

(1) Choose **Policy** > **Session Control** > **Uplink Packet Rate Limit**.

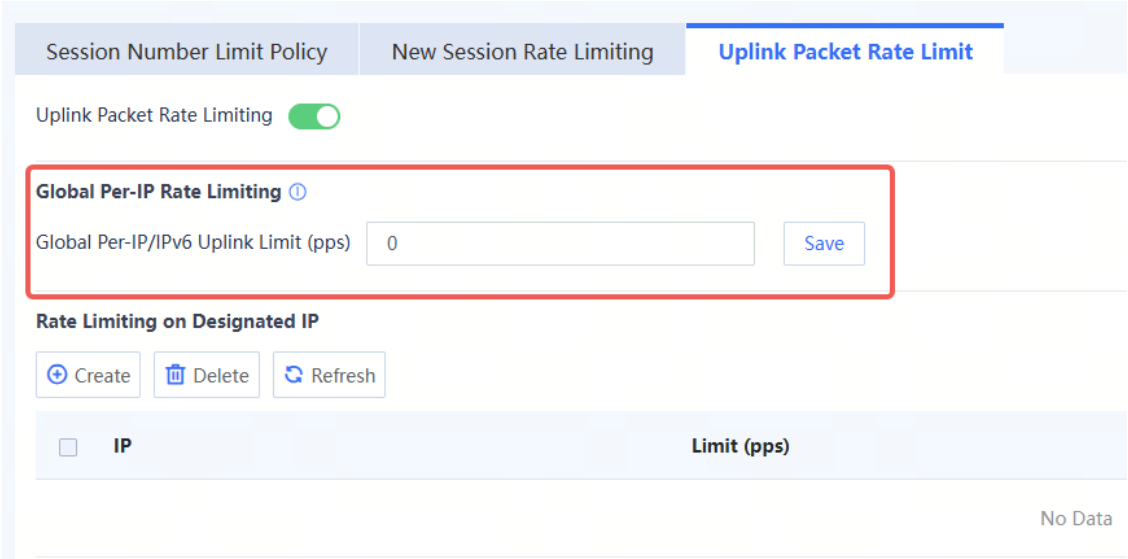
(2) Toggle on to enable uplink packet rate limiting.



(3) Configure a rate limit for uplink packets.

- Global Per-IP Rate Limiting

  a Configure a rate limit for each IP address on the entire network.

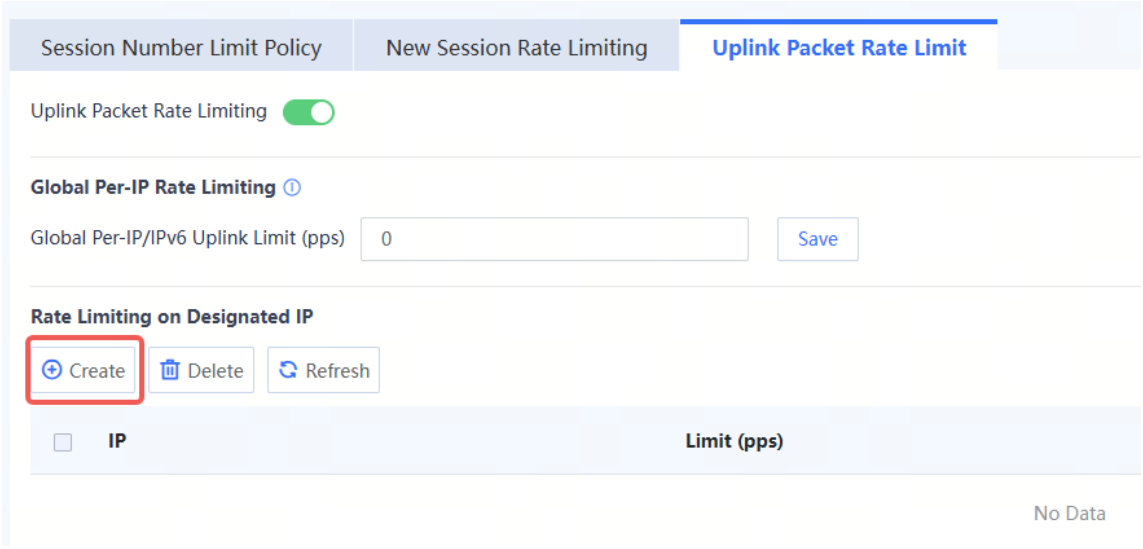


Item	Description	Remarks
Global Per-IP/IPv6 Uplink Limit (pps)	The priority of rate limiting on designated IP addresses is higher than that of global per-IP rate limiting. The default value is 0, indicating that the rate is not limited.	[Example] 3000

  b Click **Save**.

- Rate Limiting on Designated IP Addresses

  a Click **Create**.



b Configure rate limiting on a designated IP address.



Item	Description	Remarks
IP address	IP address for which the rate needs to be limited.	Enter a valid IPv4 or IPv6 address. [Example] 192.168.1.1 or 1234::100
Uplink Limit (pps)	Number of uplink packets per second.	[Example] 1

c Click **Save**.

Follow-up Procedure

- Click **Create** to add more IP addresses for rate limiting.
- Click **Delete** to remove the configuration.
- Click **Refresh** to obtain the latest configuration of rate limiting on designated IP addresses.
- Click **Edit** to modify the number of uplink packets per second allowed on a specified IP address.

4.9.2 Configuring New Session Rate Limiting

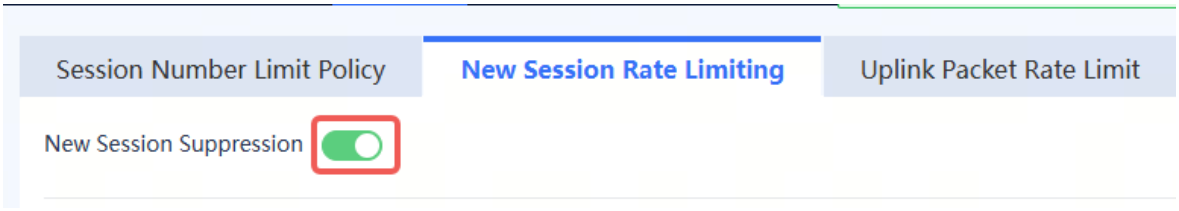
Application Scenario

Configure global new session rate limiting on each IP address or configure new session rate limiting on designated IP addresses. The priority of new session rate limiting on designated IP addresses is higher than that of global new session rate limiting. New session rate limiting prevents a large number of new connections established due to DDoS attacks, which affects normal services.

Procedure

(1) Choose **Policy** > **Session Control** > **New Session Rate Limiting**.

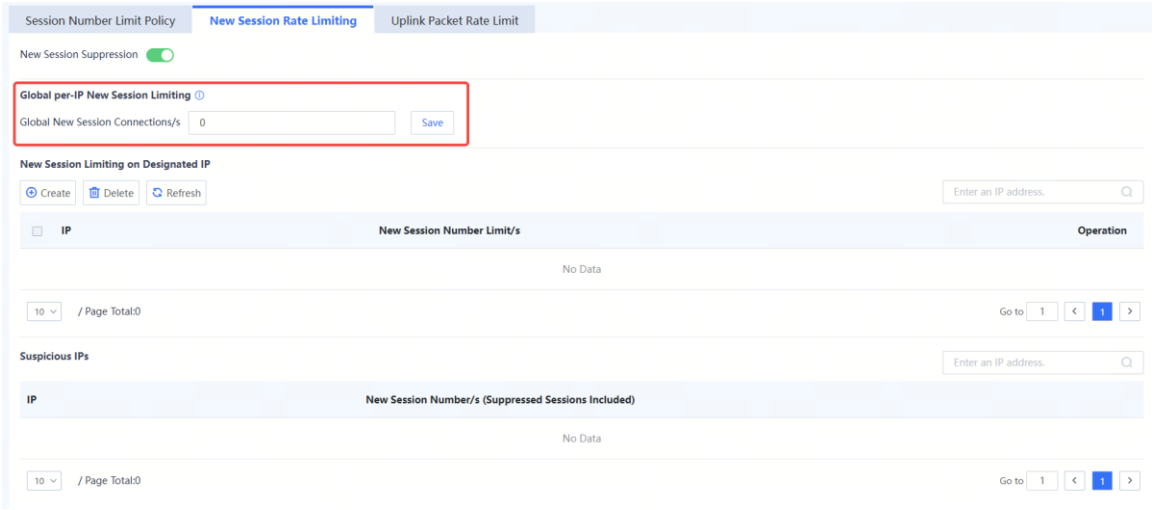
(2) Toggle on to enable new session suppression.



(3) Configure the maximum number of new sessions.

- Global New Session Limiting

  a Configure the maximum number of new session connections on the entire network.

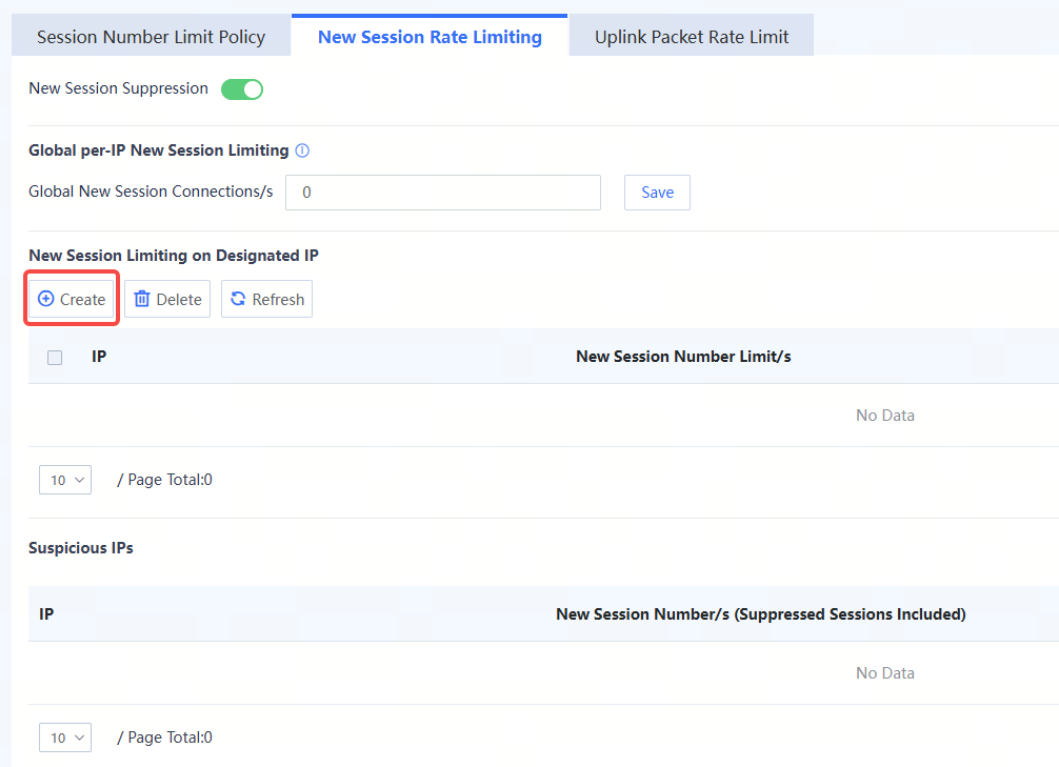


Item	Description	Remarks
Global New Session Connections/s	Configure global new session rate limiting on each IP address. The default value is 0, indicating that the rate is not limited. The priority of new session rate limiting on designated IP addresses is higher than that of global new session rate limiting.	[Example] 300

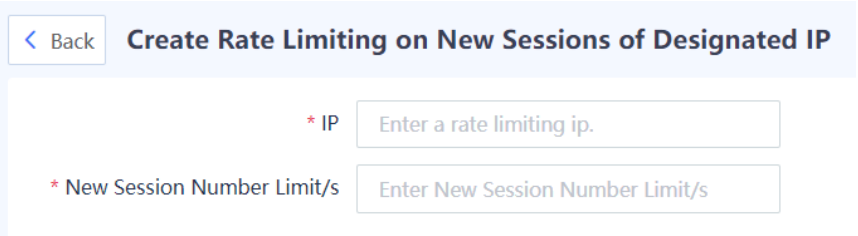
b Click **Save**.

- New Session Limiting on Designated IP Addresses

a Click **Create**.



b Configure new session limiting on designated IP addresses.

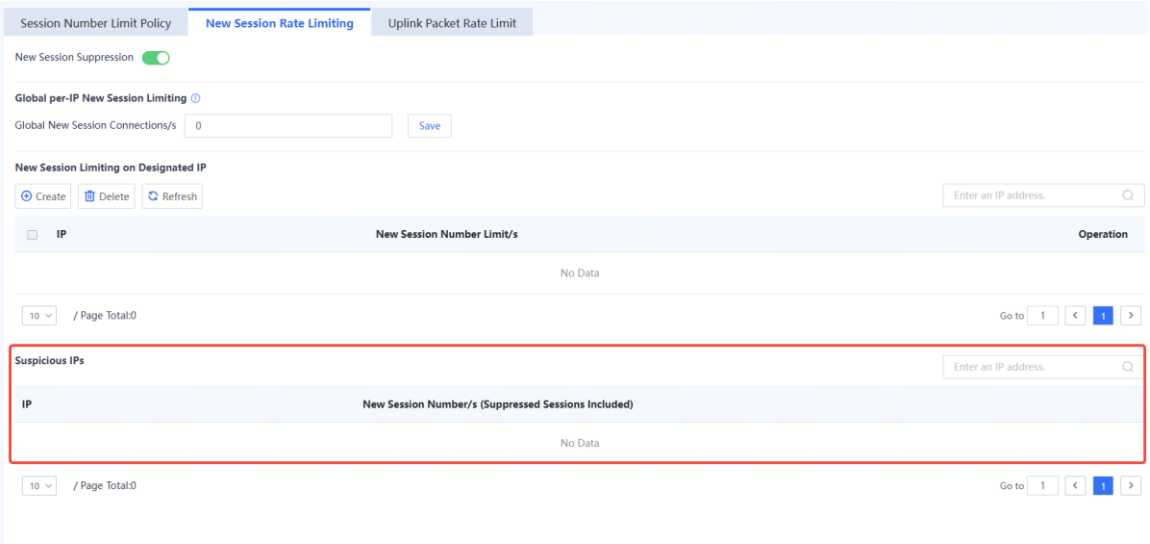


Item	Description	Remarks
IP address	IP address for which new session connections need to be limited.	Enter a valid IPv4 or IPv6 address. [Example] 192.168.1.1 or 1234::100
New Session Number Limit/s	Number of new sessions per second.	[Example] 10

c Click **Save**.

(4) Display information about suspicious IP addresses.

After new session rate limiting is configured, the device collects statistics on the number of new sessions per second based on the source IP addresses of packets. If the new session rate of an IP address exceeds the threshold, the device classifies the IP address as a suspicious IP address. You can check the statistics list to identify suspicious attackers on the network and check whether the configured new session rate limiting takes effect.



Follow-up Procedure

- Click **Create** to add more IP addresses for new session limiting.
- Click **Delete** to remove the configuration.
- Click **Refresh** to obtain the latest configuration of new session limiting on designated IP addresses.
- Click **Edit** to modify the number of new session connections per second allowed on a specified IP address.

4.9.3 Configuring a Session Number Limit Policy

1. Configuring a Manual Suppression Policy

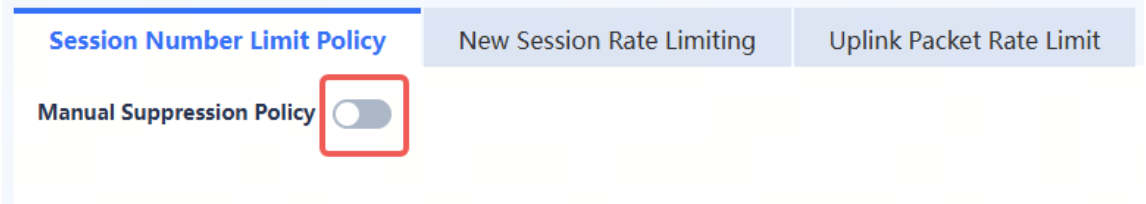
Application Scenario

Manually configure a session number limit policy to control the number of sessions based on the source address, destination address, application, user, service, and time. The session number limit can help allocate session resources more properly and prevent DDoS attacks.

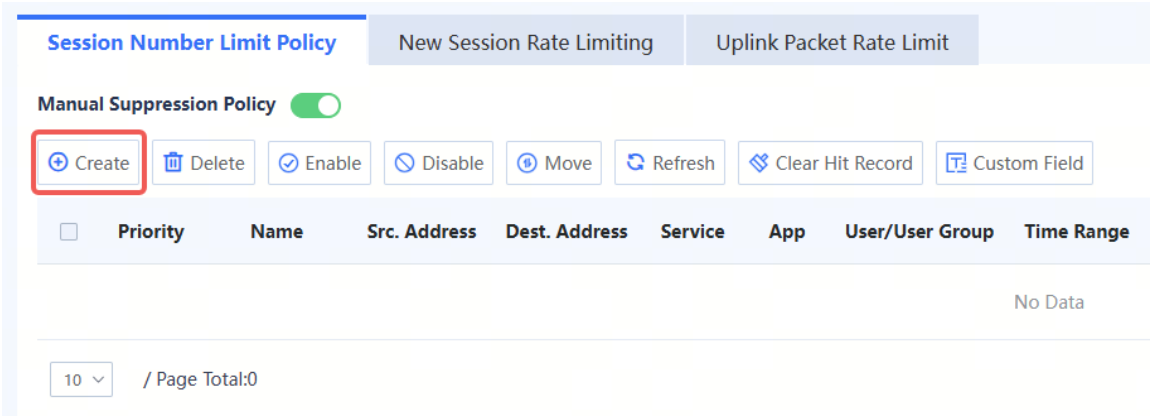
Procedure

(1) Choose **Policy** > **Session Control** > **Session Number Limit Policy**.

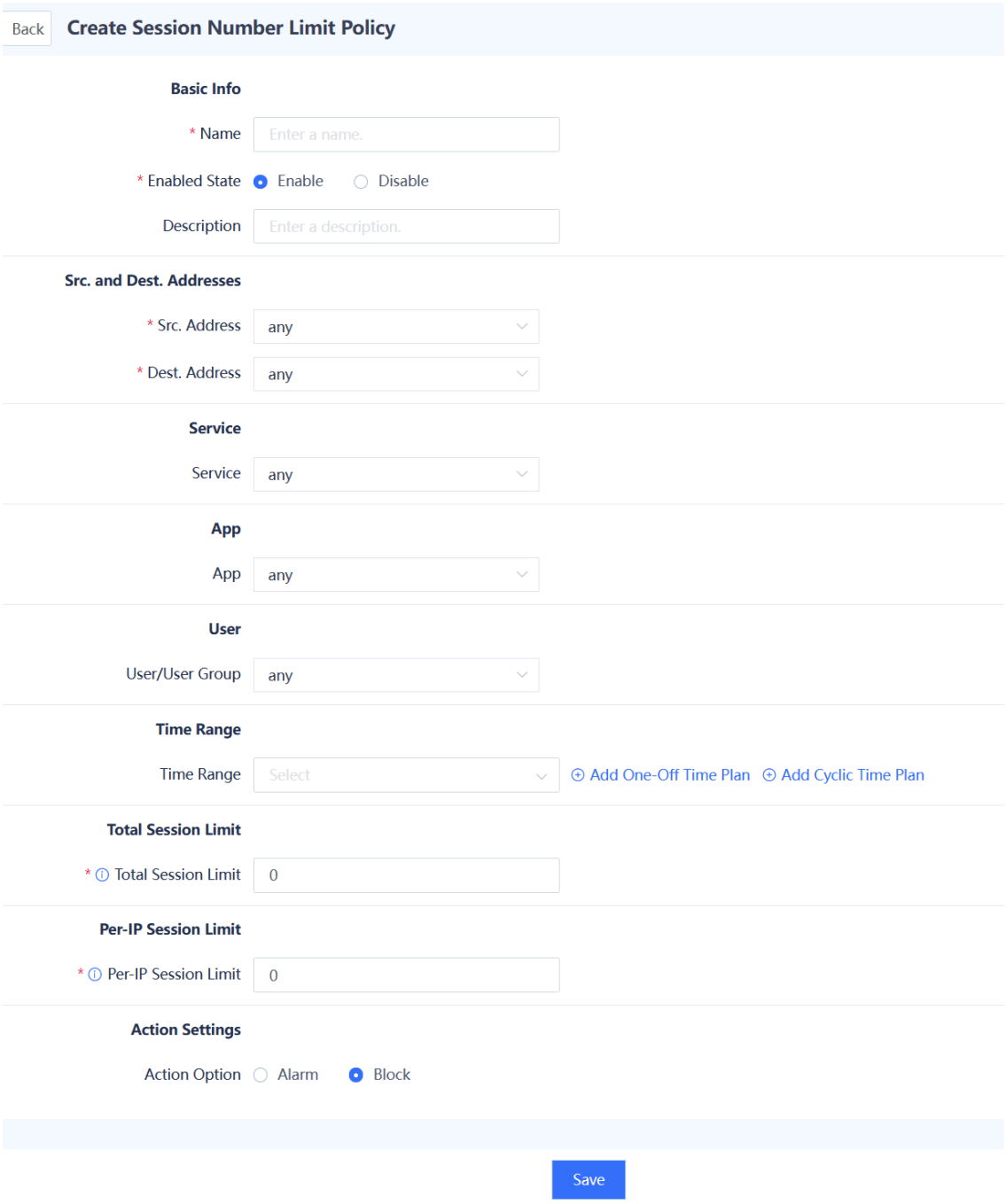
(2) Toggle on  to enable the manual suppression policy function.



(3) Click **Create**.



(4) Configure a policy for limiting the number of sessions.



Item	Description	Remarks
Name	Name of the session number limit policy.	[Example] Test
Enabled State	Enable or disable the policy.	[Example] Enable
Description	Description of the session number limit policy.	[Example] Test

Item	Description	Remarks
Src. Address	Source IP address for policy matching.	Select a value from the drop-down list. [Example] any
Dest. Address	Destination IP address for policy matching.	Select a value from the drop-down list. [Example] any
Service	Service for policy matching.	Select a value from the drop-down list. [Example] any
App	Application for policy matching.	Select a value from the drop-down list. [Example] any
User/User Group	Users for policy matching.	Select a value from the drop-down list. [Example] any
Time Range	Time range for policy matching.	Select a value from the drop-down list. [Example] any
Total Session Limit	Total number of sessions that can be established on all IP addresses that match the policy. The default value is 0, indicating no rate limiting.	[Example] 20
Per-IP Session Limit	Number of sessions that can be established on a single IP address that matches the policy. The value cannot exceed the configured total session limit. The default value is 0, indicating no rate limiting.	[Example] 2

Item	Description	Remarks
Action Option	If the total session limit or per-IP session limit is exceeded, the action specified in the policy is performed. Currently, the following modes are supported: ● **Alarm**: Packets are allowed to pass through, and a log is recorded. ● **Block** (default value): The session is blocked, and a log is recorded.	[Example] Alarm

(5) Click **Save**.

Follow-up Procedure

- Click **Create** to add more session number limit policies.
- Select a session number limit policy and click **Delete** to delete the policy.
- Select a session number limit policy and click **Enable** to enable the policy or click **Disable** to disable the policy.
- Select a session number limit policy and click **Move** to move a policy. The policy listed before has a higher matching priority.
- Select a policy and click **Clear Hit Record** to clear the hit record of the policy and start statistics collection again.
- Click **Custom Field** to specify the fields to be displayed in the policy list to quickly obtain required information.
- Click **Refresh** to obtain the latest policy configuration.

4.10 Blocklist and Allowlist

4.10.1 Overview

CF series firewalls support blocklists and allowlists to block or forward packets based on IP addresses, MAC addresses, or usernames.

- 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, MAC address, or username is added to the blocklist, the packets sent to or from the IP address, MAC address, or username will be discarded by the device.

  For example, if you want to prevent traffic of some IP addresses, MAC addresses, or usernames (such as the attacker sources) on the network from passing the device, add them to the blocklist.

> **Caution**
>
> The IP addresses, MAC addresses, or usernames 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.

4.10.2 Creating an IPv4 Allowlist

Application Scenario

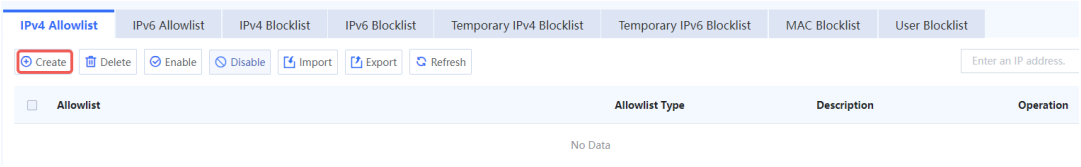
Configure an IPv4 allowlist on the web UI.

Procedure

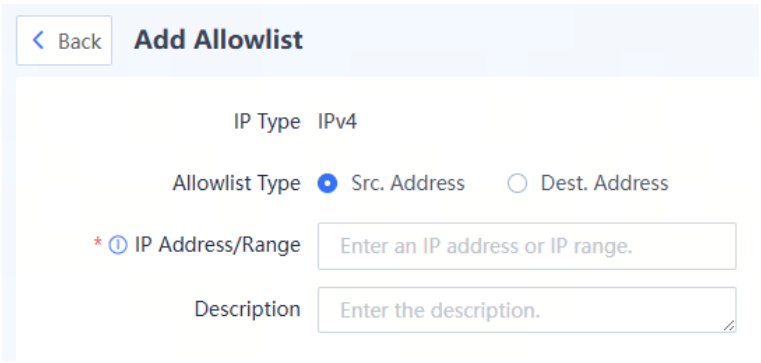
(1) Access the **Add Allowlist** page.

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**.



Item	Description	Remarks
Allowlist Type	Type of the allowlist: ● **Src. Address**: Permit packets sent from this address. ● **Dest. Address**: Permit packets sent to this address.	[Example] Src. Address

IP Address/Range	Allowlist IP address/range.	The following three formats are supported: ● Single IP address: 192.168.1.1 ● Subnet: 192.168.1.0/24 ● IP range: 192.168.1.1-192.168.1.10
Description	Description of the temporary blocklist.	-

(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.

4.10.3 Creating an IPv6 Allowlist

Application Scenario

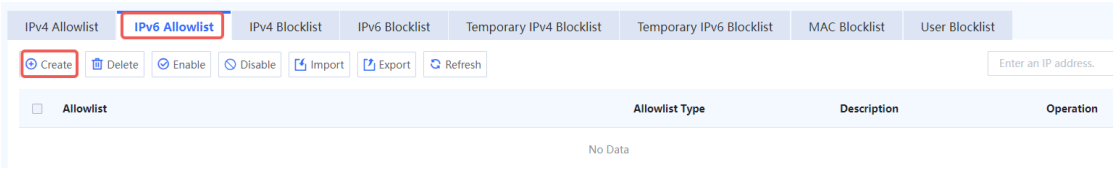
Configure an IPv6 allowlist on the web UI.

Procedure

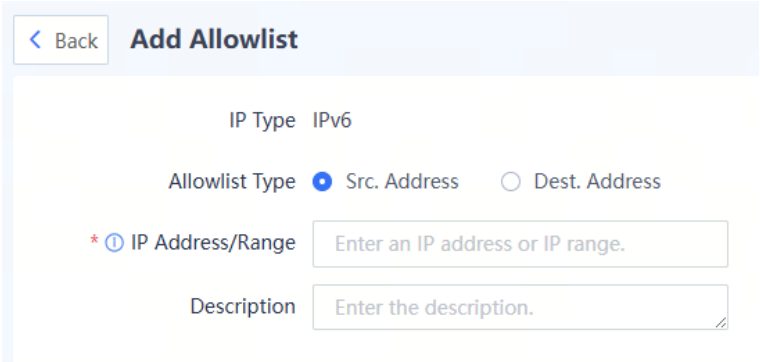
(1) Access the **Add Allowlist** page.

a Choose **Policy** > **Blocklist and Allowlist** > **IPv6 Allowlist**.

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

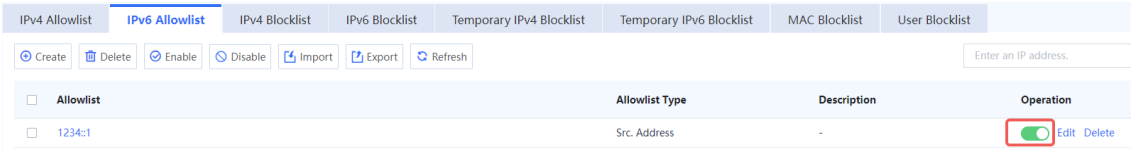


(2) Set parameters for the allowlist policy and click **Save**.



Item	Description	Remarks
Allowlist Type	Type of the allowlist: **Src. Address**: Permit packets sent from this address. **Dest. Address**: Permit packets sent to this address.	[Example] Src. Address
IP Address/Range	Allowlist IP address/range.	The following three formats are supported: Single IP address: 1234::100 Subnet: 1234:100::/64 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.

4.10.4 Creating an IPv4 Blocklist

Application Scenario

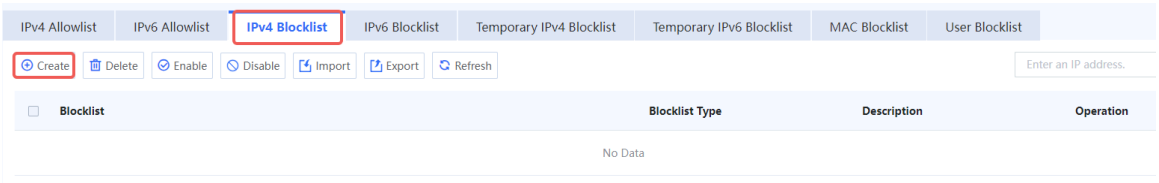
Configure an IPv4 blocklist on the web UI.

Procedure

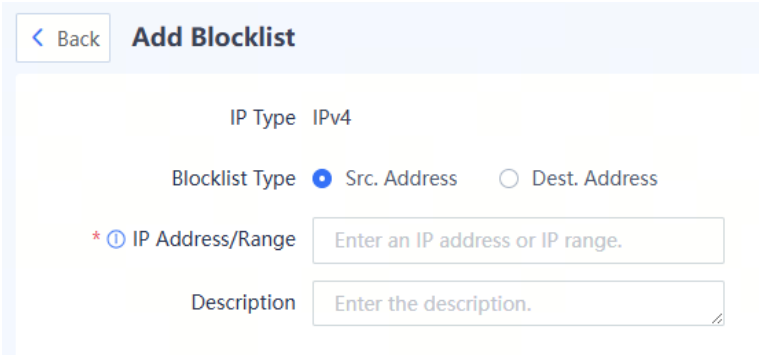
(1) Access the **Add Blocklist** page.

a Choose **Policy** > **Blocklist and Allowlist** > **IPv4 Blocklist**.

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

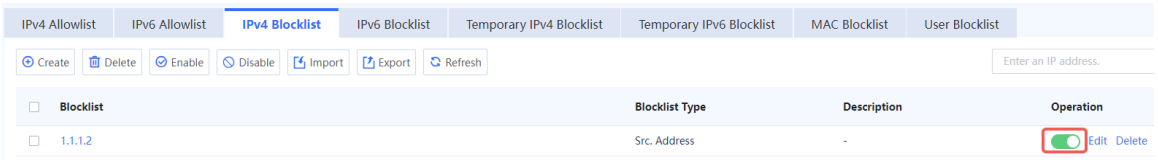


(2) Set parameters for the blocklist policy and click **Save**.



Item	Description	Remarks
Blocklist Type	Type of the blocklist: ● **Src. Address**: Block packets sent from this address. ● **Dest. Address**: Block packets sent to this address.	[Example] Src. Address
IP Address/Range	Blocklist IP address/range.	The following three formats are supported: ● Single IP address: 192.168.1.1 ● Subnet: 192.168.1.0/24 ● 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.

4.10.5 Creating an IPv6 Blocklist

Application Scenario

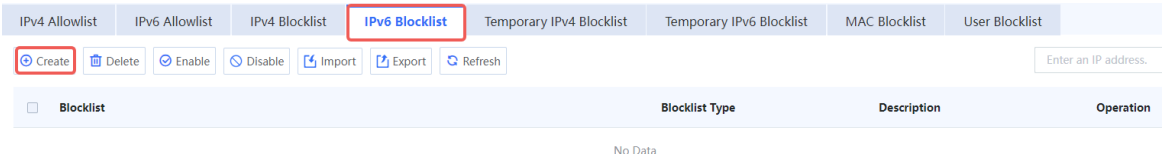
Configure an IPv6 blocklist on the web UI.

Procedure

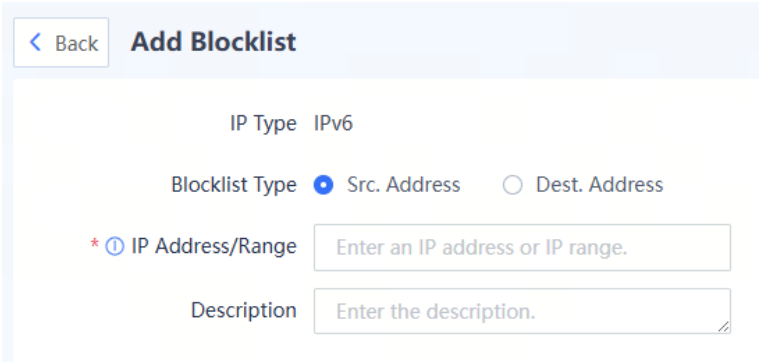
(1) Access the **Add Blocklist** page.

a Choose **Policy** > **Blocklist and Allowlist** > **IPv6 Blocklist**.

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



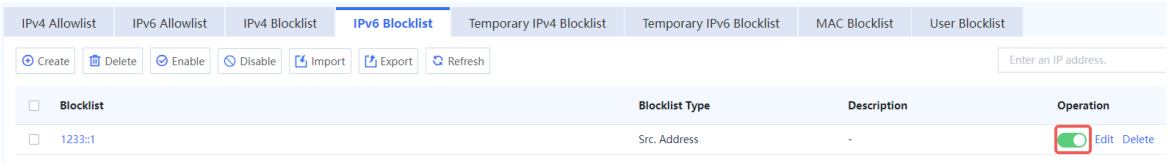
(2) Set parameters for the blocklist policy and click **Save**.



Item	Description	Remarks
Blocklist Type	Type of the blocklist: ● **Src. Address**: Block packets sent from this address. ● **Dest. Address**: Block packets sent to this address.	[Example] Src. Address

IP Address/Range	Blocklist IP address/range.	The following three formats are supported: ● Single IP address: 1234::100 ● Subnet: 1234:100::/64 ● 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.

4.10.6 Creating a Temporary IPv4 Blocklist

Application Scenario

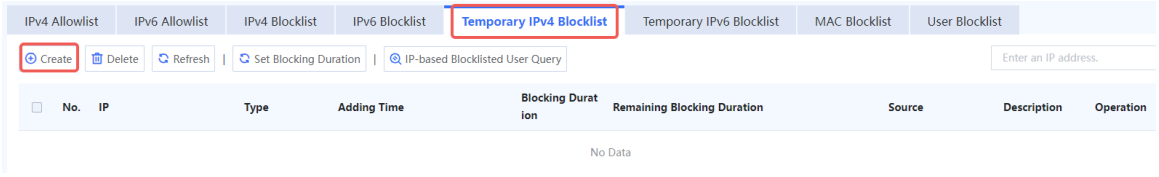
Configure a temporary IPv4 blocklist on the web UI.

Procedure

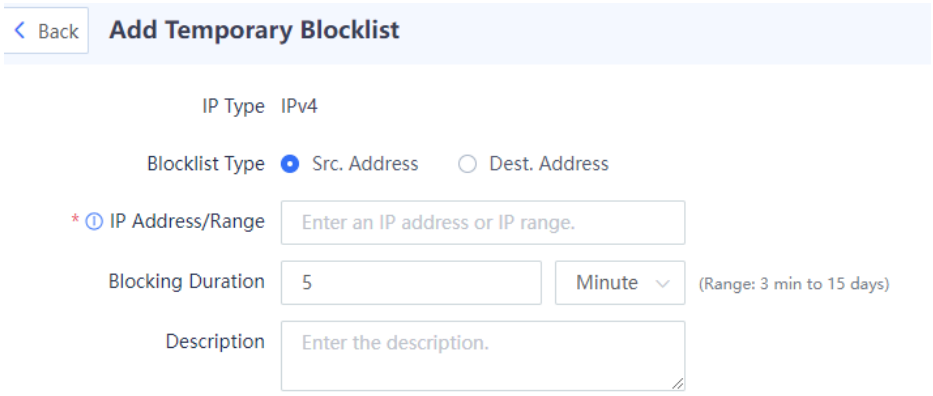
(1) Access the **Add Temporary Blocklist** page.

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**.

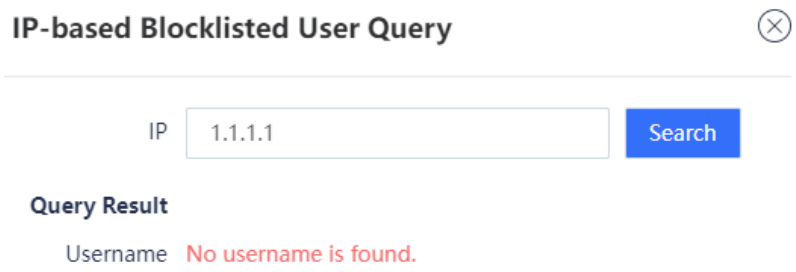


Item	Description	Remarks
Blocklist Type	Type of the temporary blocklist: ● **Src. Address**: Block packets sent from this address. ● **Dest. Address**: Block packets sent to this address.	[Example] Src. Address
IP Address/Range	Temporary blocklist IP address/range.	The following three formats are supported: ● Single IP address: 192.168.1.1 ● Subnet: 192.168.1.0/24 ● 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.	-

(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**. This setting takes effect only for the temporary blocklist that is not manually added.
- Click **IP-based Blocklisted User Query** to query the username of a specified IPv4 address.



4.10.7 Creating a Temporary IPv6 Blocklist

Application Scenario

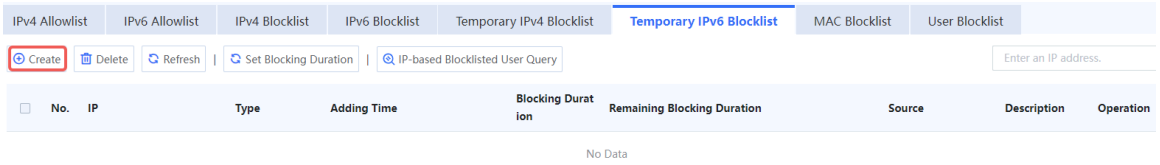
Configure a temporary IPv6 blocklist on the web UI.

Procedure

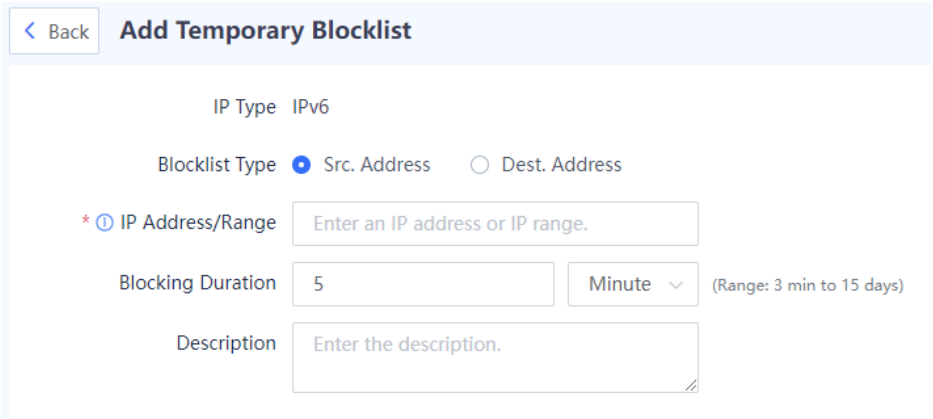
(1) Access the **Add Temporary Blocklist** page.

a Choose **Policy** > **Blocklist and Allowlist** > **Temporary IPv6 Blocklist**.

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



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



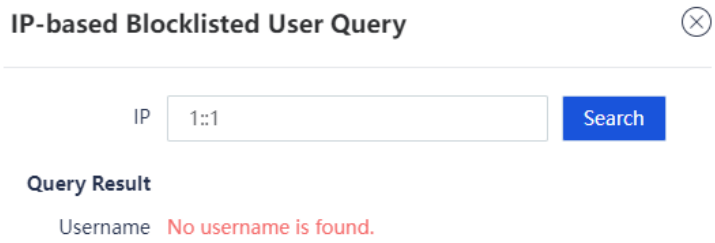
Item	Description	Remarks
Blocklist Type	Type of the temporary blocklist: ● **Src. Address**: Block packets sent from this address. ● **Dest. Address**: Block packets sent to this address.	[Example] Src. Address

IP Address/Range	Temporary blocklist IP address/range.	The following three formats are supported: ● Single IP address: 1234::100 ● Subnet: 1234:100::/64 ● 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.	-

(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**. This setting takes effect only for the temporary blocklist that is not manually added.
- Click **IP-based Blocklisted User Query** to query the username of a specified IPv6 address.



4.10.8 Creating a MAC Address Blocklist

Application Scenario

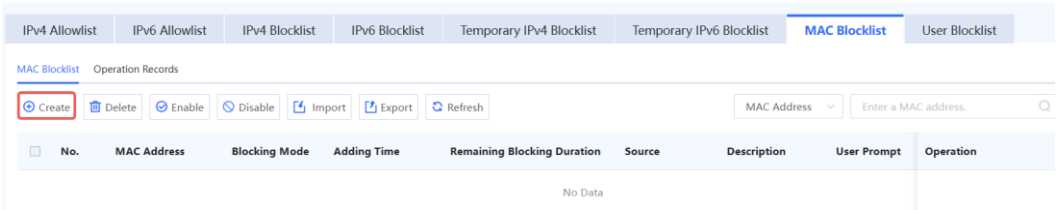
Manually configure a MAC address blocklist through the web.

Procedure

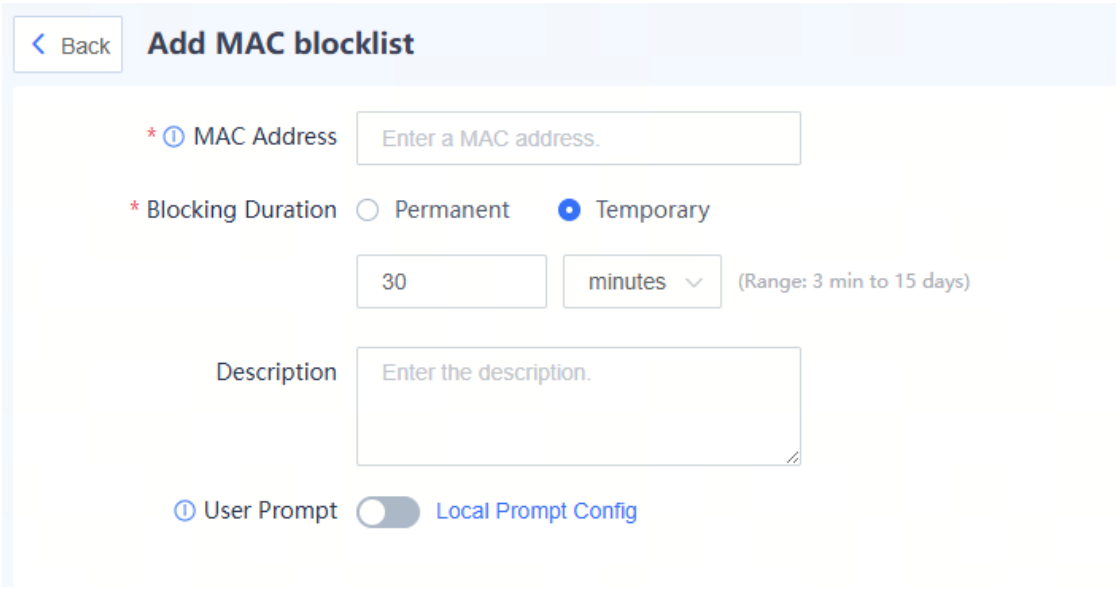
(1) Access the **Add MAC blocklist** page.

d Choose **Policy** > **Blocklist and Allowlist** > **MAC Blocklist** > **MAC Blocklist**.

e Click **Create** at the top of the operation pane.

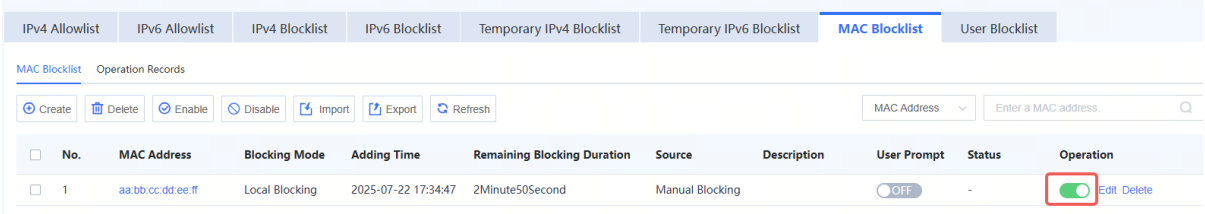


(2) Configure the blocklist and click **Save**.



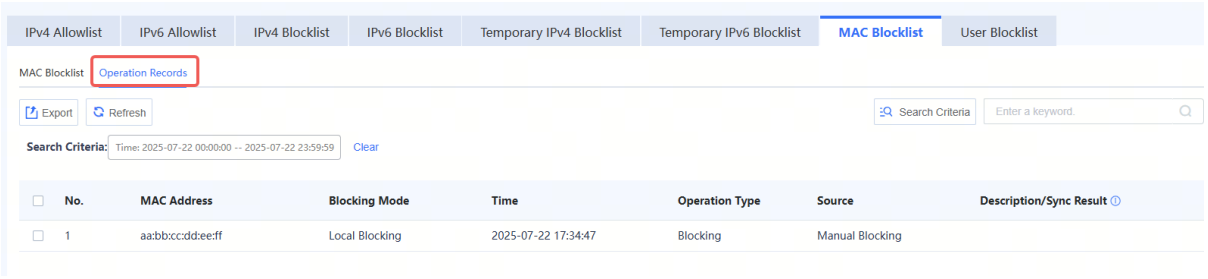
Item	Description	Remarks
MAC Address	MAC address in the blocklist.	[Example] aa:bb:cc:dd:ee:ff
Blocking Duration	● **Permanent**: Blocks traffic from a blocklisted MAC address permanently. ● **Temporary**: Blocks traffic from a MAC address in the blocklist temporarily. After the blocking period expires, the MAC address is automatically deleted from the blocklist.	[Example] Temporary
Description	Reason for traffic blocking.	-
User Prompt	Configure the function of sending blocking notifications to users. After this function is enabled, the system will automatically remind the handled terminal and display customized prompt information on the blocking page. Click **Local Prompt Config** to access the **Info Push** page and configure the blocklist-based blocking prompt. For details, see 7.8 Information Push.	-

(3) For local blocking, toggle on the switch in the **Operation** column to enable the blocklist.

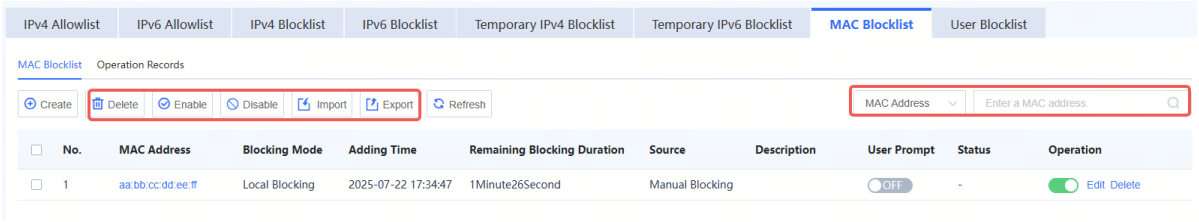


(4) (Optional) Choose **Policy** > **Blocklist and Allowlist** > **MAC Blocklist** > **Operation Records** to display the operation history of the MAC address blocklist.

When a MAC address blocklist is added or deleted, the operation history is recorded.



Follow-up Procedure



- To delete multiple blocklists in a batch, select the blocklists and click **Delete**.
- To make multiple blocklists for local blocking take effect, select the blocklists and click **Enable**.
- To disable multiple blocklists for local blocking, select the blocklists and click **Disable**.
- Click **Import**, download the CSV template, and fill in local blocklists to import them in batches.
- Click **Export** to export all blocklists of local blocking to the local device.
- Enter **MAC Address** or **Source** in the search bar to search for blocklists matching the search criteria.

4.10.9 Creating a User Blocklist

Application Scenario

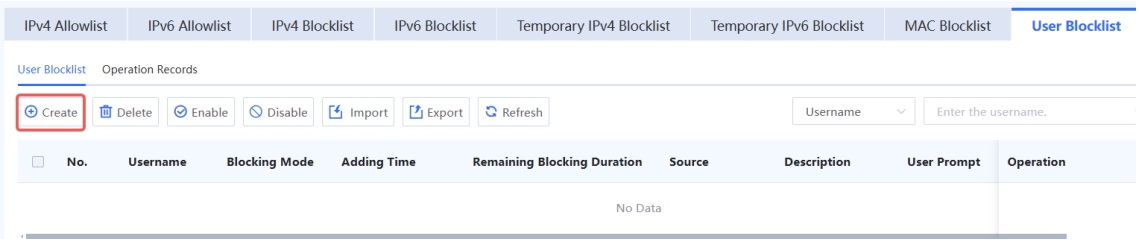
Manually configure a user blocklist through the web.

Procedure

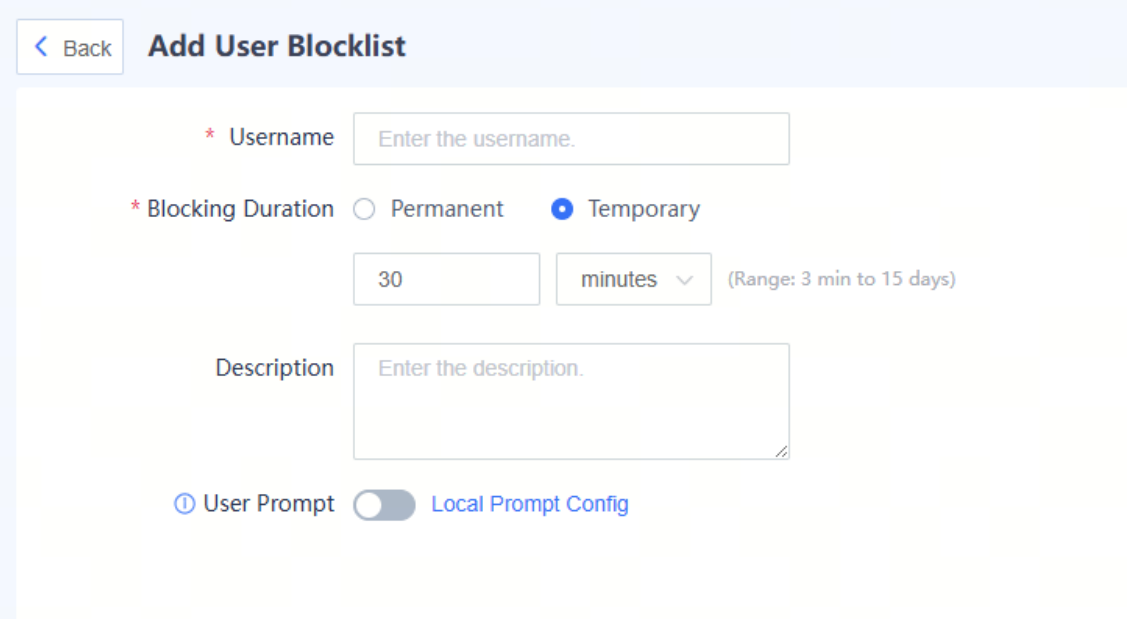
(1) Access the Add User Blocklist page.

a Choose **Policy** > **Blocklist and Allowlist** > **User Blocklist** > **User Blocklist**.

b Click **Create** at the top of the operation pane.

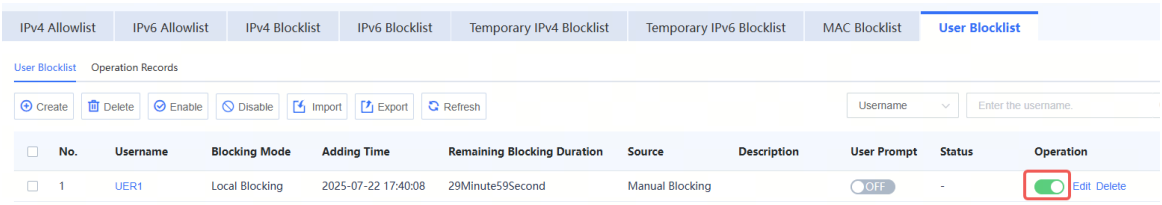


(2) Configure the blocklist and click **Save**.



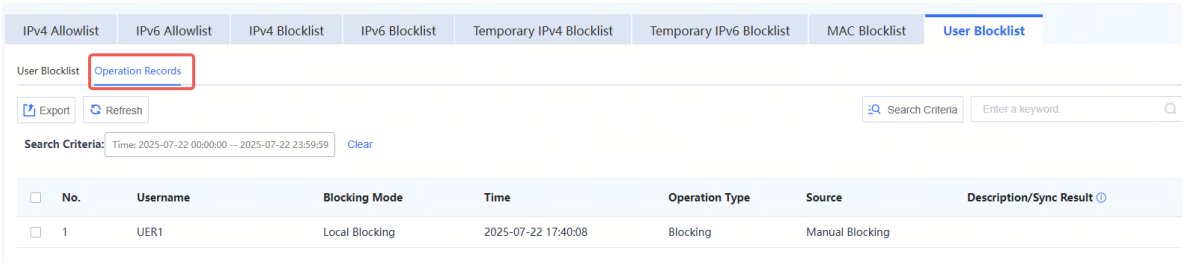
Item	Description	Remarks
Username	Blocklisted user name.	[Example] User1
Blocking Duration	● Permanent: Blocks traffic from a blocklisted MAC address permanently. ● Temporary: Blocks traffic from a MAC address in the blocklist temporarily. After the blocking period expires, the MAC address is automatically deleted from the blocklist.	[Example] Temporary
Description	Reason for traffic blocking.	-
User Prompt	Configure the function of sending blocking notifications to users. After this function is enabled, the system will automatically remind the handled user and display customized prompt information on the blocking page. Click **Local Prompt Config** to access the **Info Push** page and configure the blocklist-based blocking prompt. For details, see 7.8 Information Push.	-

(3) For local blocking, toggle on the switch in the **Operation** column to enable the blocklist.

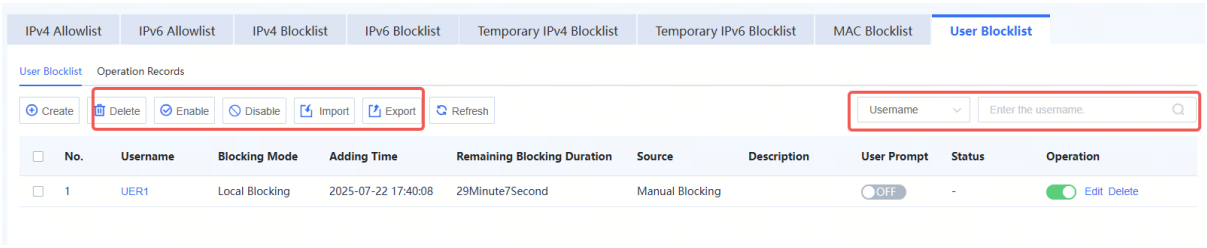


(4) (Optional) Choose **Policy** > **Blocklist and Allowlist** > **User Blocklist** > **Operation Records** to display the operation history of the user blocklist.

When a user blocklist is added or deleted, the operation history is recorded.



Follow-up Procedure



- To delete multiple blocklists in a batch, select the blocklists and click **Delete**.
- To make multiple blocklists for local blocking take effect, select the blocklists and click **Enable**.
- To disable multiple blocklists for local blocking, select the blocklists and click **Disable**.
- Click **Import**, download the CSV template, and fill in local blocklists to import them in batches.
- Click **Export** to export all blocklists of local blocking to the local device.
- Enter **Username** or **Source** in the search bar to search for blocklists matching the search criteria.

4.11 SSL Proxy

4.11.1 Configuring an SSL Proxy Policy

To protect data security and privacy, traffic of many applications is encrypted by Transport Layer Security (TLS) during transmission. To guarantee service security, the device needs to decrypt the encrypted traffic so that security functional modules such as intrusion prevention and virus protection can thoroughly check the decrypted traffic and files. The firewall can decrypt only IPv4-based HTTPS traffic.

The SSL proxy function supports the following decryption modes.

Decryption Mode	Description
Decrypt Internet access packets of terminals	The device decrypts Internet access traffic from intranet terminals passing through it and works with security check functions such as intrusion prevention and virus protection to block risky traffic and protect intranet terminal security.
Decrypt packets destined for LAN servers	The device decrypts intranet server access traffic from extranet terminals passing through it and works with security check functions such as intrusion prevention and virus protection to block risky traffic and protect intranet server security.

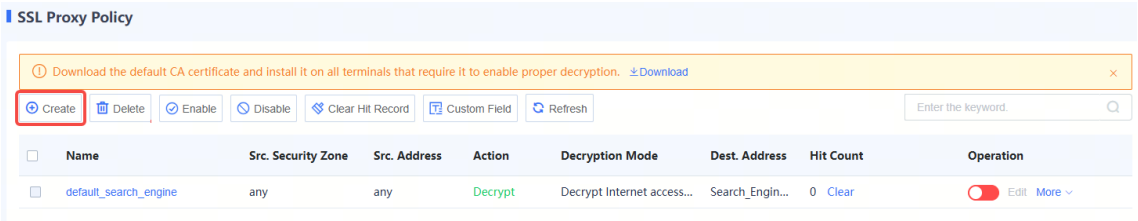
Prerequisites

- You have obtained the URL category license and updated the URL signature library to the latest version before configuring an SSL proxy policy to decrypt Internet access packets to domain names of a specific type. For details about URL category, see 5.3.2 URL Category.
- It is recommended to enable the hardware acceleration function to improve the SSL proxy performance. For details about hardware acceleration, see 7.2.5 Hardware Acceleration.
- If you set the SSL decryption mode to **Decrypt Internet access packets of terminals**, you must configure an SSL proxy certificate (CA certificate) first. For details about the SSL proxy certificate, see 5.9.3 SSL Certificate.
- If you set the SSL decryption mode to **Decrypt packets destined for LAN servers**, you must import a server certificate first. For details about the server certificate, see 5.9.3 4. Importing a Server Certificate,

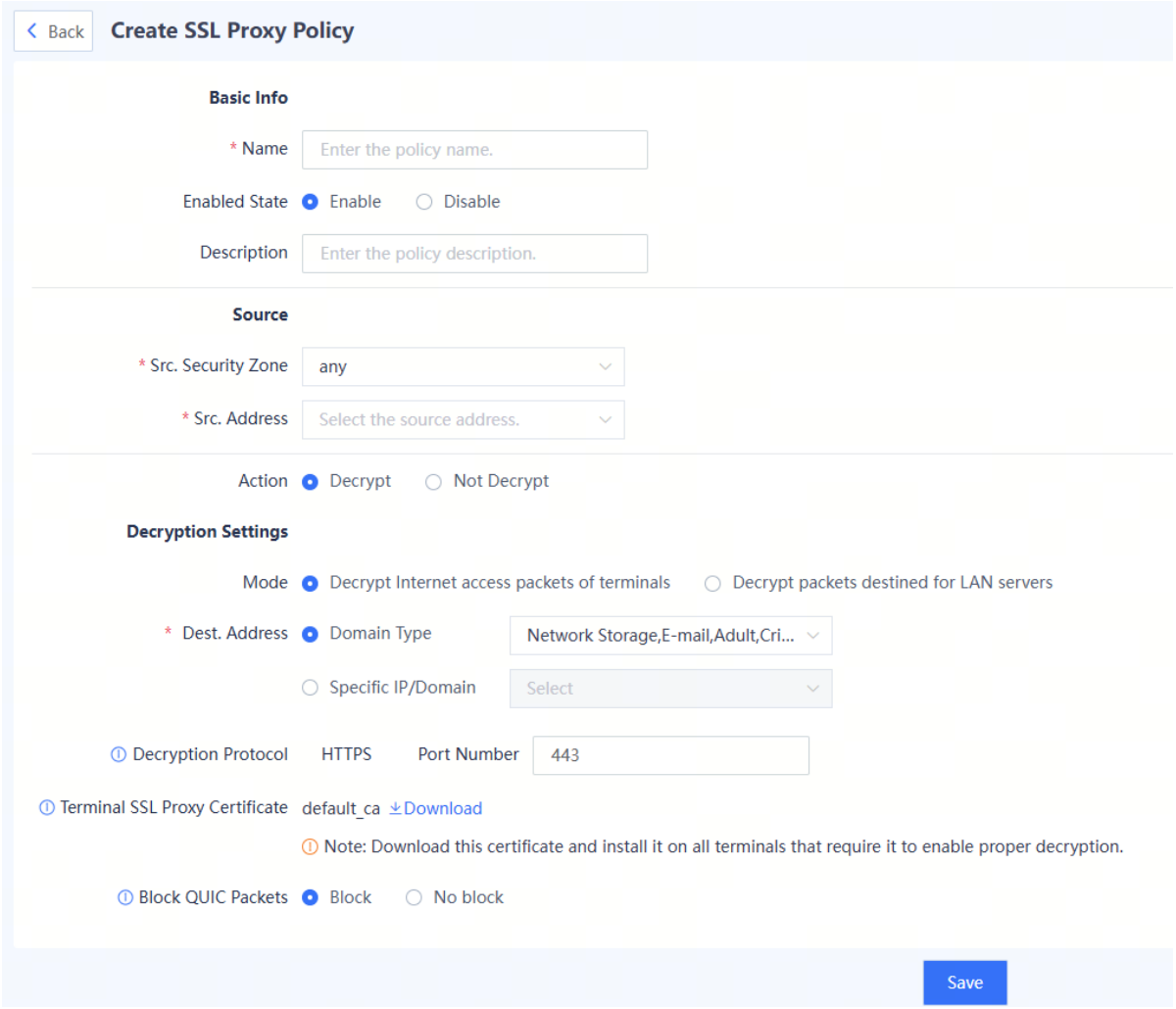
Procedure

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

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



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



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

Item	Description	Remarks
Basic Info		
Name	Name of the SSL proxy policy.	[Example] SSLPolicy_1
Enabled State	Whether to enable the new SSL proxy policy.	[Example] Enable
Description	Description of SSL proxy policy.	[Example] Decrypt the HTTPS encrypted traffic from security zone 1 to security zone 2.
Src. and Dest.		

Item	Description	Remarks
Src. Security Zone	Source security zone that initiates the target data connection.	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. Any indicates all interfaces. [Example] trust
Src. Address	Source address that initiates the target data connection.	Click the drop-down list, and select a source address in the **To-be-selected** area. The selected address is automatically added to the **Selected** area. [Example] any
Dest. Security Zone	Destination security zone of the target data connection.	Click the drop-down list, and select a destination security zone in the **To-be-selected** area. The selected zone is automatically added to the **Selected** area. Click **Add Security Zone** to add a custom security zone. Any indicates all interfaces. [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
Service	Service type of the target data connection request.	[Example] any

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

Item	Description	Remarks
Basic Info		
Name	Name of the SSL proxy policy.	[Example] SSLPolicy_1
Enabled State	Whether to enable the new SSL proxy policy.	[Example] Enable
Description	Description of SSL proxy policy.	[Example] Decrypt the HTTPS encrypted traffic from security zone 1 to security zone 2.
Source		

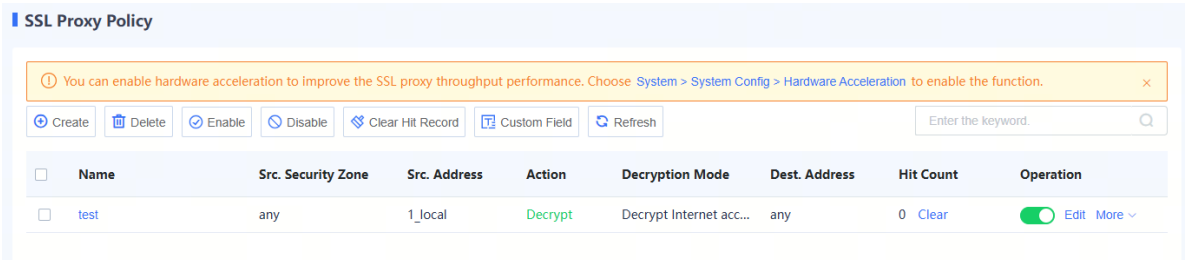
Item	Description	Remarks
Src. Security Zone	Source security zone that initiates the target data connection.	Click the drop-down list, and select a source security zone in the **To-be-selected** area. The selected zone is automatically added to the **Selected** area. Click **Add Security Zone** to add a custom security zone. Any indicates all interfaces. [Example] trust
Src. Address	Source address that initiates the target data connection.	Click the drop-down list, and select a source address in the **To-be-selected** area. The selected address is automatically added to the **Selected** area. [Example] any
Action Option	Action taken by the SSL proxy policy: decrypting or not decrypting the content of target data connection. If **Decrypt** is selected, you need to configure parameters in the Decryption Settings area to specify the scope for decryption and the certificate required.	[Example] Decrypt
Decryption Settings		
Mode	Decryption mode: Decrypt Internet access packets of terminals Decrypt packets destined for LAN servers	[Example] Decrypt Internet access packets of terminals
Mode: Decrypt Internet access packets of terminals		

Item	Description	Remarks
Dest. Address	Destination address of traffic from terminals to be decrypted. Domain Type: Specifies the domain name type of traffic from terminals to be decrypted. Select a domain name type to be decrypted from URL categories predefined in the system. The option any indicates all domain names. Specific IP/Domain: Specifies the IP address or domain name of traffic from terminals to be decrypted. Click the input field and select the destination IPv4 address or domain name to be decrypted.	If the destination address is a specific IP address or domain name, click Add Address to create a custom IPv4 address object and a domain name object. If the destination address is a domain name type or a specific domain name, encrypted DNS packets may fail to match an SSL proxy policy. It is recommended to enable Encrypted Request Blocking and Disable ECH for Negotiation Requests in the DNS Protection area. For details about DNS protection, see 4.7.6 DNS Protection. [Example] any
Decryption Protocol	Protocol type and port number of packets to be decrypted. Currently, the device can decrypt HTTPS packets only.	The default port number of the protocol is 443. If you enter multiple port numbers, separate them with a comma (,), such as "443,800". [Example] HTTPS and Port Number 443

Item	Description	Remarks
Terminal SSL Proxy Certificate	SSL proxy certificate used for decryption. The built-in CA certificate of the device (default_ca) is used by default. If you want to modify the SSL proxy certificate, choose **Object** > **Certificate** > **SSL Certificate** > **SSL Proxy Certificate**, import the new certificate, and then set the certificate as trusted. For details, see 5.9.3 2. Importing an SSL Proxy Certificate. After you configure an SSL proxy certificate, you must download the certificate and install it to all the terminals whose traffic needs to be decrypted.	[Example] default_ca
Block QUIC Packets	QUIC packets cannot be decrypted. To guarantee security, you are advised to block QUIC packets. After QUIC packets are blocked, communicating parties automatically switch to HTTPS for connection, not affecting normal service operation.	[Example] Block
Mode: Decrypt packets destined for LAN servers		
Server IP	IP address of the specified server traffic from which is decrypted.	Select an existing address object from the field. Then, click Add Address to add an IPv4 address object or click Add Address Group to add an IPv4 address group.
Decryption Protocol	Protocol type and port number of packets to be decrypted. Currently, the device can decrypt HTTPS packets only.	The default port number of the protocol is 443. If you enter multiple port numbers, separate them with a comma (,), such as "443,800". [Example] HTTPS and Port Number 443

Item	Description	Remarks
Server Certificate	Server certificate used to establish a trust relationship between the device and the client or server when SSL proxy is enabled.	Select a server certificate that has been imported to the device from the drop-down list box, or click Import to import a server certificate. For details about how to import a server certificate, see 5.9.3 4. Importing a Server Certificate.

Follow-up Procedure



- 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.

4.11.2 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.

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

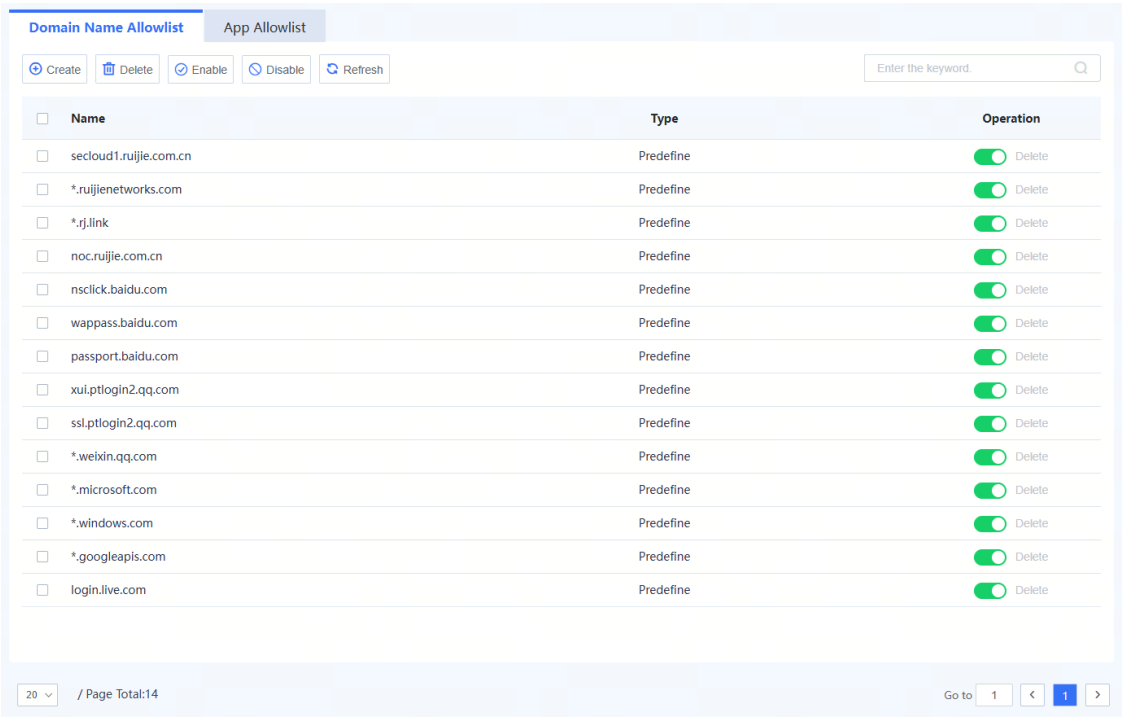
If the traffic of certain domain names does not need to be decrypted, you can add the domain names to the allowlist. The device does not decrypt the traffic of the domain names in the allowlist.

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

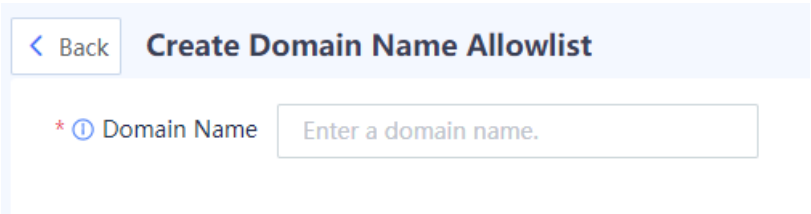
(1) Choose **Policy** > **SSL Proxy** > **SSL Proxy Allowlist** > **Domain Name Allowlist**.

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.



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

The Create Domain Name Allowlist page is displayed.



(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

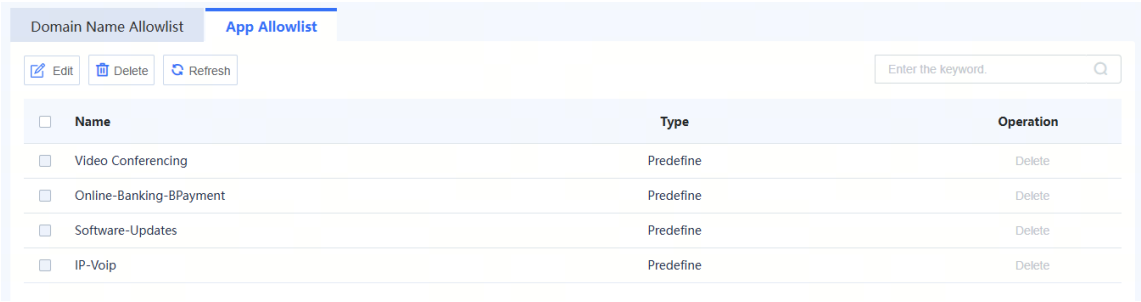
Application Scenario

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.

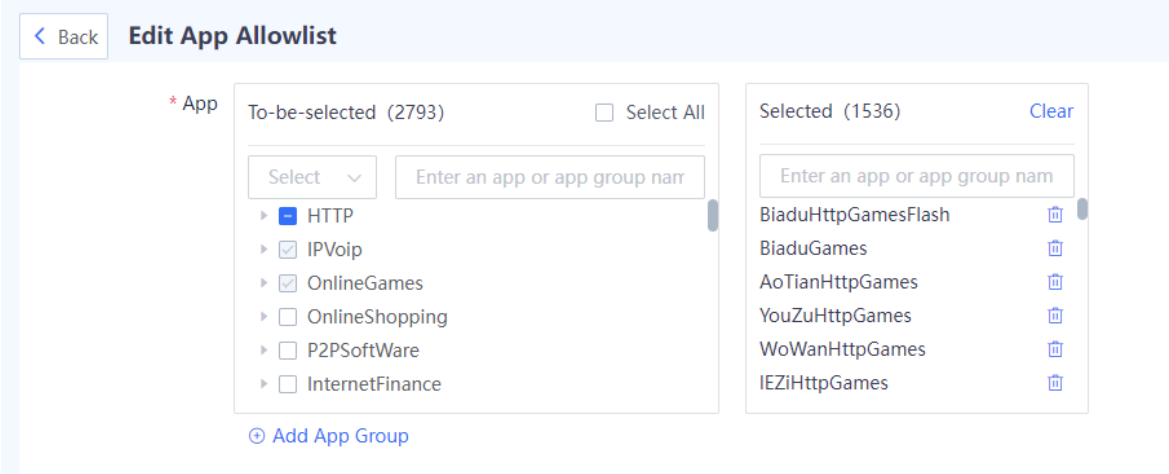
Procedure

(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.

5 Object Configuration and Management

5.1 Address Object

5.1.1 Overview

1. Address Object and Address Group Object

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

Address Object

An address object contains one or more IP addresses or MAC 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:

- IPv4 addresses, IPv6 addresses, or MAC addresses
- 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.

2. Domain Name Object

A domain name object is a set of domain names and can be referenced by policies (such as security policies, traffic control policies, and intelligent routing) to implement domain name-based traffic control based on policies.

For example, a school campus network has multiple external network lines with different bandwidths. Some courses require long-term access to specific online education platforms, and related websites have high requirements for network speeds and stability. To ensure smooth access, you can configure a domain name-based traffic control policy.

Create a domain name object that contains the domain names of online education platforms, and reference the domain name object as the destination address in a traffic control policy to steer traffic destined for the domain names to high-speed and low-latency external network lines.

5.1.2 Creating an IPv4 Address Object

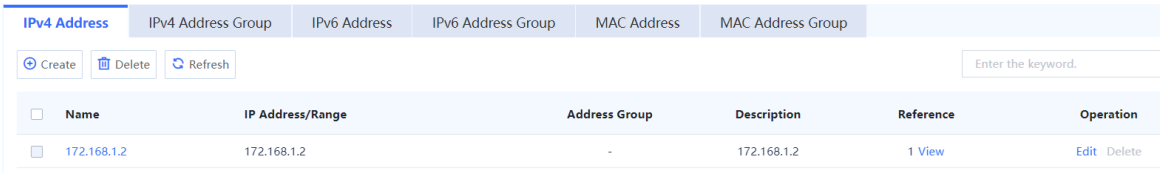
Application Scenario

Create an address object on the web UI.

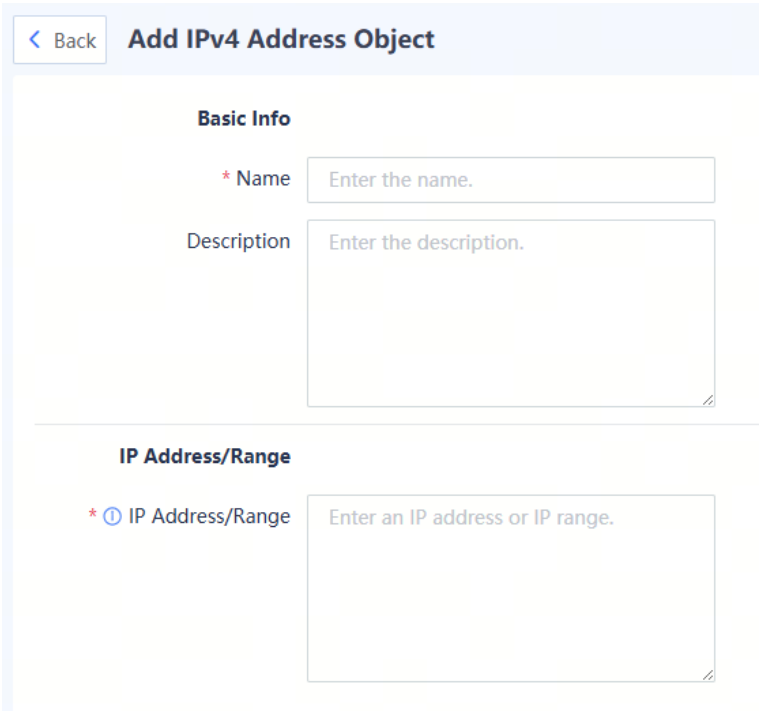
Procedure

(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.	[Example] Addr1
Description	Description of the IP address object.	[Example] For office area 1

Item	Description	Remarks
IP Address/Range	IP address or range.	Three configuration methods are supported: ● 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 The wildcard (*) indicating any string can be added in an IP address or IP range. It can only be placed in the middle two bytes of an IP address, for example, 192.*.*.1 or 192.*.*.1-192.*.*.3. Other positions are not supported.

(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.

5.1.3 Creating an IPv4 Address Group Object

Application Scenario

Create an address group object on the web UI.

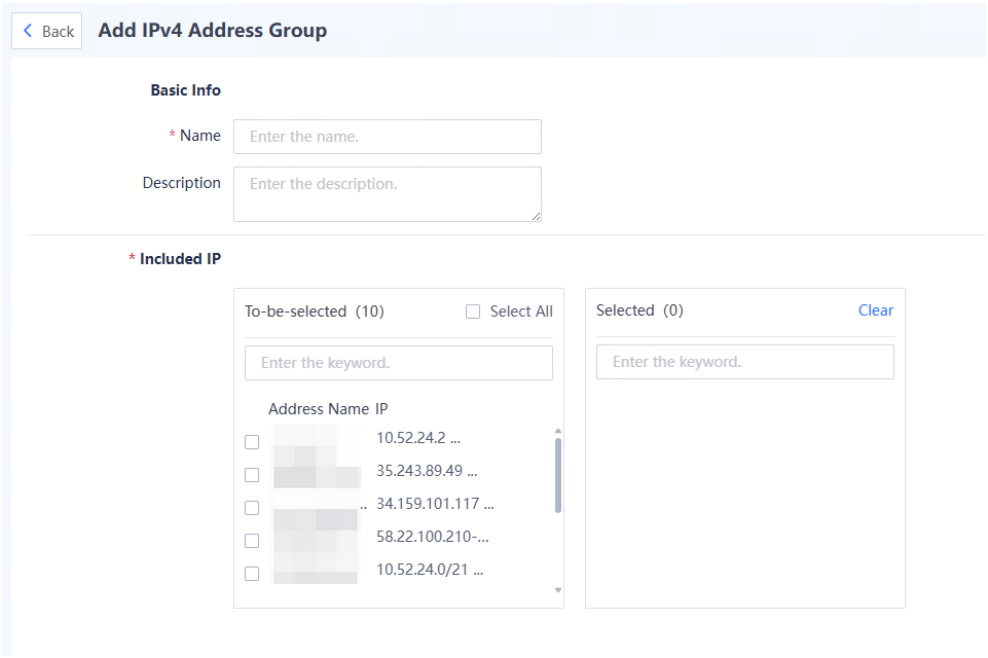
Procedure

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

a Choose **Object** > **Address** > **IPv4 Address Group**.



b Click **Create**.



(2) Set parameters for the address group object.

Item	Description	Remarks
Name	Name of the address group object.	[Example] Addr_total
Description	Description of the address group object.	[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.

5.1.4 Creating an IPv6 Address Object

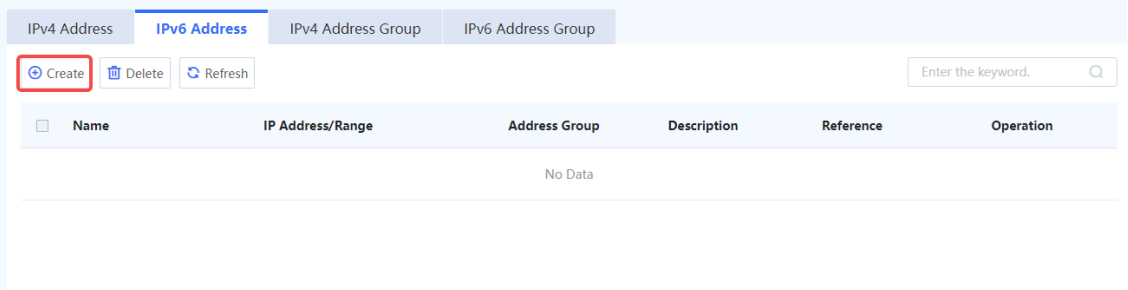
Application Scenario

Create an address object on the web UI.

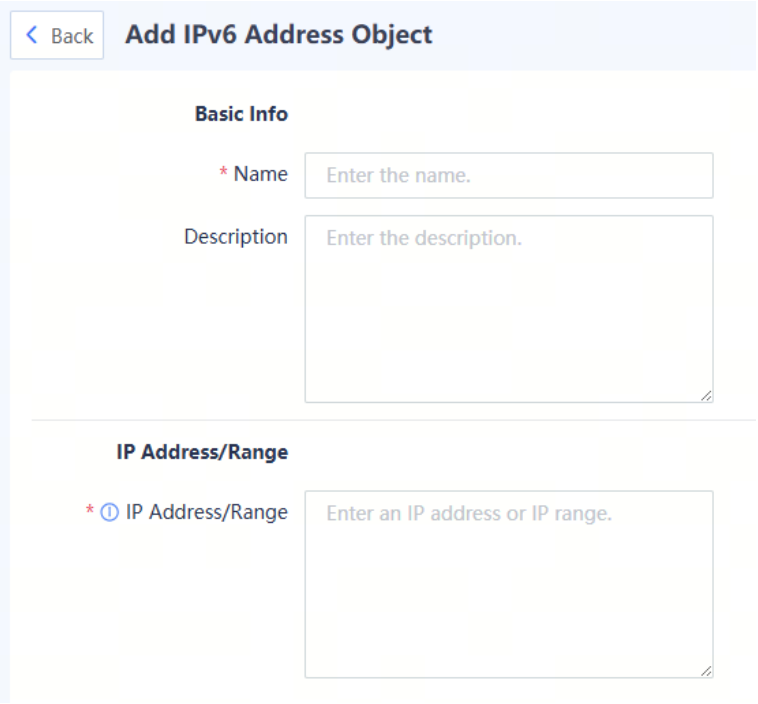
Procedure

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

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



b Click **Create**.



(2) Set parameters for the address object.

Item	Description	Remarks
Name	Name of the IP address object.	[Example] Addr1
Description	Description of the IP address object.	[Example] For office area 1

Item	Description	Remarks
IP Address/Range	IP address or range.	Three configuration methods are supported: ● 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

(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.

5.1.5 Creating an IPv6 Address Group Object

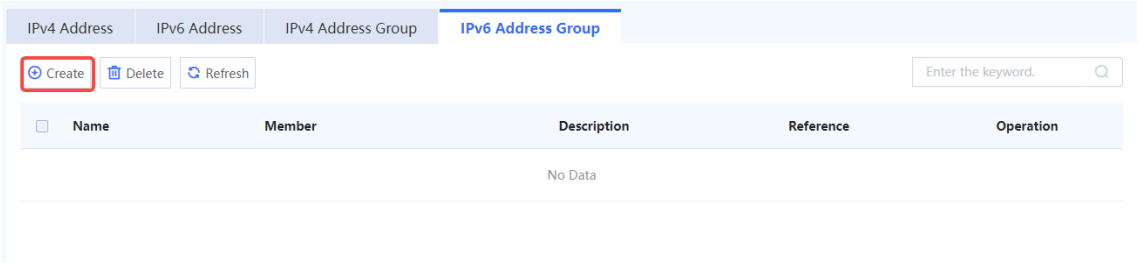
Application Scenario

Create an address group object on the web UI.

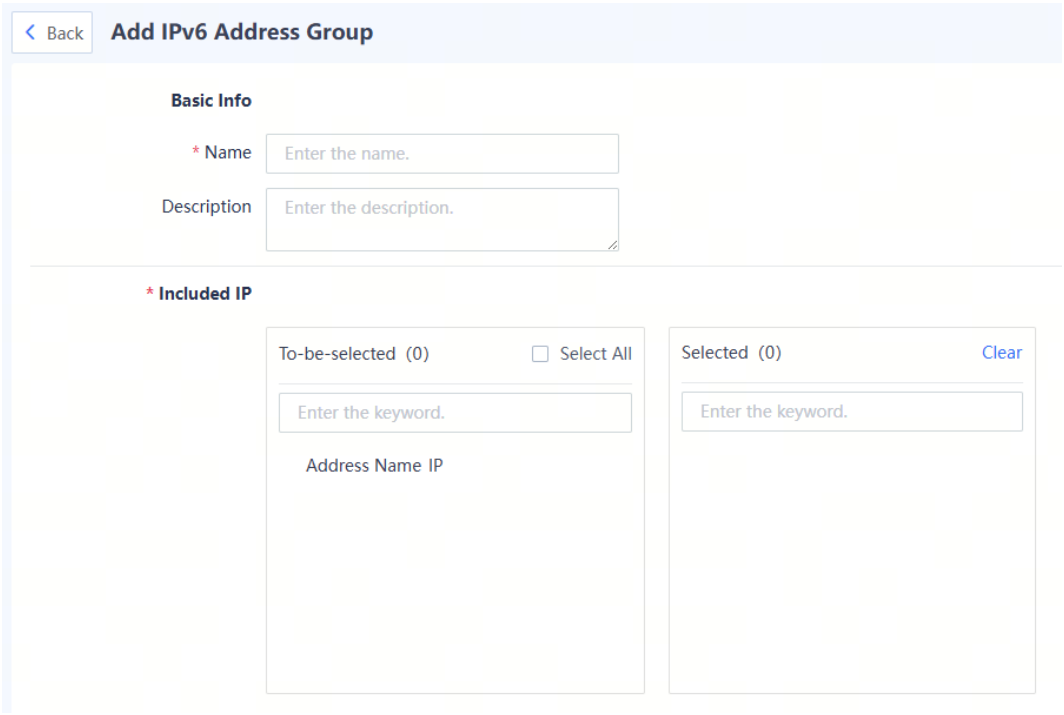
Procedure

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

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



b Click **Create**.



(2) Set parameters for the address group object.

Item	Description	Remarks
Name	Name of the address group object.	[Example] Addr_total
Description	Description of the address group object.	[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.

5.1.6 Creating a MAC Address Object

Application Scenario

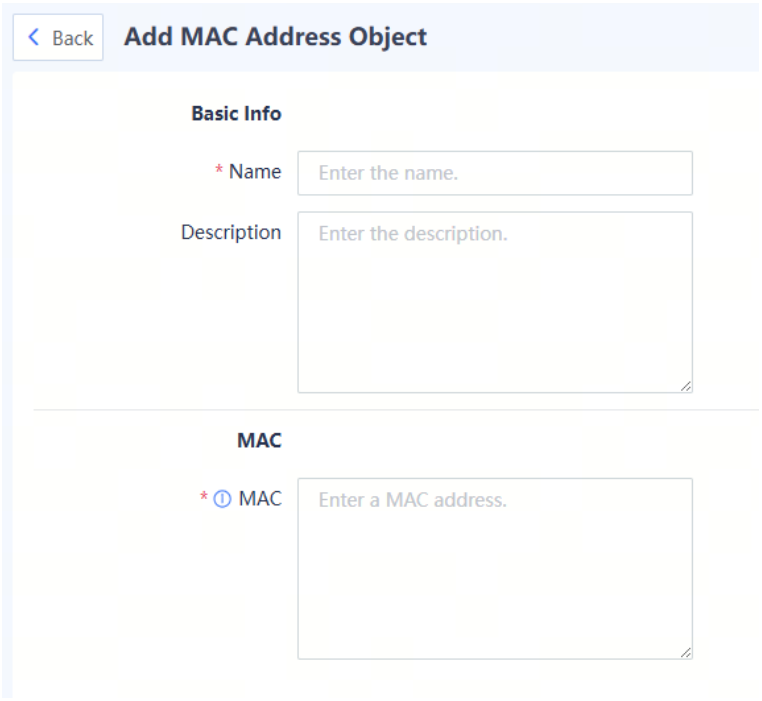
Create a MAC address object on the web UI.

Procedure

(1) Access the **Add MAC Address Object** page.

a Choose **Object** > **Address** > **MAC Address**.

b Click **Create**.



(2) Set parameters for the address object.

Item	Description	Remarks
Name	Name of the MAC address object.	[Example] MAC_Addr1
Description	Description of the MAC address object.	[Example] For office area 1
MAC address	One or more MAC addresses.	Configure one or more MAC addresses. Enter one MAC address per line. Press **Enter** to separate lines. Example: 1a:2b:3c:4d:5e:6f

(3) Click **Save**.

Follow-up Procedure

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

5.1.7 Creating a MAC Address Group Object

Application Scenario

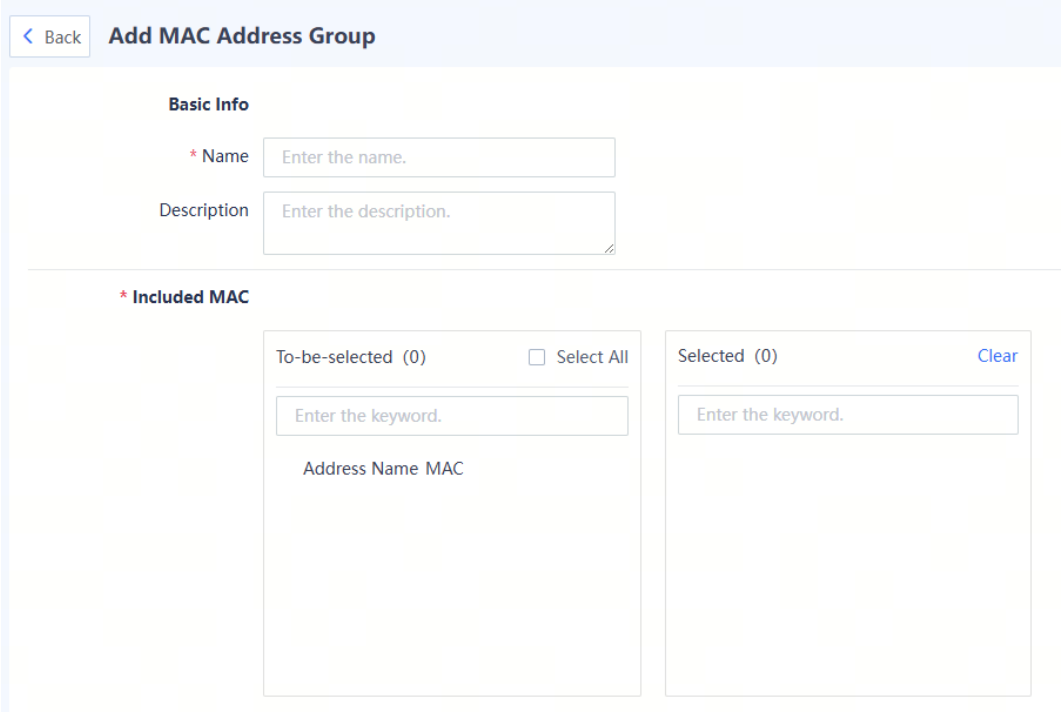
Create a MAC address group object on the web UI.

Procedure

(1) Access the Add MAC Address Group page.

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

b Click **Create**.



(2) Set parameters for the address group object.

Item	Description	Remarks
Name	Name of the address group object.	[Example] Addr_total
Description	Description of the address group object.	-
Included MAC	Address objects contained 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.

(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.

5.1.8 Creating a Domain Name Object

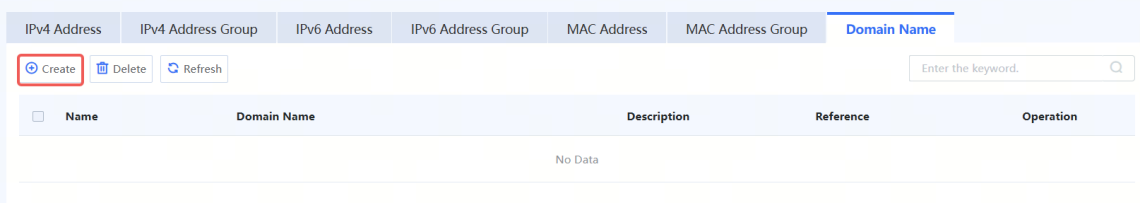
Application Scenario

On the web UI, create a domain name object.

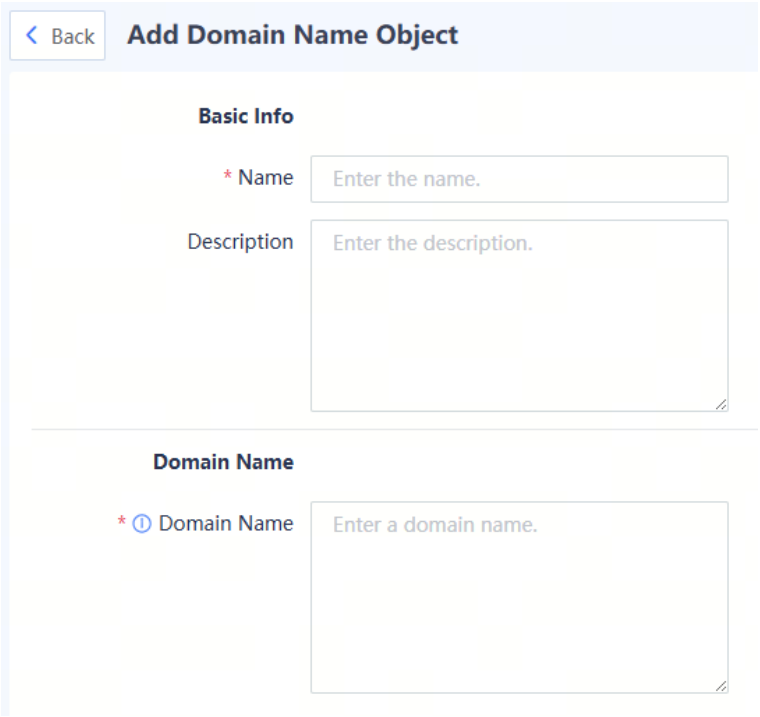
Procedure

(1) Access the **Add Domain Name Object** page.

a Choose **Object** > **Address** > **Domain Name**.



b Click **Create**.



(2) Set parameters for a domain name object.

Item	Description	Remarks
Name	Name of a domain name object.	[Example] Domain_test
Description	Description of a domain name object.	-

Item	Description	Remarks
Domain Name	Domain names contained in a domain name object. The following two domain name formats are supported: ● Exact domain name: Enter complete domain names. Exact match is applied to match only the domain names that are exactly the same as the specified strings. ● Wildcard domain name: Enter the wildcard (*) in a domain name to indicate any subdomain name. Suffix match is applied to match all domain names with the specified strings (primary domain names) as suffixes.	● Enter one domain name per line. Press **Enter** to separate lines. ● Wildcard domain names are supported: Configure a domain name starting with the wildcard (*) to match all subdomain names with the specified strings as suffixes. The wildcard (*) must be added to the beginning of a domain name, and must be followed by a dot ("."). [Example] www.test.com.cn *.test.com.cn *.test.abc.com

(3) Click **Save**.

Follow-up Procedure

- Click **Edit** to modify the description and domain names of a domain name object.
- Click **Delete** to delete a domain name object that is not referenced.

5.2 Application

5.2.1 Overview

To identify different applications that use the same protocol and port number, the concept of applications is introduced on the CF 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.
- If the application identification function is not authorized or the license expires, the function can be used normally, but the signature library cannot be upgraded.

5.2.2 Viewing Application Information in a Signature Library

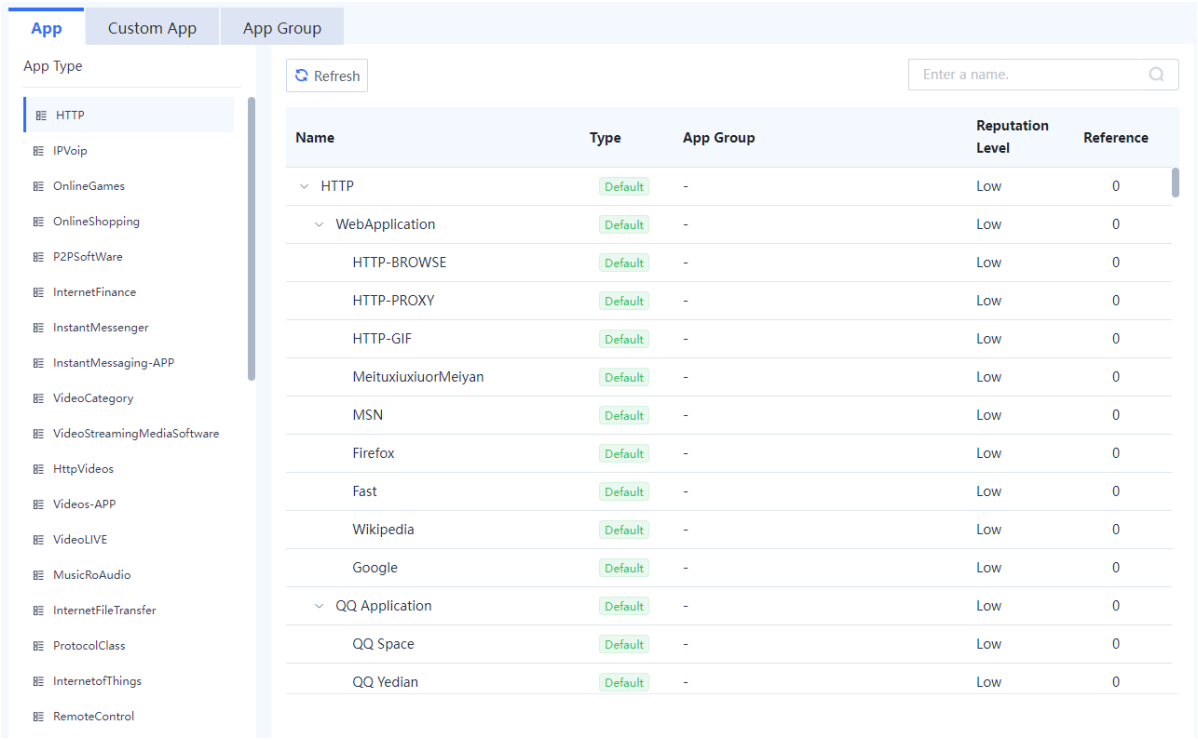
Application Scenario

View application information defined by the system.

Procedure

(1) Choose **Object** > **App** > **App**.

(2) View application details.



The following table describes application details.

Item	Description
Type	Application type, which can be custom or default (predefined).
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 8.3.2 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 7.5 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.
- If you have any question about predefined application types, you can provide feedback through the URL feedback channel. For details, see 5.3.2 5. Feedback Channel for URL/Application Identification Signature Library Errors.

5.2.3 Creating a Custom Application

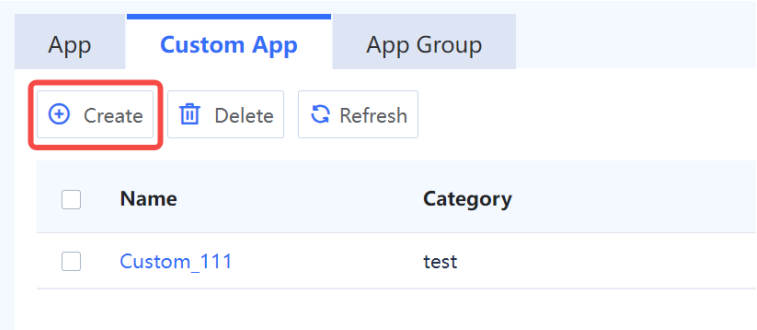
Application Scenario

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

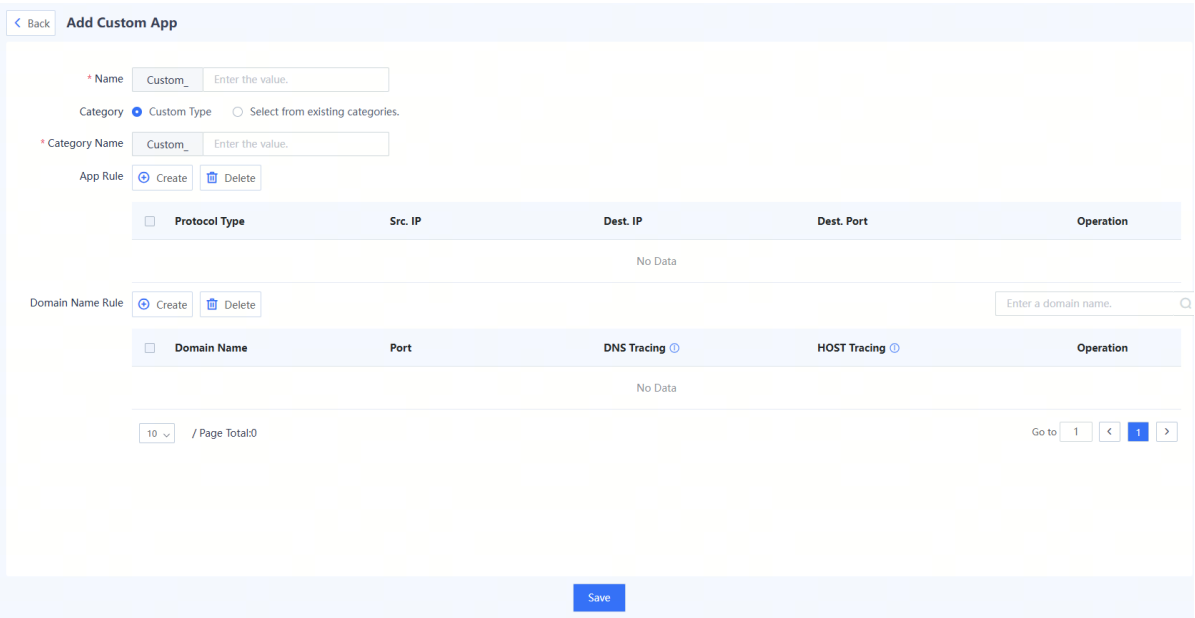
Procedure

(1) Choose **Object** > **App** > **Custom App**.

(2) Click **Create**.



(3) Configure the parameters for the custom application.



Item	Description	Remarks
Name	Name of the custom application. The naming format is **Custom**_*Name*.	● 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. [Example] Custom_app_1
Category	Customize the application category. You can customize a category or select an existing category.	-
App Rule	Configure the IP 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 IP matching rules for application traffic.
Domain Name Rule	Configure a domain name rule for the custom application. Traffic matching the rule is deemed as the traffic of this application. The device supports DNS tracing and host tracing for identifying applications. ● **DNS Tracing**: Trace DNS packets to associate domain names with IP addresses and identify destination domain names based on destination IP addresses to identify applications. ● **HOST Tracing**: Identify only HTTP/HTTPS packets. Match the Host field in HTTP/HTTPS packets with domain names to identify applications. ● If both DNS tracing and host tracing are enabled, DNS tracing has a higher priority. If an application is successfully identified through DNS tracing, host tracing is not performed.	In the **Domain Name Rule** area, click **Create** and configure a domain name rule for matching traffic of this application.

(4) Click **Save**.

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.

5.2.4 Creating a Custom Application Group

Application Scenario

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

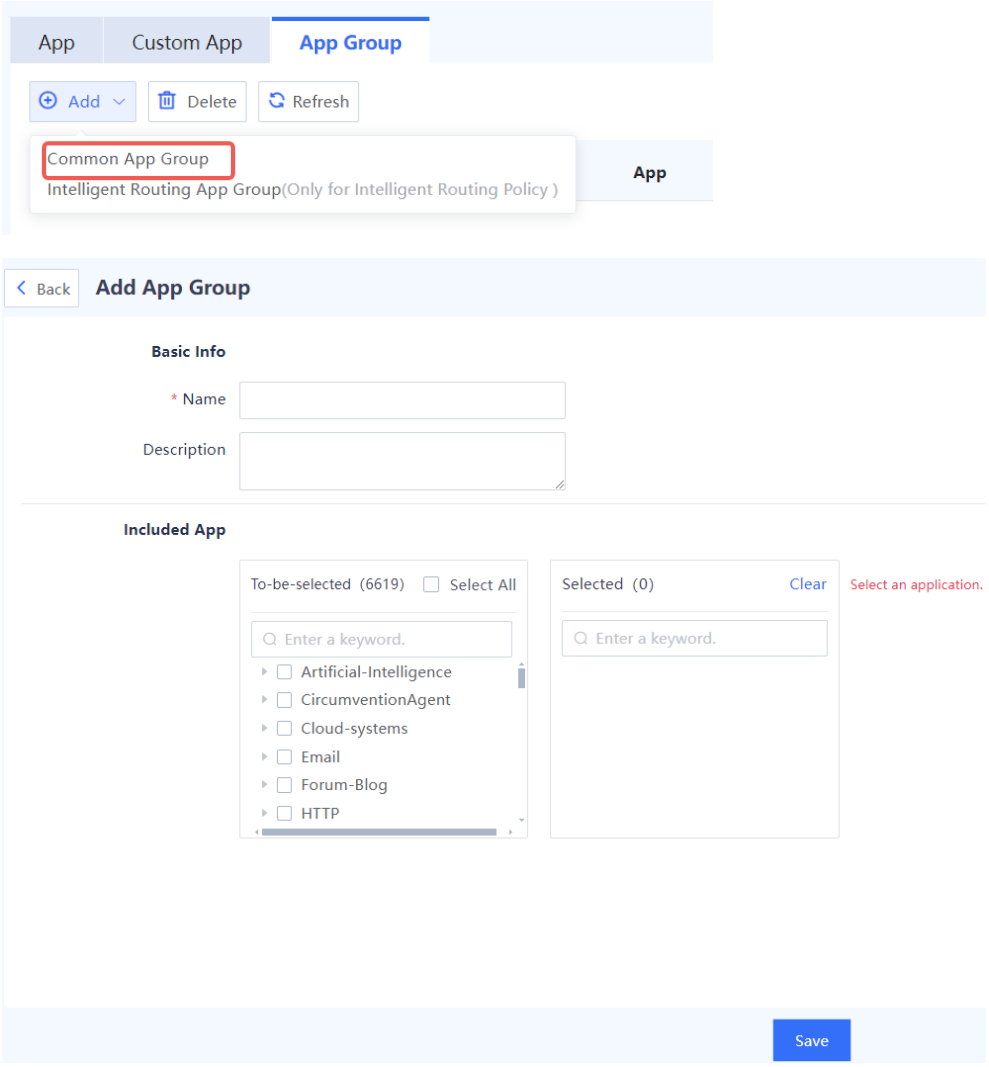
The device supports common application groups and intelligent routing application groups. The intelligent routing application groups are available only when they are invoked by intelligent routing policies.

Procedure

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

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

b Click **Add**. The following uses common application group as an example.



(2) Set parameters for the application group.

Item	Description	Remarks
Name	Name of the custom application group.	● 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.	[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
Name	Application group name.
Type	Common application group or intelligent routing application group.
App	Applications in the application group.
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.

5.2.5 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 7.5 Signature Library Upgrade.

5.3 Content Identification Library

5.3.1 Configuring a Keyword Set

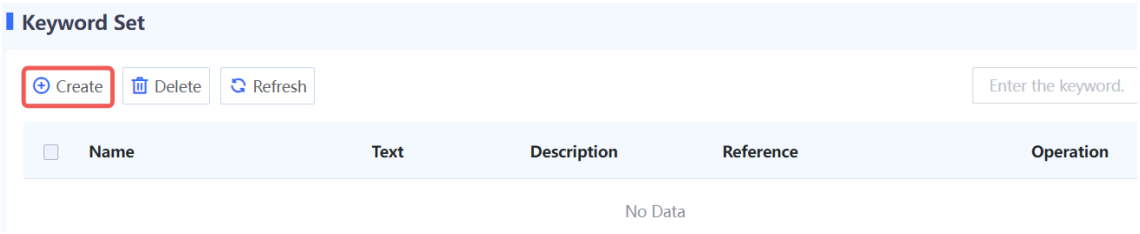
Application Scenario

Configure a keyword set to specify the keyword text for filtering. The keyword set can be used together with a keyword filtering template to block or generate an alarm for traffic containing keywords. For details about the keyword filtering template, see 5.10.5 Keyword Filtering.

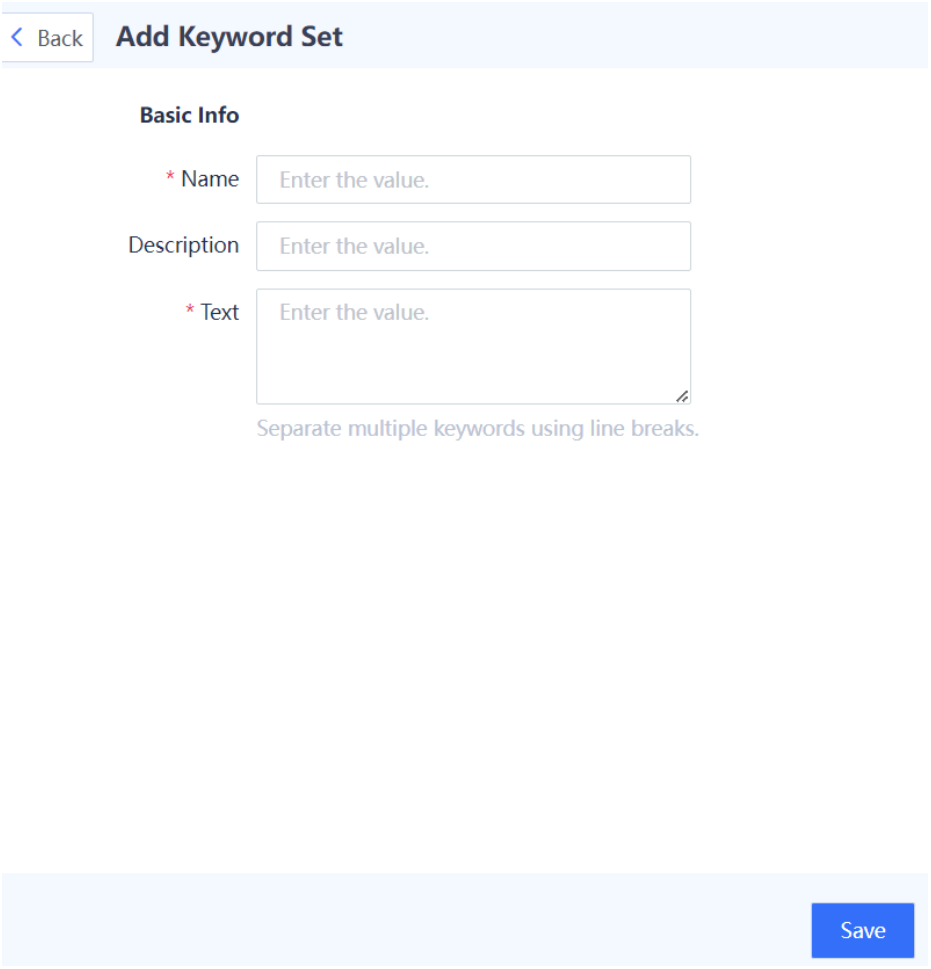
Procedure

(1) Choose **Object** > **Content Identification Lib.** > **Keyword Set**.

(2) Click **Create**.



(3) Configure a keyword set.



Item	Description	Remarks
Basic Info		

Item	Description	Remarks
Name	Name of the keyword set.	[Example] key_group
Description	Description of the keyword set.	N/A
Text	Keyword text for filtering the traffic that contains keywords.	Separate multiple keywords by line breaks. The text length per line ranges from 3 bytes to 31 bytes, and the text cannot be all spaces or contain a backslash (\). [Example] abc1 abc2

(4) Click **Save**.

Follow-up Procedure

- Click **Create** to add more keyword sets.
- Click **Delete** to delete a specified keyword set. If a keyword set is referenced by a filtering template, you need to delete the reference to the keyword set before deleting the keyword set.
- Click **Refresh** to obtain the latest keyword set configuration.

5.3.2 URL Category

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 5.10.3 URL Filtering.

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 7.2.4 Activating the License.

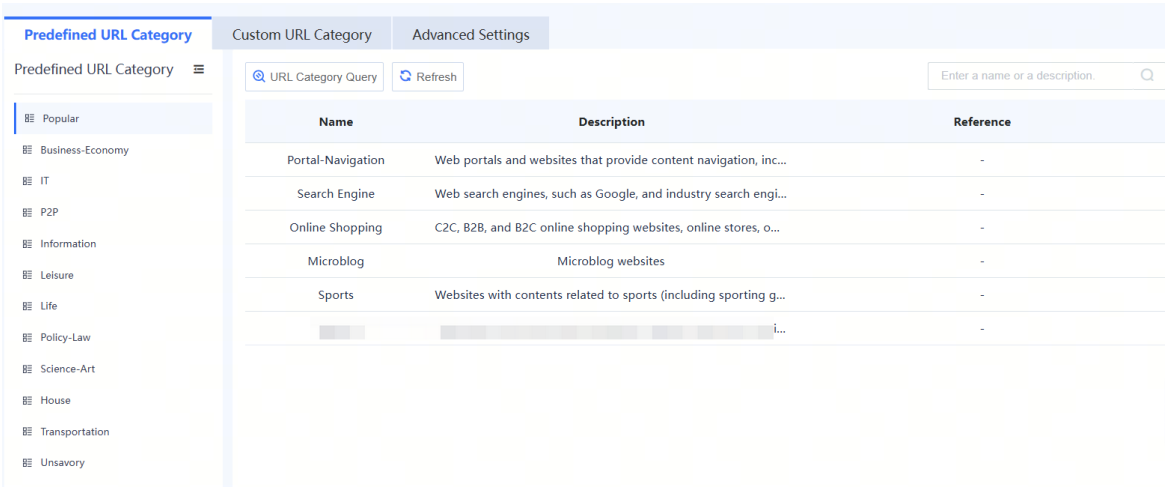
Note

- If the URL category function is not authorized, predefined URL categories are unavailable for URL filtering, and custom URL categories are available for URL filtering.
- If the license of the URL category function expires, the function is available based on existing URL signature libraries, but the URL signature libraries cannot be upgraded.

Procedure

(1) Choose **Object** > **Content Identification Lib.** > **URL Category** > **Predefined URL Category**.

(2) View details about predefined URL categories.



3. Configuring a Custom URL Category

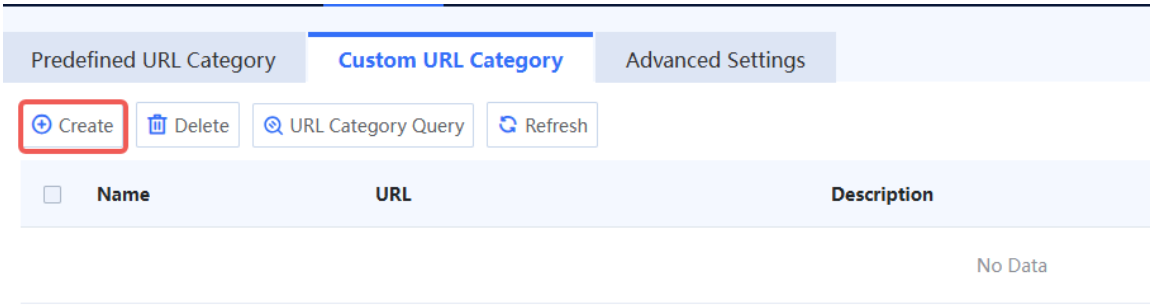
Application Scenario

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.

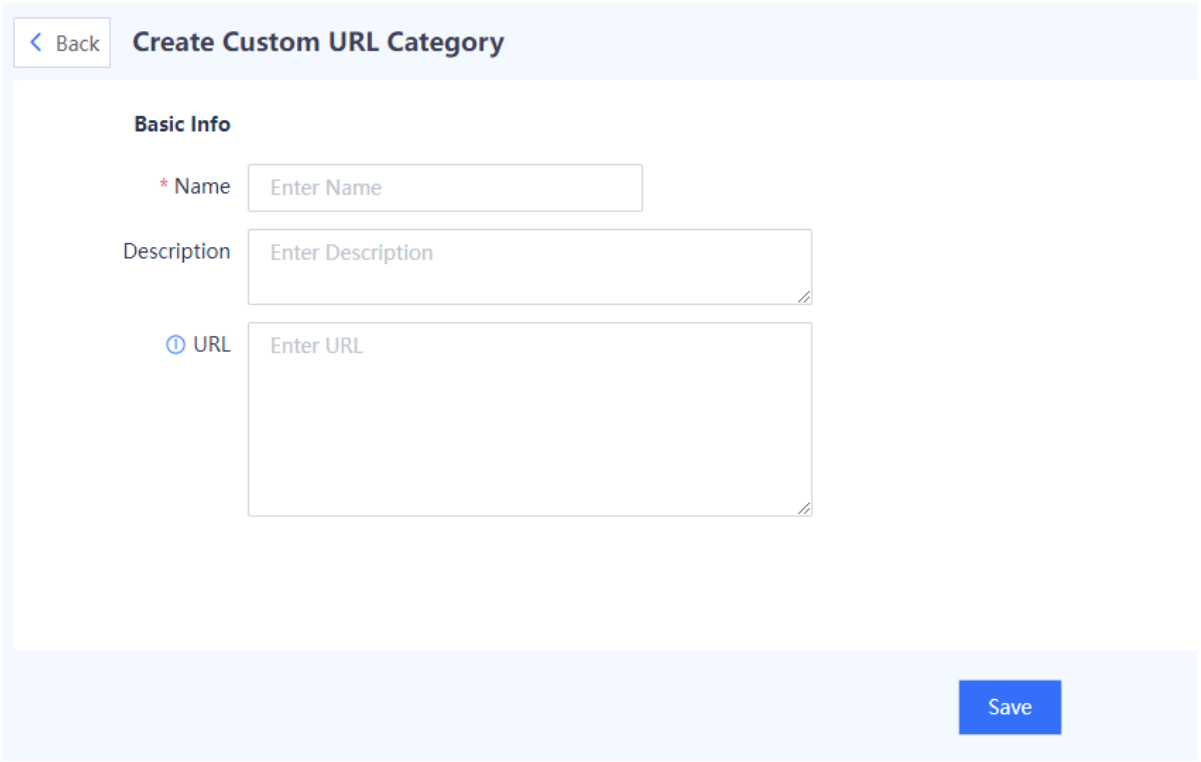
Procedure

(1) Choose **Object** > **Content Identification Lib.** > **URL Category** > **Custom URL Category**.

(2) Click **Create**.



(3) Enter URL category information.

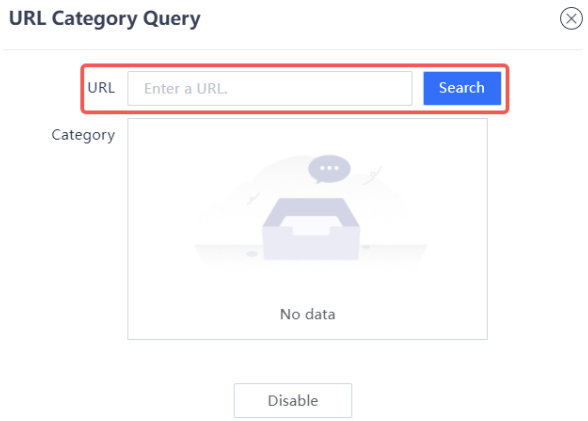


Item	Description	Remarks
Basic Info		
Name	URL category name.	[Example] category_1
Description	Description of the URL category.	N/A
Indicates the URL.	URLs in this category. A URL can contain the wildcard character (*). Enter one URL per line. Press **Enter** to separate lines. Note: ● If a URL contains the pound sign (#), the sign and the string after the sign do not take effect for matching. For example, if **www.test.com/#123** is configured, all the domain names that start with **www.test.com/** will be matched. ● If a URL contains the characters **http://** or **https://,** these characters will be automatically removed during matching. ● If an IPv6 address is configured as a URL, the input format should be [*IPv6 address*]. For example, **[2001::1].**	[Example] www.abc1.com www.abc2.com

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

Follow-up Procedure

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



4. Enabling Cloud-based Analysis

Application Scenario

The capacity of the local URL signature library is limited. With the cloud-based analysis function enabled, the device sends the URLs accessed by users not in the local library to the cloud for analysis to achieve comprehensive URL filtering.

Precautions

- The cloud-based analysis results are locally cached so that subsequent queries for the same URLs directly hit the cache. The cache aging time is 6 hours and the cache is not updated when a URL is accessed again. That is, if a user accesses the same URL repeatedly within 6 hours, the cache retention time is not extended.

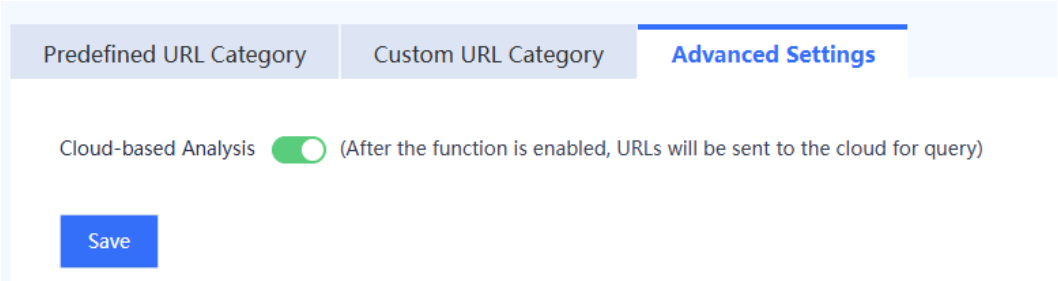
Prerequisites

- The local URL signature library of the device has been upgraded to the version with the prefix **url_db_i_2_**.
- The device is connected to the Internet.

Procedure

(1) Choose Object > Content Identification Lib. > URL Category > Advanced Settings.

(2) Toggle on to enable cloud-based analysis.



(3) Click **Save**.

5. Feedback Channel for URL/Application Identification Signature Library Errors

Application Scenario

The device provides a feedback channel for predefined URL signature library and application identification signature library errors. After feedback or adjustment requests from users are collected, filtering and

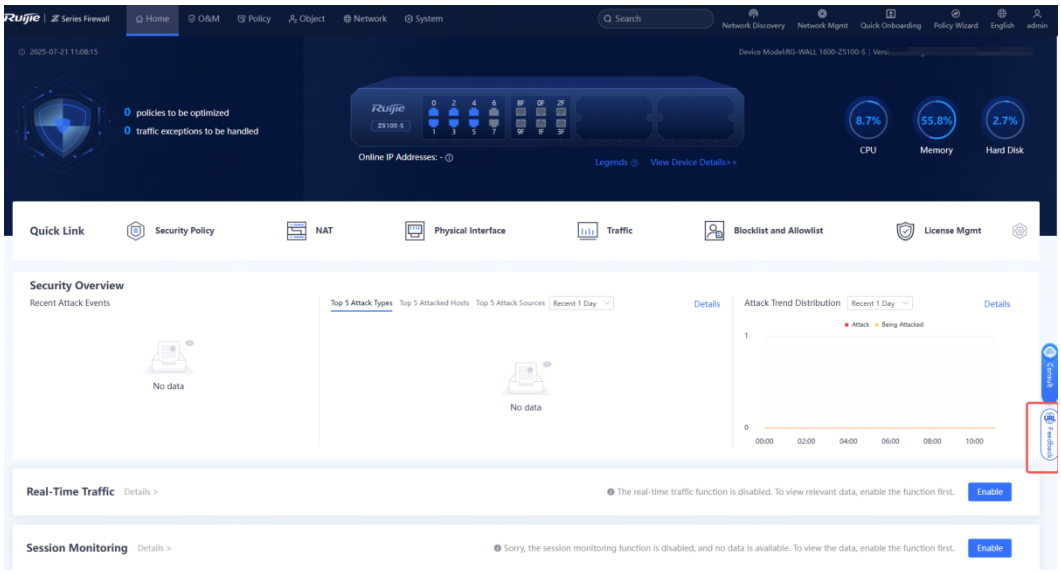
classification rules can be optimized. This improves filtering accuracy and flexibility, and ensures that network access control policies are more aligned with the security and management needs of users or organizations.

Procedure

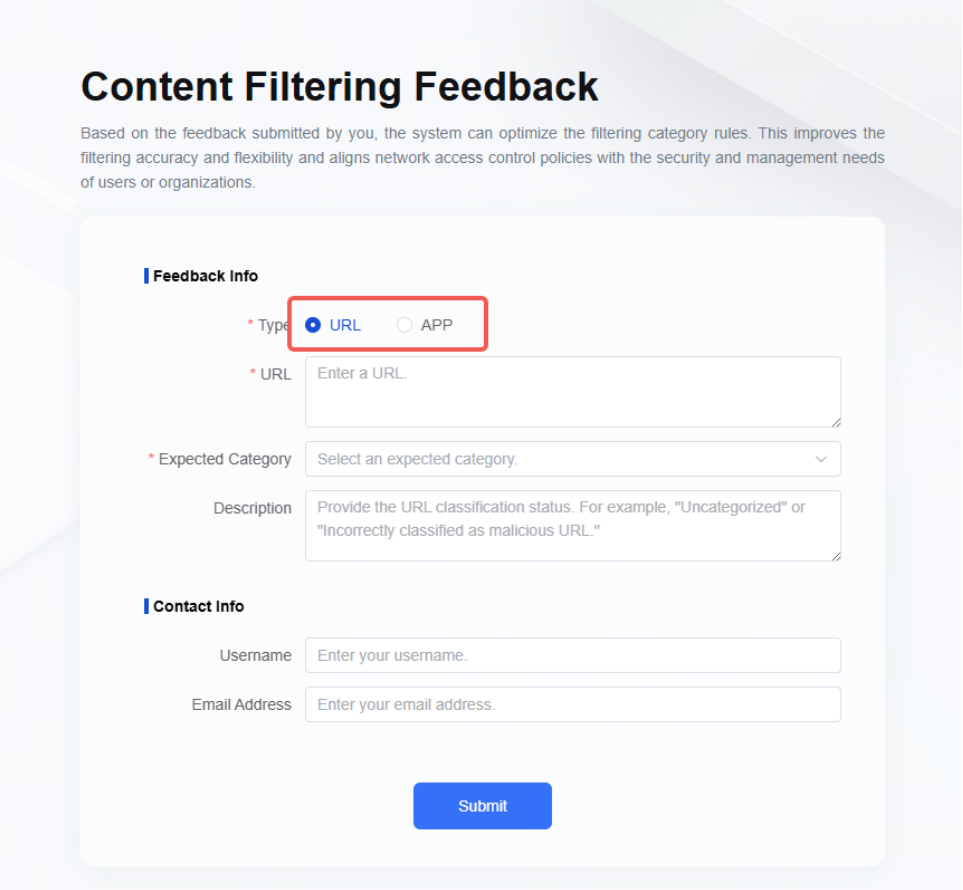
(1) Click **URL Feedback** on the right to go to the **Content Filtering Feedback** page.

Note

URL Feedback is a persistent feedback channel. You can click it on any page of the device web UI to submit feedback. If you click **X** to hide the feedback channel, you can refresh the page to restore it.



(2) Enter feedback information for URLs or applications. After completing the required information, click **Submit**.



(3) After the feedback is submitted, it will be reviewed by the administrator of Ruijie Security Cloud Platform. Once approved, the corresponding signature library will be updated. After the signature library is upgraded to the corresponding latest version on the device, the latest signature library can be verified and used.

5.3.3 File Type Group

1. Overview

A file type group is used to specify the file types to be filtered during content filtering. With file filter templates, file type group configuration can block or generate alarms on the transmission of files of specific types to prevent such files from entering the internal network or internal confidential information from being leaked to external networks. For details about file filtering templates, see 5.10.6 File Filtering.

2. Viewing Predefined File Type Groups

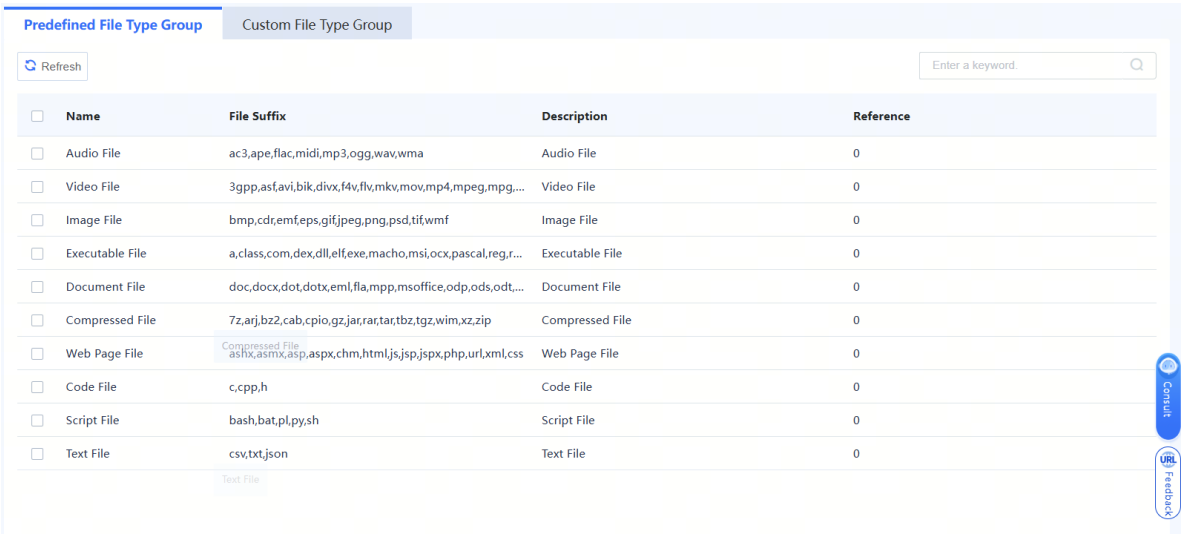
Application Scenario

The device classifies common file extensions by file type and predefines multiple file type groups. When configuring a file filter template, you can reference a predefined file type group to set the file types to be filtered. Predefined file type groups cannot be modified or deleted.

Procedure

(1) Choose **Object** > **Content Identification Lib.** > **File Type Group** > **Predefined File Type Group**.

(2) Check the details on predefined file type groups.



3. Configuring a Custom File Type Group

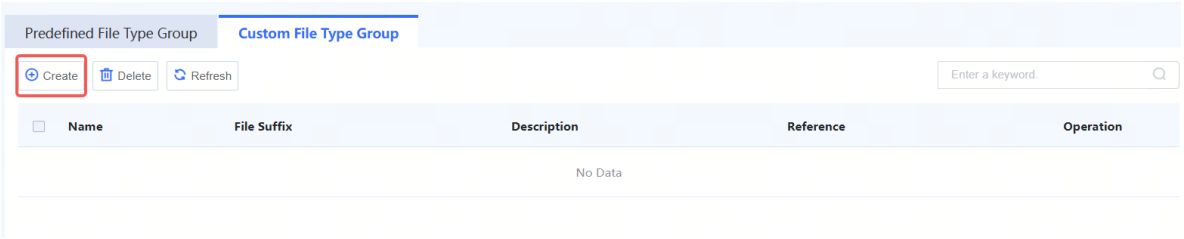
Application Scenario

The device provides common file type information. You can also customize file type groups as required to restrict file types that pose risks or need to be prohibited from transmission.

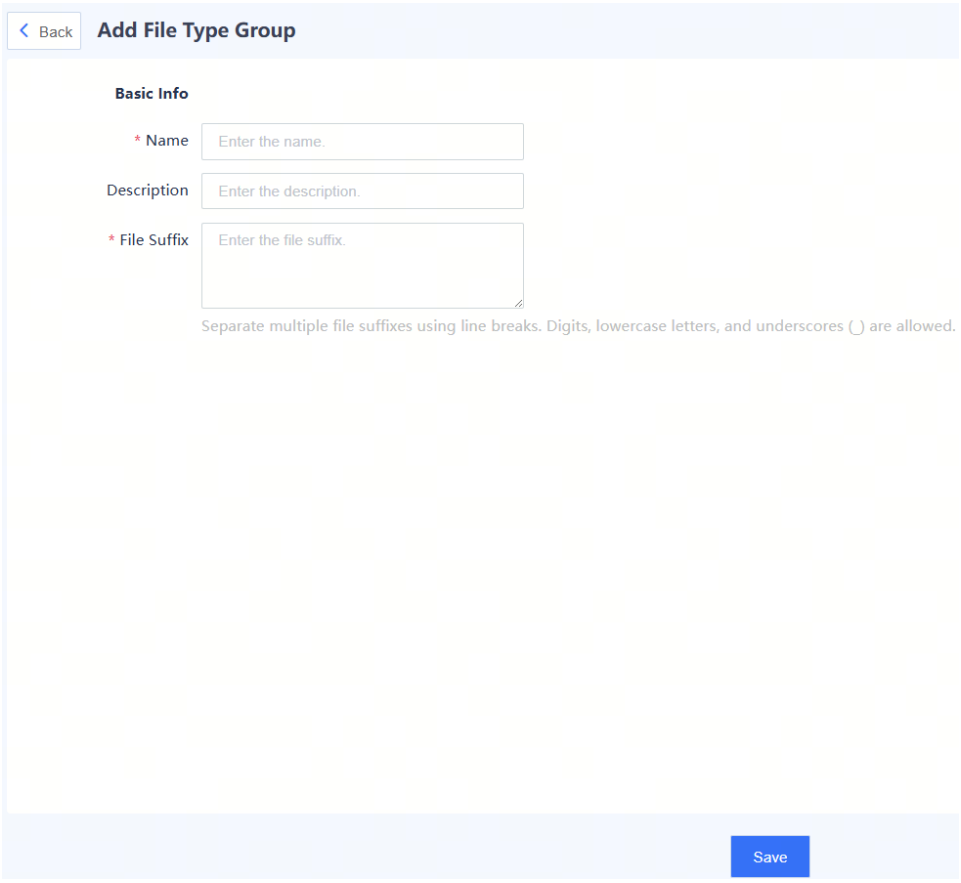
Procedure

(1) Choose **Object** > **Content Identification Lib.** > **File Type Group** > **Custom File Type Group**.

(2) Click **Create**.



(3) Set parameters for the file type group.



Item	Description	Remarks
Basic Info		
Name	Name of a file type group.	[Example] Test file
Description	Description of a file type group.	-
File Suffix	File suffixes (or file extensions) contained in the file type group. You can enter multiple file suffixes, and digits, lowercase letters, and underscores (_) are supported. Press **Enter** to separate multiple file suffixes.	[Example] .sys .drv

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

Follow-up Procedure

- To batch delete custom file type groups, select them and click **Delete**. If a custom file type group is being used in a file filter template (that is, the reference count is not 0), the file type group cannot be deleted. To delete it, modify the file filter template to dereference the file type group first.
- Enter keywords in the name, description, or file suffixes of a file type group in the search box to query information about the file type group.

5.4 Services

5.4.1 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 CF 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

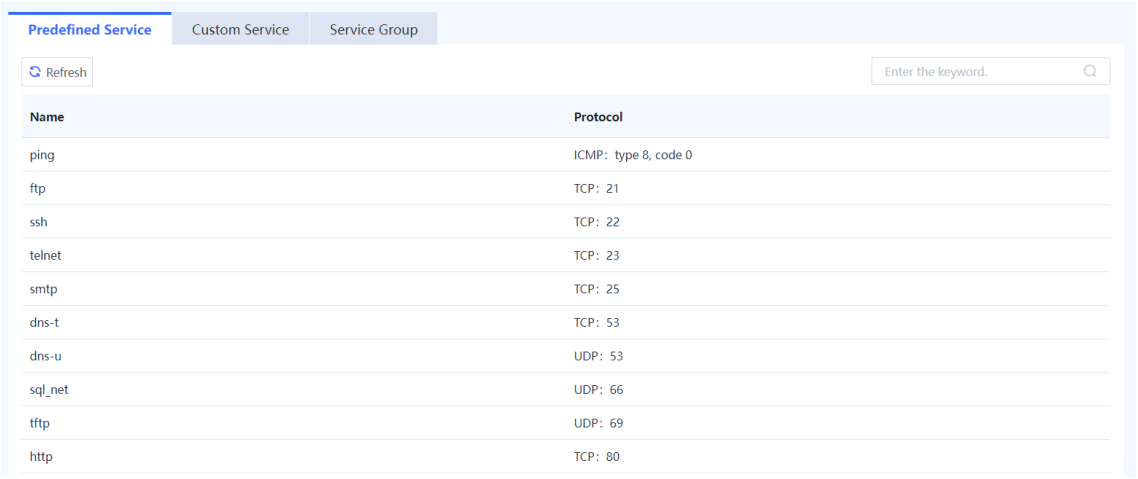
  The application protocol is defined by protocol type (for example, TCP, UDP, or ICMP), port number, or other information.

  - 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.

5.4.2 Predefined Service

(1) Choose **Object** > **Service** > **Predefined Service**.

On the **Predefined Service** tab page, check predefined services.



Item	Description	Remarks
Name	Service name.	N/A
Protocol	Protocol type.	N/A

5.4.3 Configuring a Custom Service

Application Scenario

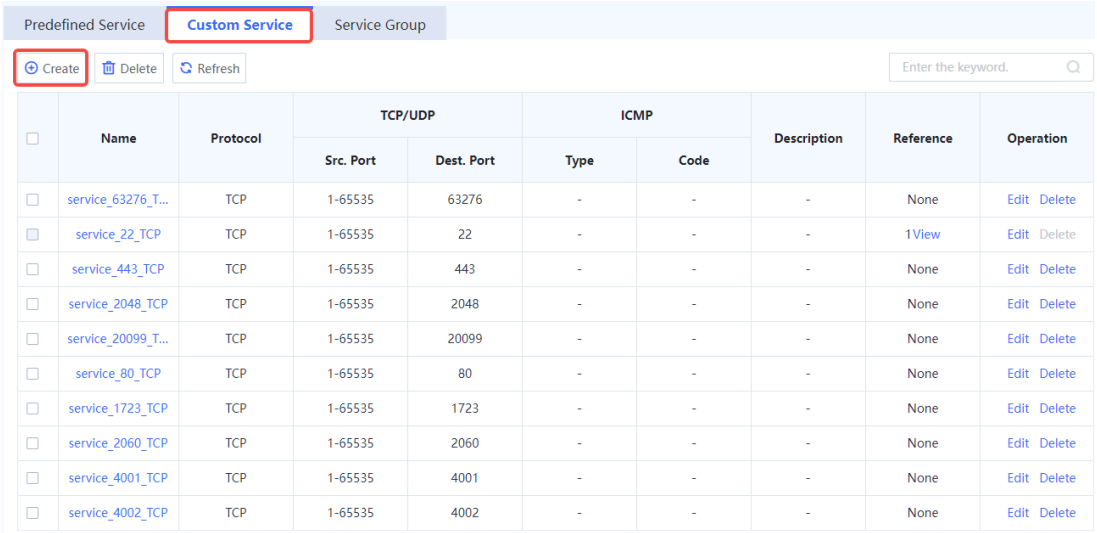
Define the application protocol by protocol type (for example, TCP, UDP, or ICMP), port number, or other information.

Procedure

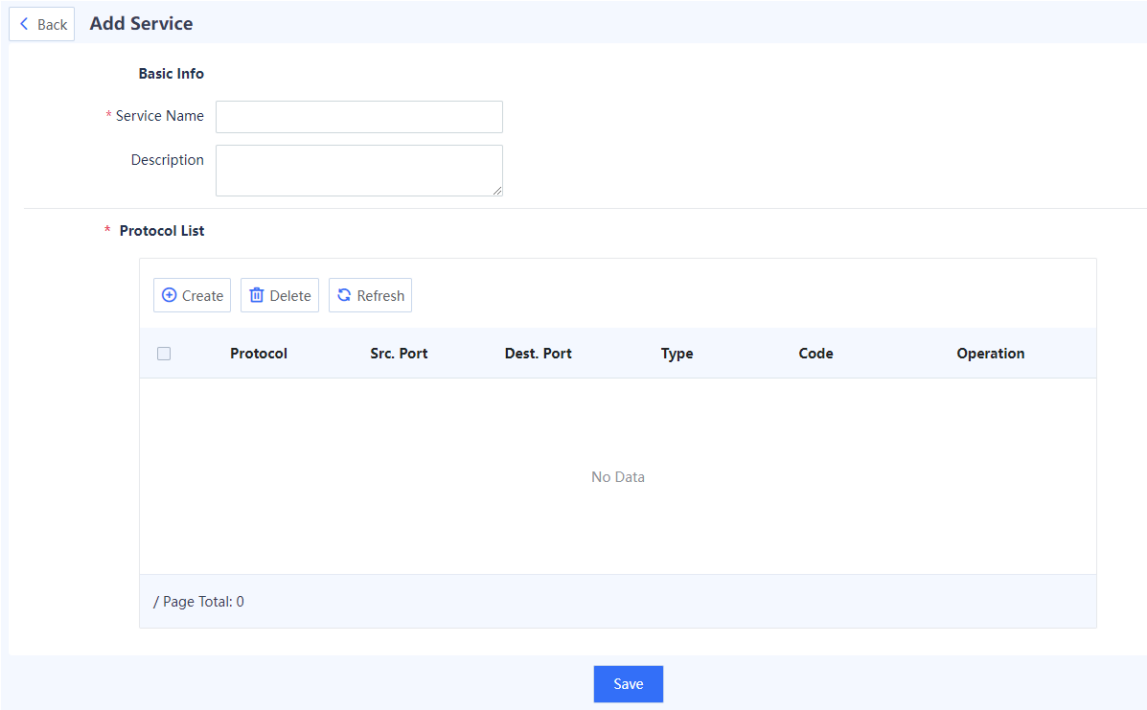
(1) Access the **Add Service** page.

a Choose **Object** > **Service** > **Custom Service**.

b Click **Create**.



(2) Set parameters for the service.



Item	Description	Remarks
Basic Info		
Service Name	Name of the new service.	● 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.	[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: ● Protocol Number ● Src. Port ● Dest. Port
UDP	Services that use the UDP protocol.	The parameters are as follows: ● Protocol Number ● Src. Port ● Dest. Port

Item	Description	Remarks
ICMP	Services that use the ICMP protocol.	The parameters are as follows: ● Protocol Number ● Type ● Code
ICMPv6	Services that use the ICMPv6 protocol.	The parameters are as follows: ● 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.

5.4.4 Creating a Service Group

Application Scenario

You can create a service group to manage multiple services.

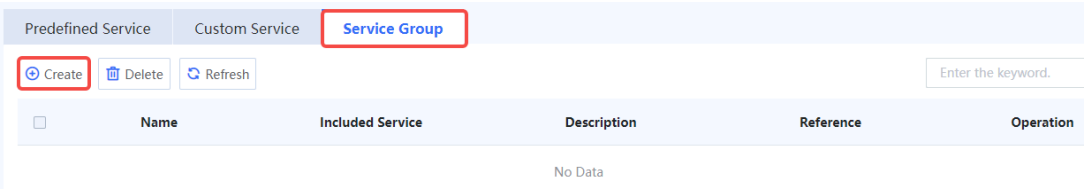
Both custom and predefined services can be added to service groups.

Procedure

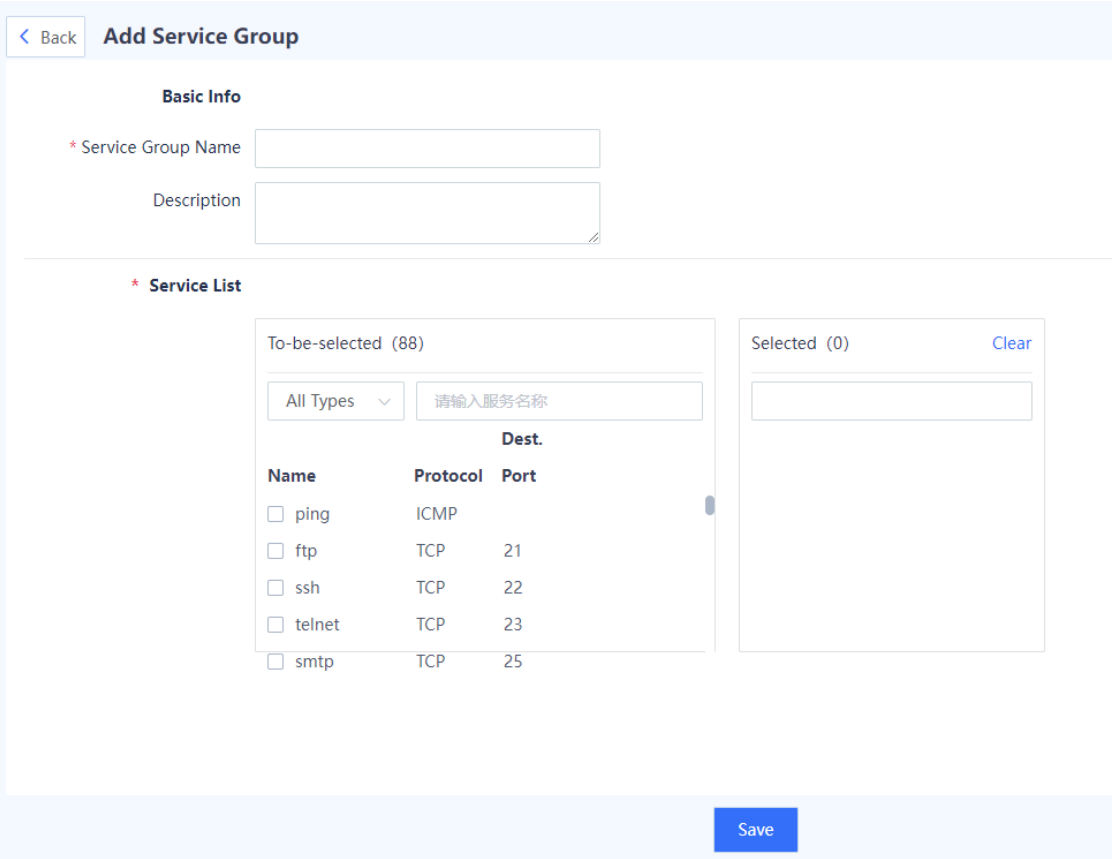
(1) Access the **Add Service Group** page.

a Choose **Object** > **Service** > **Service Group**.

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



(2) Set parameters for the service group.



Item	Description	Remarks
Basic Info		
Service Group Name	Name of the new service group.	The name of an existing service group cannot be used. [Example] Service_group_1
Description	Description of the new service group.	[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.

5.5 Region

5.5.1 Overview

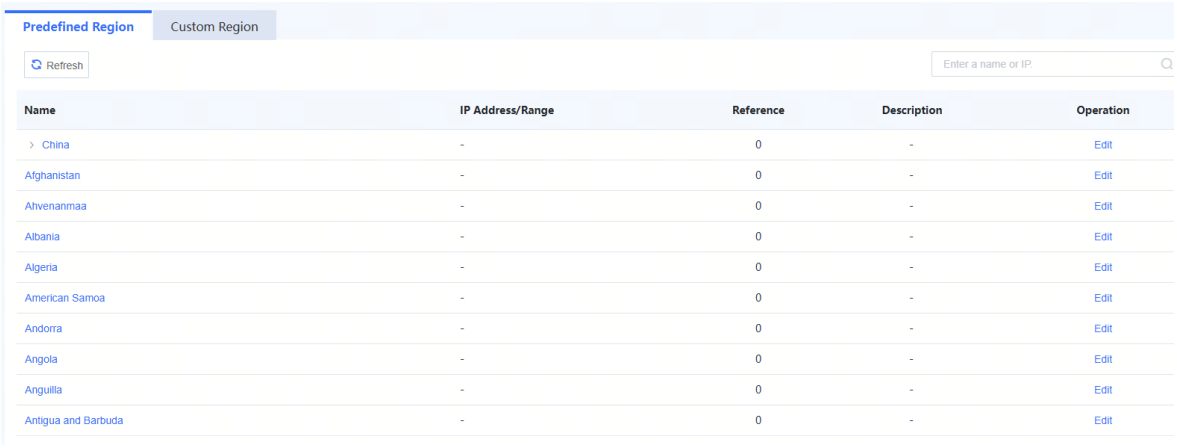
The device supports two types of region objects: predefined region objects and custom region objects. Predefined region objects are available for selection on the system by default and cannot be deleted. If the regional scope required by the actual network differs from the predefined region objects on the device, you can create a custom region object.

You can then reference custom or predefined region objects in a security policy to control data packets of these region objects.

5.5.2 Predefined Region

(1) Choose **Object** > **Region** > **Predefined Region**.

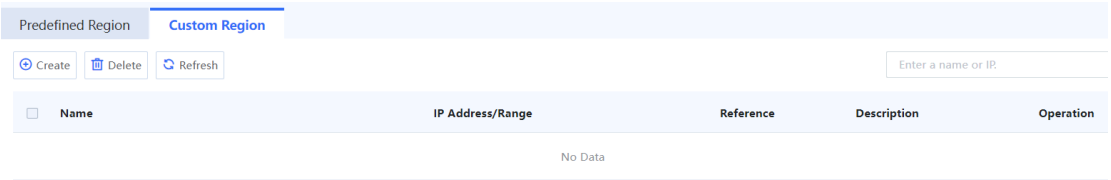
On the **Predefined Region** tab page, check predefined region objects.



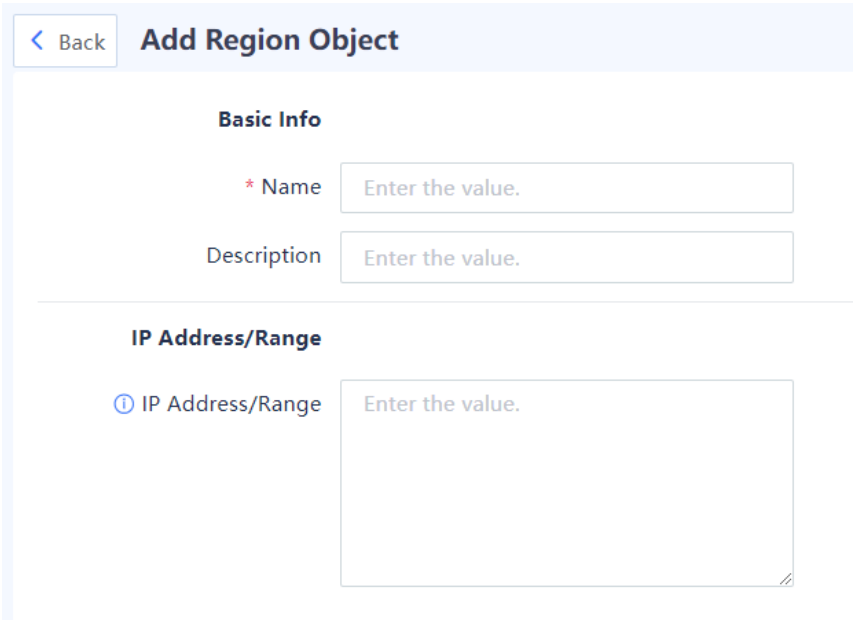
5.5.3 Custom Region

(1) Choose **Object** > **Region** > **Custom Region**.

(2) Click **Create**.



(3) Set parameters for the custom region object.



Item	Description	Remarks
Basic Info		
Name	Name of the new region object.	● The name of the new region object cannot be the same as that of an existing region object. ● After a region object is created, its name cannot be modified. [Example] Region 1
Description	Description of the new region object for distinguishing different regions.	[Example] New region
IP Address/Range		
IP Address/Range	IP address or range of the new region object. An IP address can only belong to one region.	Enter one IP address per line. Press **Enter** to separate lines. [Example] ● IP address: 192.168.1.1 ● IP range: 192.168.1.1-192.168.1.10 ● Subnet: 192.168.1.0/24 or 192.168.1.0/255.255.255.0

(4) Click **Save**.

Follow-up Procedure

- You can only delete the region objects with no reference.
- You cannot add or delete predefined region objects. Predefined region objects are region object types that are commonly used.

5.5.4 Upgrading a Regional Signature Library

The regional signature library is continuously updated. By upgrading the regional signature library, the device can obtain the latest region information. For details about regional signature library upgrade, see 7.5 Signature Library Upgrade.

5.6 Time Plan

5.6.1 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 external network 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 external network only from 19:00:00 to 22:00:00 every Friday night.

5.6.2 Creating a Cyclic Time Plan

Application Scenario

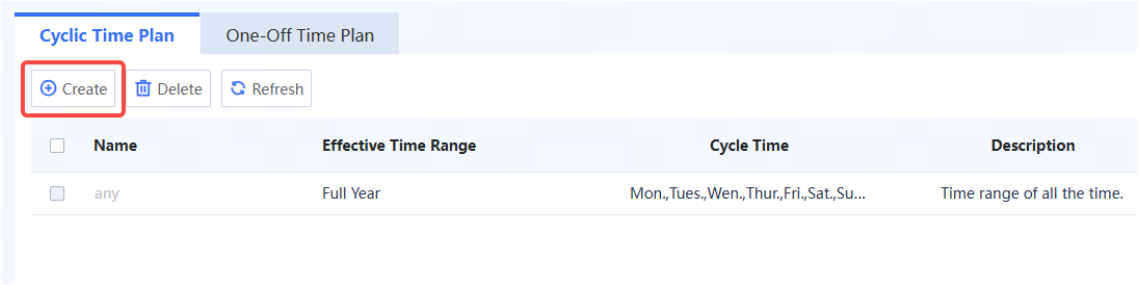
Configure a cyclic time plan to make policies take effect within the specified time range.

Procedure

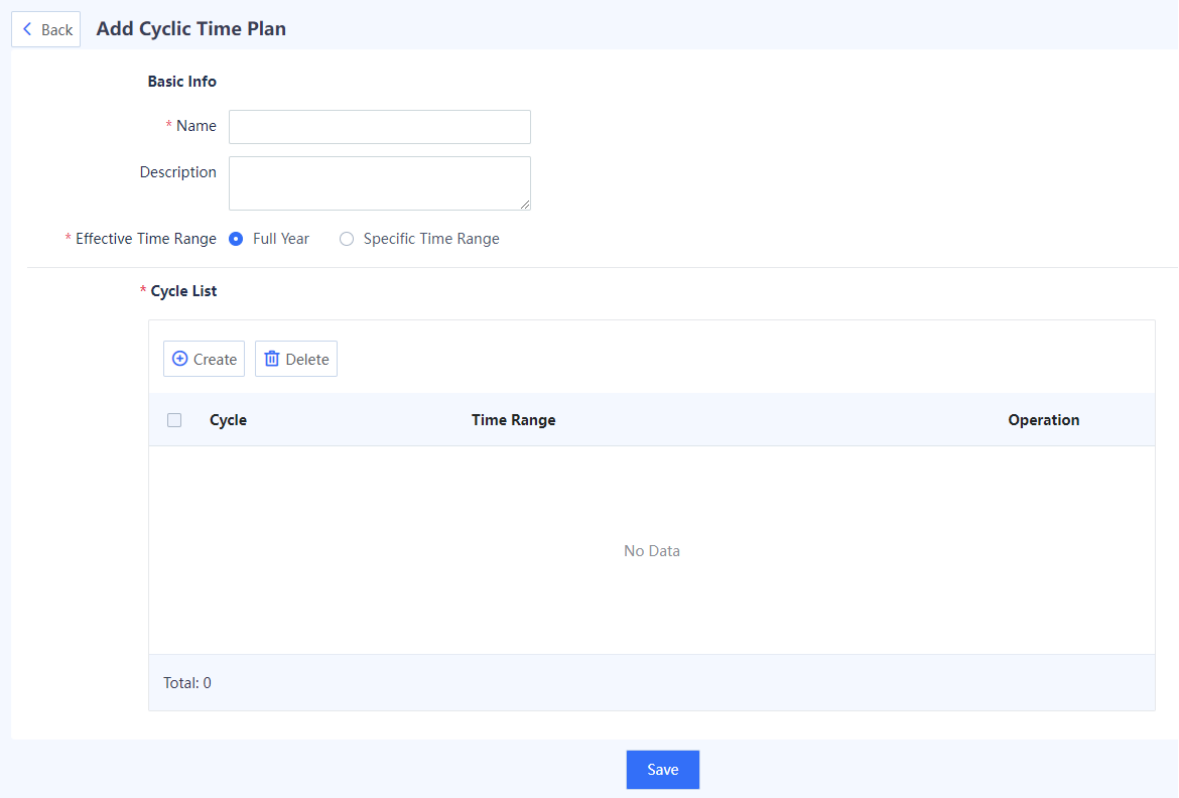
(1) Access the **Add Cyclic Time** Plan page.

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.	[Example] Plan 1
Description	Description of the new cyclic time plan.	[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.

5.6.3 Creating a One-Off Time Plan

Application Scenario

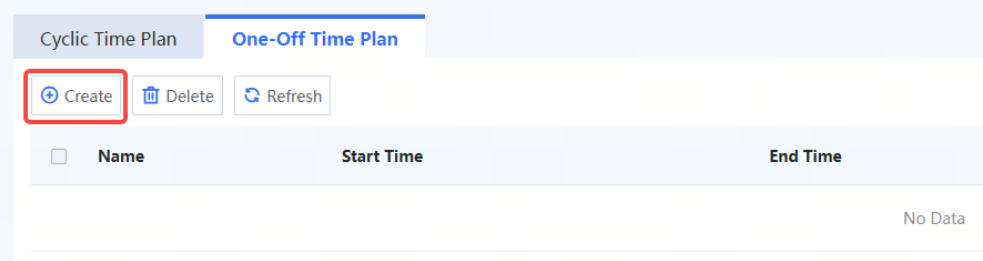
Configure a one-off time plan to execute policies only once.

Procedure

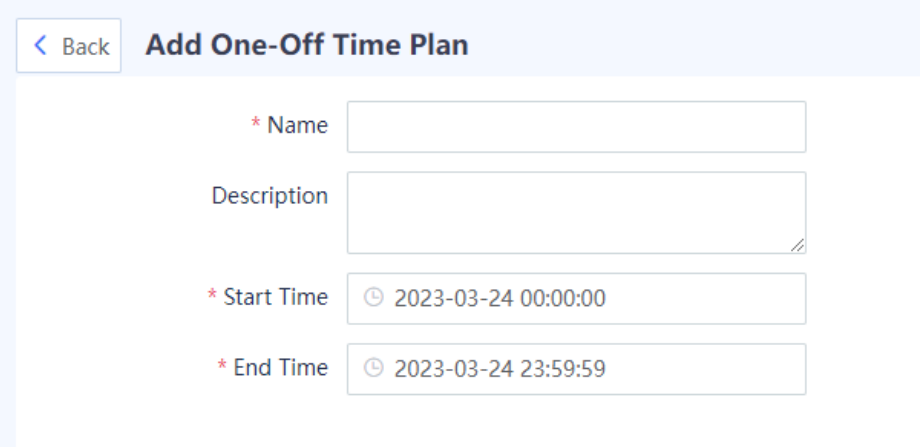
(1) Access the **Add One-Off Time Plan** page.

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.



Item	Description	Remarks
Name	Name of the new one-off time plan.	[Example] Plan 1
Description	Description of the new one-off time plan.	-
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.

5.7 ISP Address Library

5.7.1 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.

5.7.2 Creating an ISP Address Library Manually

Application Scenario

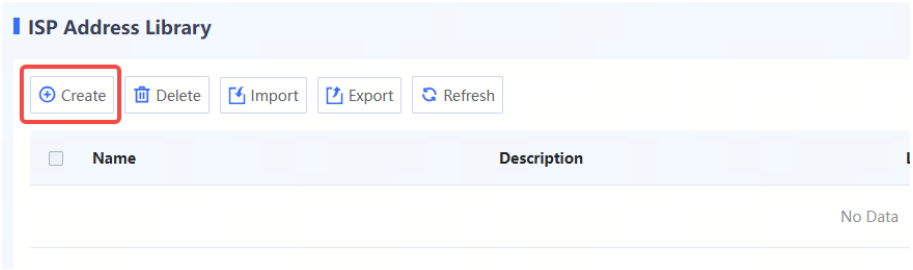
You can add addresses to the ISP address library one by one. This method is applicable to the address library containing a few addresses.

Procedure

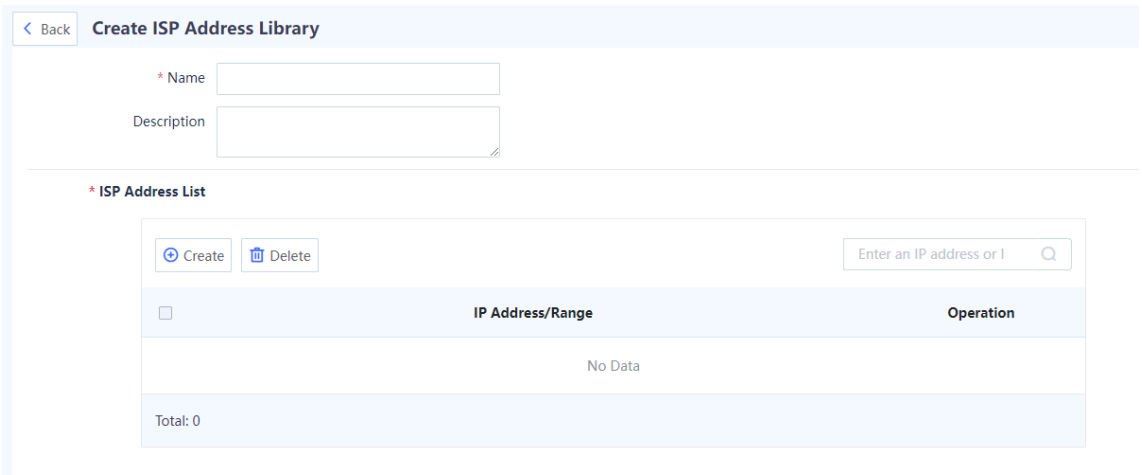
(1) Access the **Create ISP Address Library** page.

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.	[Example] Address library 1
Description	Description of the ISP address library.	-
ISP Address List	IP addresses contained in the address library.	Click **Create** to enter a single IP address or an IP address range. Three configuration methods are supported: ● IP address: One or multiple IP addresses. Input an IP address per line. Press Enter to separate lines. Example: 192.168.20.3 ● IP 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.

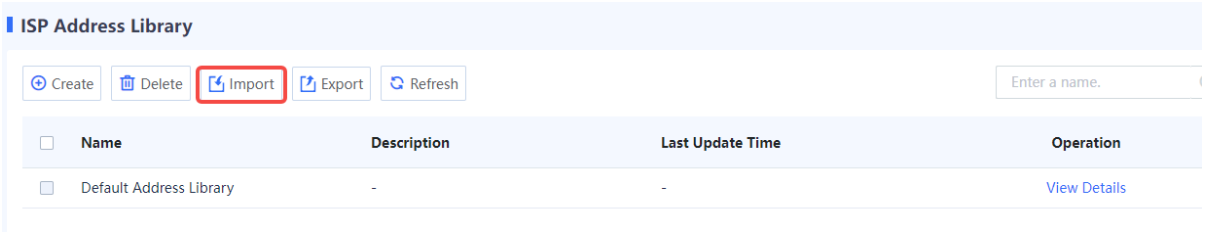
5.7.3 Creating an ISP Address Library by Importing an Address File

Application Scenario

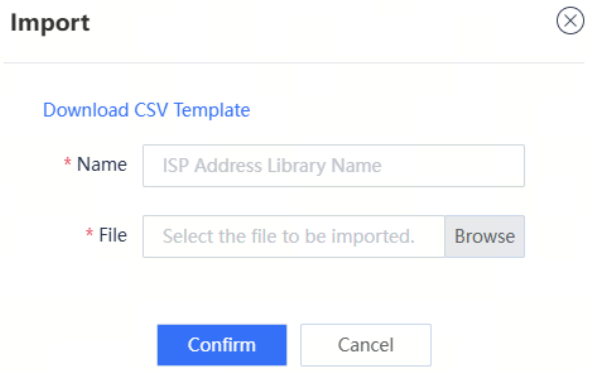
You can create the ISP address library by importing an address file. This method is applicable to the address library containing many addresses.

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.



(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**.

5.8 User Authentication

5.8.1 Overview

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

1. SSL VPN Authentication

The SSL VPN authentication process is as follows:

(1) On the VPN client, a remote user enters the IP address or domain name of the SSL VPN gateway, username, and password to request establishment of an SSL connection.

(2) The virtual gateway authenticates the user and supports the following authentication modes:

- Local authentication

  The remote user's identity information, including the username and password, is stored on the local device. After receiving the identity information, the virtual gateway authenticates the user according to the authentication domain configuration.

- Server authentication

  The remote user's identity information, including the username and password, is stored on the authentication server. After receiving the identity information, the virtual gateway forwards it to the

authentication 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 redirect URL (portal authentication page) to the browser.

(3) The device supports both local portal authentication and external 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 external portal authentication, a portal server is required.

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

(5) When performing the required authentication operations on the portal page (such as entering a username and password) and passing the authentication, you can continue to access the Internet.

5.8.2 User Management

1. Configuring User Groups

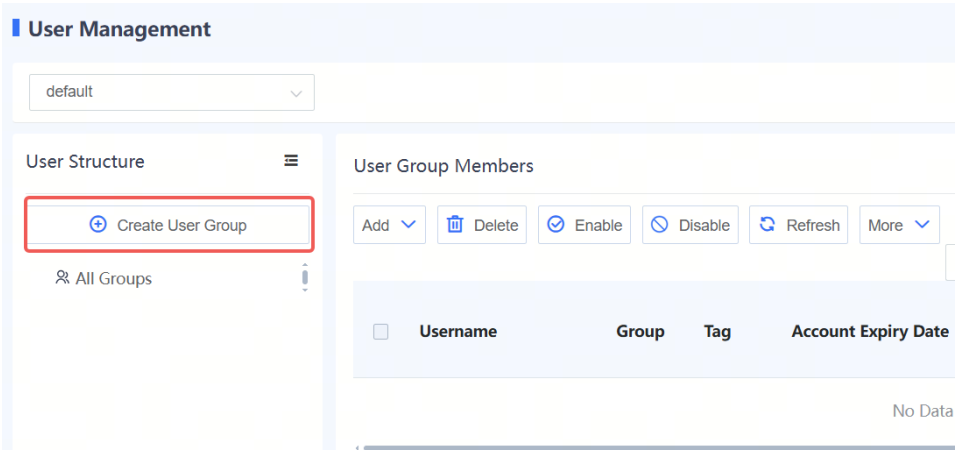
Application Scenario

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

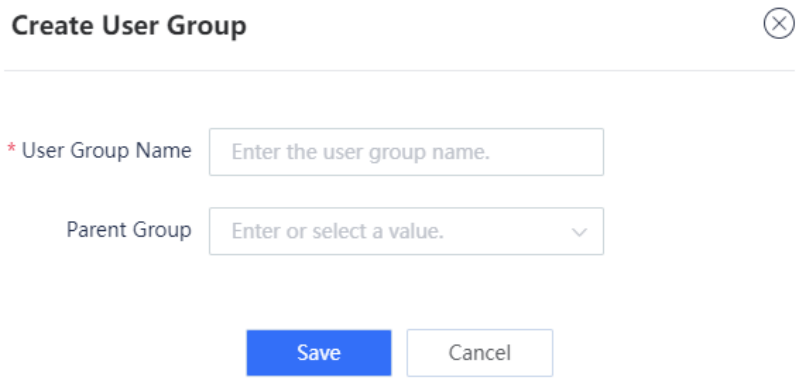
Procedure

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

(2) Click **Create User Group**.



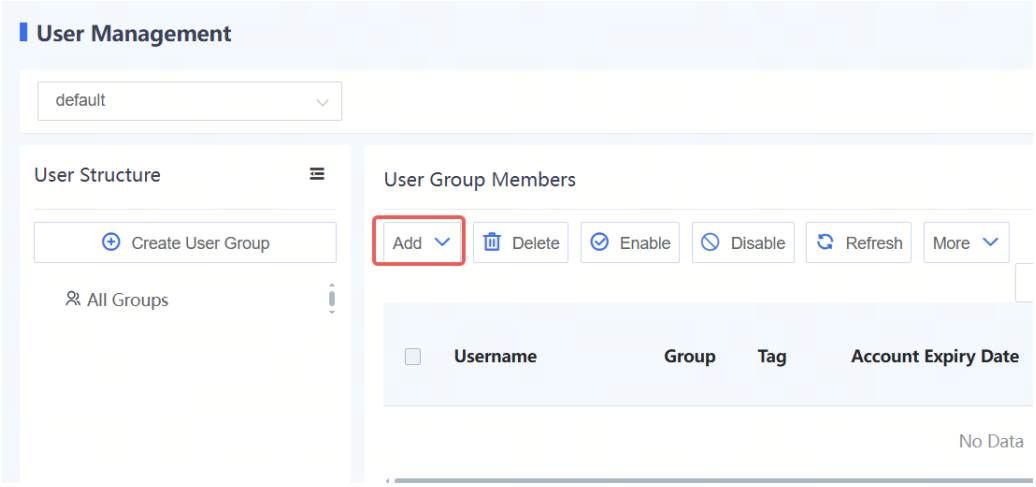
(3) Enter the user group name and select a parent group.



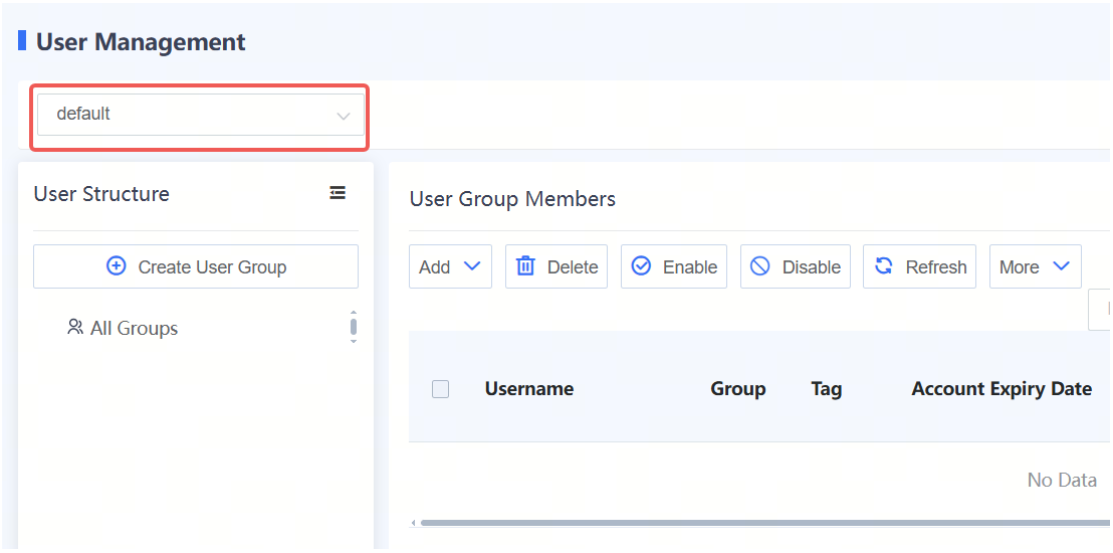
(4) After verifying the configuration, click **Save**.

Follow-up Procedure

- Click **Add** to configure users for the user group.



- Click the drop-down list in the upper left corner to switch the authentication domain and view user group and user information in the authentication domain.



2. Configuring Users

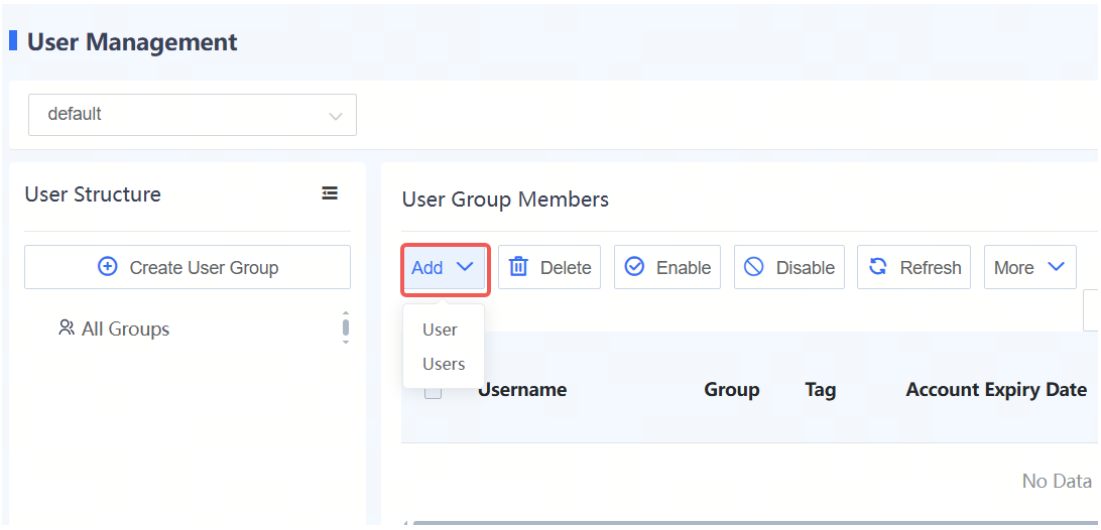
Application Scenario

In an authentication scenario, 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.

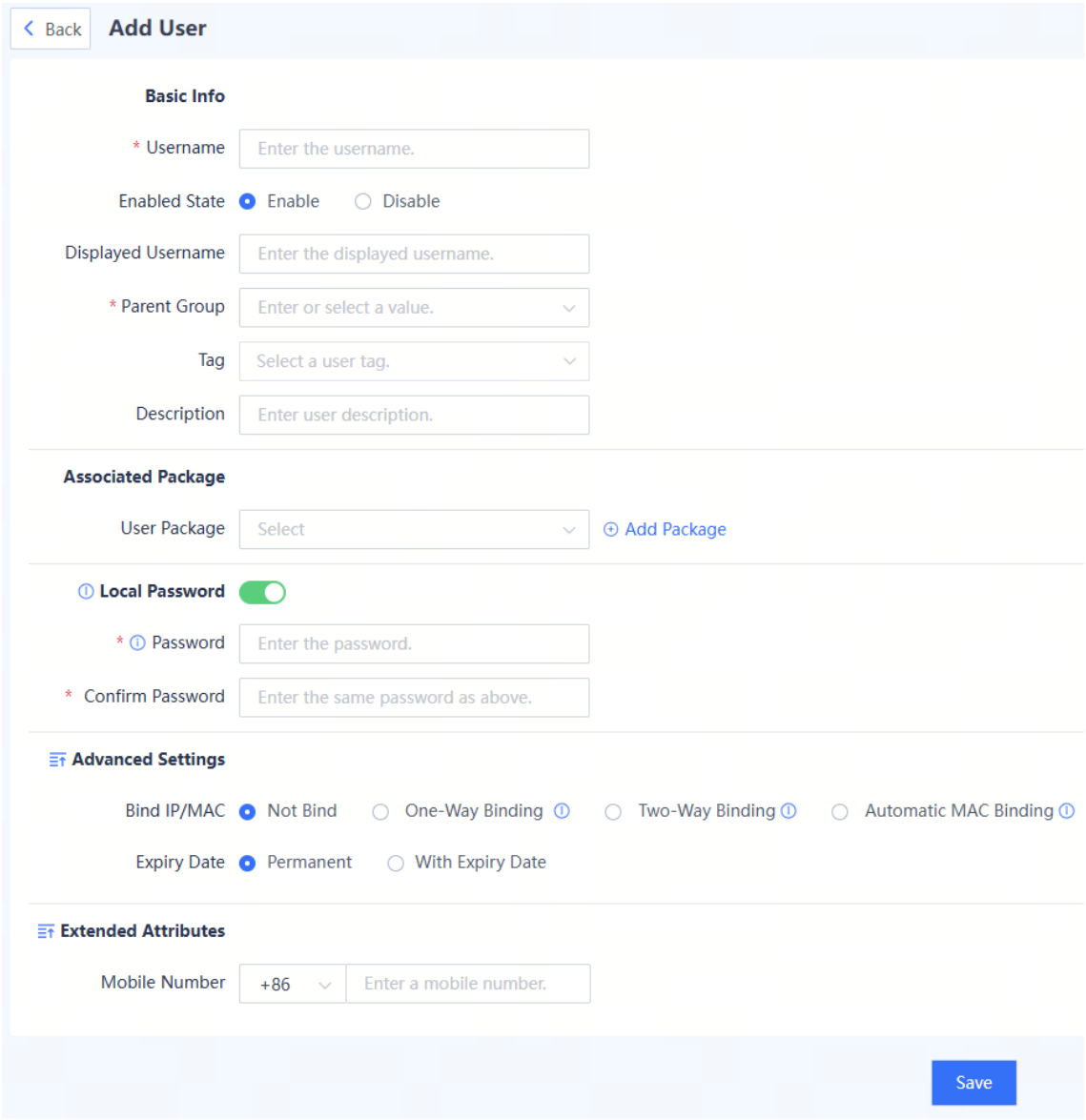
Procedure

(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

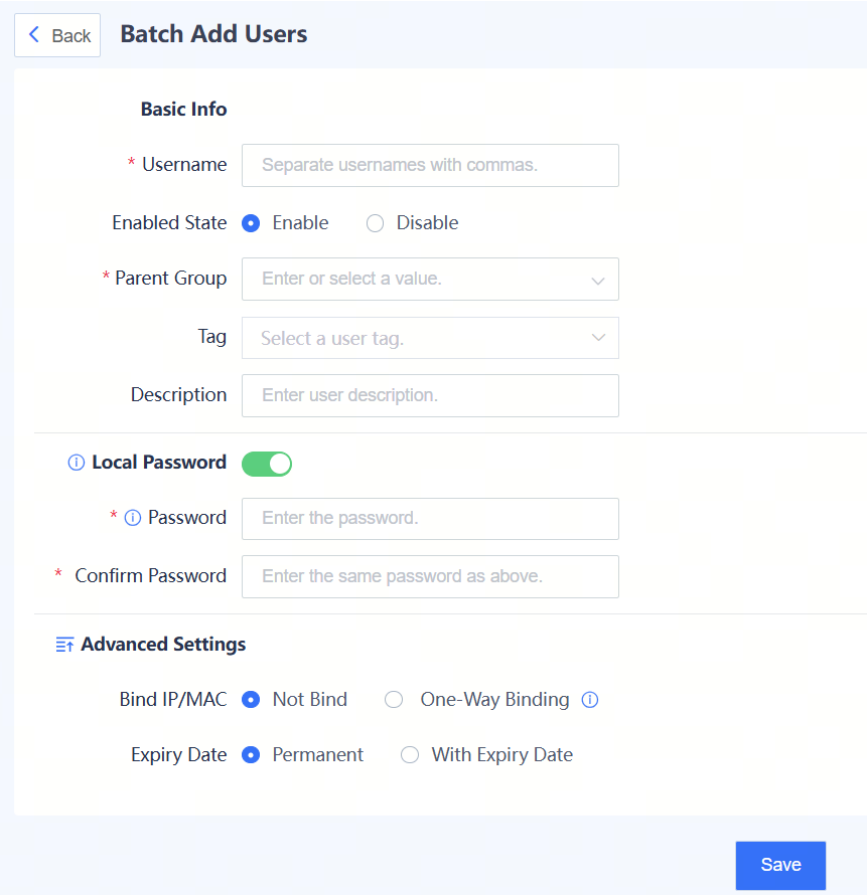


Item	Description	Remarks
Basic Info		

Item	Description	Remarks
Username	Username used for user authentication.	If a user is added to the default authentication domain, the actual login username is the string entered here. If a user is added to a custom authentication domain, the actual login username is the string entered here plus **@** and the custom authentication domain name. For example, if the entered username is **user1**, the login username in the default authentication domain is **user1**; and the login username in a custom authentication domain (for example, **testdomain**) is **user1@testdomain**. Usernames of users in the same authentication domain cannot be duplicated.
Enabled State	Whether to enable user information for authentication. Users in disabled status cannot be authenticated.	[Example] Enable
Displayed Username	Username displayed upon successful authentication. The value can be the same as that of **Login Username**.	[Example] user1
Parent Group	Group to which the user belongs.	[Example] /default
Tag	Tag to which a user belongs.	Click the drop-down list and select an existing user tag.
Description	User description.	N/A
Associated Package ● Associate users with packages and enable package attributes, for example, limiting the number of terminals that can be connected per account concurrently. ● The package function does not take effect for SSL VPN users.		
User Package	Package associated with a user.	● Each user can only be associated with one package. ● Click **Add Package** to create a user package.

Item	Description	Remarks
Local Password You do not need to enable it when external authentication is used.		
Password	Password for user login. For details about password complexity requirements, see 5.8.11 3. Other Authentication Settings.	N/A
Confirm Password	The value must be the same as that of **Password**.	N/A
Advanced Settings		
Bind IP/MAC	Whether to specify the IP or MAC address for user login: ● **Not Bind**: Unrestricted. ● **One-Way Binding**: The current user can log in using only the specified IP or MAC address of a PC. Other users can also use this IP or MAC address for login. ● **Two-Way Binding**: The current user an log in using only the specified IP or MAC address of a PC. Other users cannot use this IP or MAC address for login. ● **Automatic MAC Binding**: When a user uses an account for authentication for the first time and is successfully authenticated for login, the system automatically binds the account to the MAC address of the terminal. In subsequent authentication, the user can only use the same MAC address for authentication.	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
Extended Attributes		
Mobile Number	User's mobile number. If SMS two-factor authentication needs to be performed for an SSL VPN access user, or web-based authentication users are required to undergo SMS authentication, the user's mobile number must be configured.	Select an area code from the drop-down list and enter the mobile number.

- Adding users in a batch



Item	Description	Remarks
Basic Info		

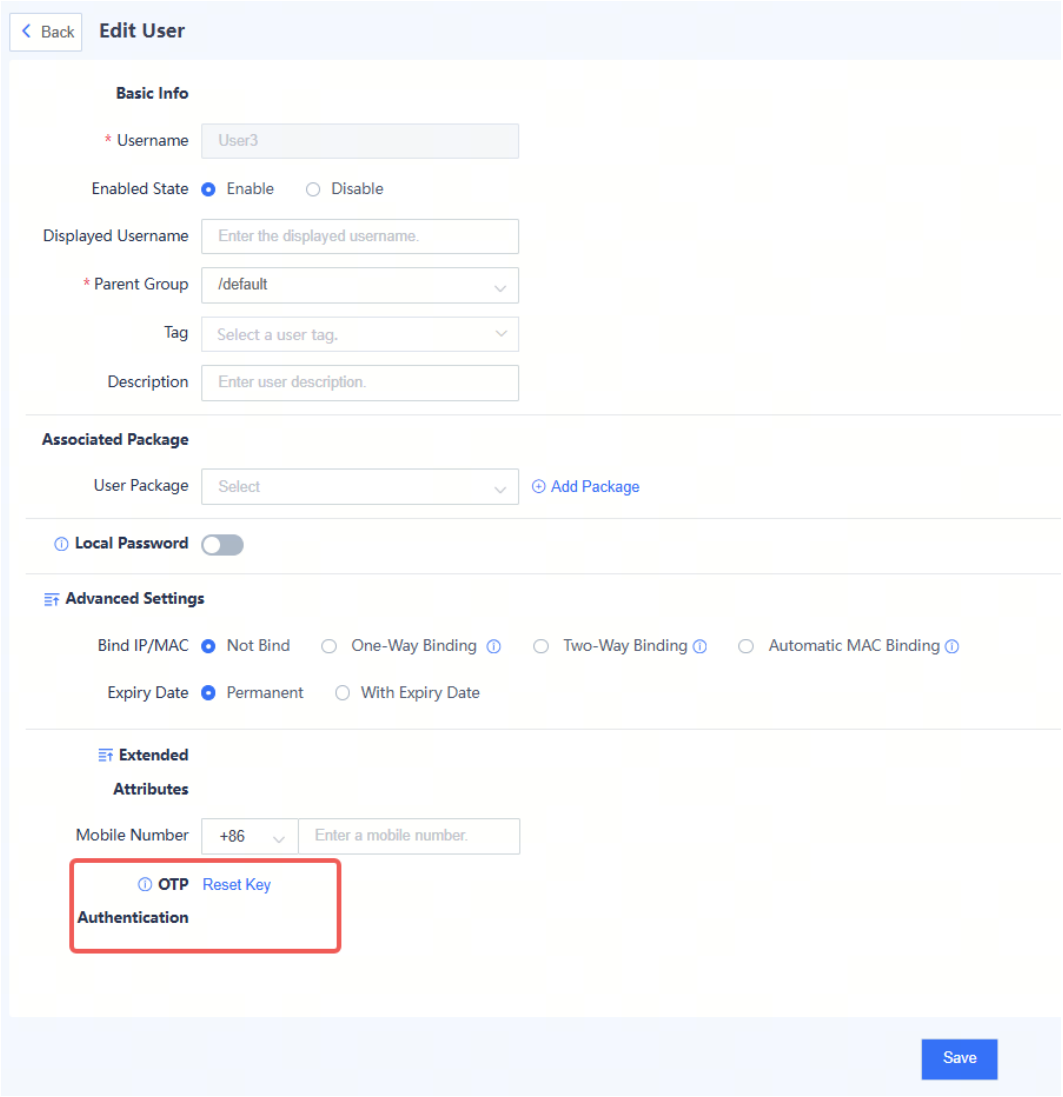
Item	Description	Remarks
Username	Username used for remote user authentication. Separate usernames with commas (,).	If a user is added to the default authentication domain, the actual login username is the string entered here. If a user is added to a custom authentication domain, the actual login username is the string entered here plus **@** and the custom authentication domain name. For example, if the entered username is **user1**, the login username in the default authentication domain is **user1**; and the login username in a custom authentication domain (for example, **testdomain**) is **user1@testdomain**.
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
Tag	Tag to which a user belongs.	Click the drop-down list and select an existing user tag.
Description	User description.	N/A
Local Password You do not need to enable it when external authentication is used.		
Password	Password for user login, which can be used by multiple users.	N/A
Confirm Password	The value must be the same as that of **Password**.	N/A
Advanced Settings		

Item	Description	Remarks
Bind IP/MAC	Whether to specify the IP or MAC address for user login: ● **Not Bind**: Unrestricted. ● **One-Way Binding**: The current user can log in using only the specified IP or MAC address of a PC. Other users can also use this IP or MAC address for login. ● **Two-Way Binding**: The current user can log in using only the specified IP or MAC address of a PC. Other users cannot use this IP or MAC address for login.	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 view the extended attributes of OTP authentication. To reset OTP keys, click **Reset Key**. For details about how to configure OTP authentication, see 6.9.2 Creating an SSL VPN Gateway.



- 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.

5.8.3 User Tag

Application Scenario

The device supports user tag-based management. User identification and classification can be performed through flexible tag configuration. The tags can serve as the basis for policy configuration and permission management, simplifying the organization and control of users.

Precautions

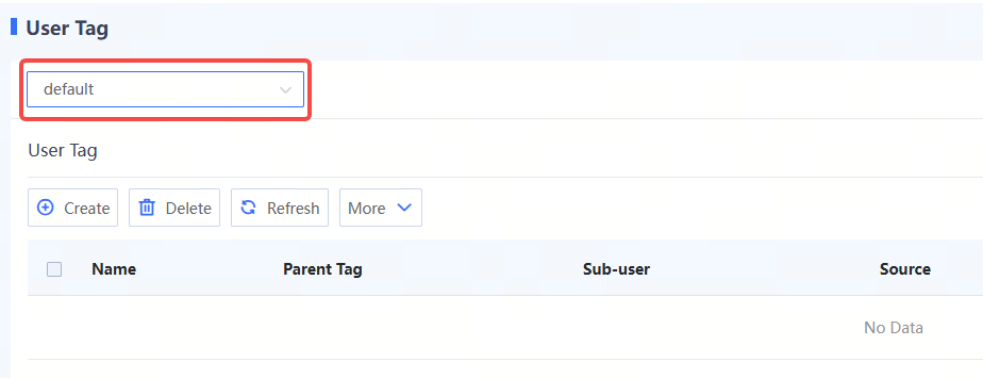
- A user tag must be unique in an authentication domain.
- Up to three levels can be configured for users and user tags in total. That is, a single user can have up to two levels of nested tags (parent tag and child tag).
- A single tag can be associated with up to four parent tags, and a single user can be associated with up to 40 parent tags.
- A user tag can contain multiple child tags and can also be included in multiple parent tags.
- If a security group has been associated with users on the LDAP server, the security group is configured as the user tag during import to the device, and the users in the security group are also imported to the device. If a security group is not associated with users, the security group is ignored and is not imported to the device.

  For example, a security group **group1** exists on the LDAP server and a user **user1** exists in the security group. During import to the device, **group1** is added as a user tag on the **User Tag** page, and **user1** is added as a user (with the user tag of **group1**) on the **User Management** page.

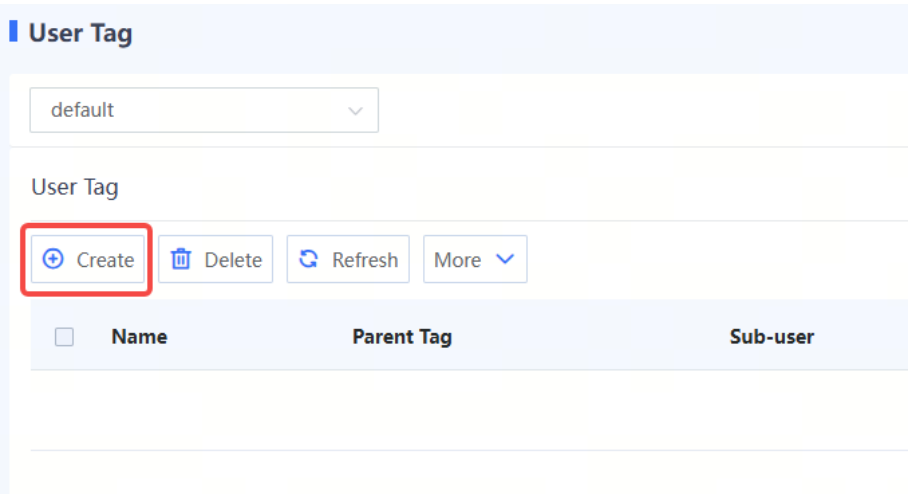
Procedure

(1) Choose Object > User Authentication > User Tag.

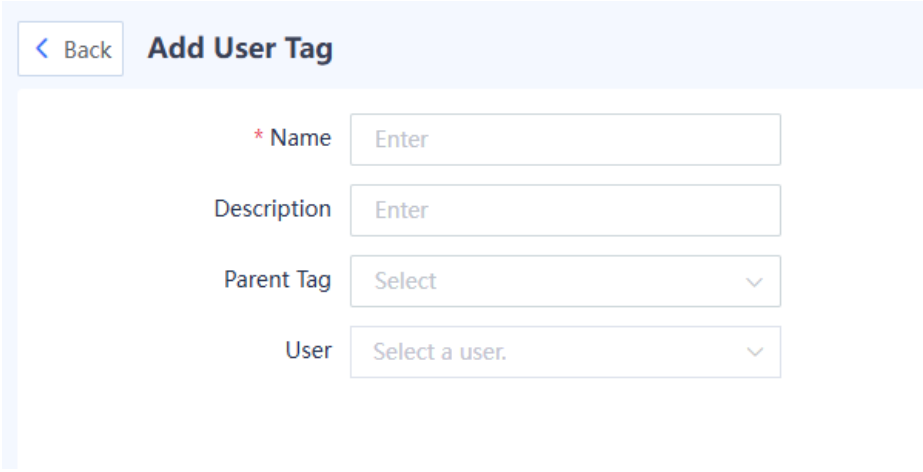
(2) Select an authentication domain to which a user tag needs to be added.

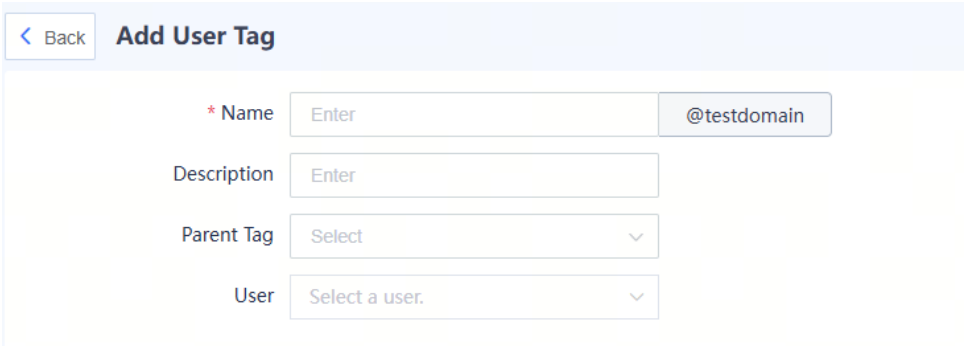


(3) Click **Create** to add a user tag.



(4) Configure user tag information.





Item	Description	Remarks
Name	User tag name.	If a user tag is added to the default authentication domain, the actual tag name is the character string entered here. If a user tag is added to a custom authentication domain, the actual tag name is *entered character string@custom authentication domain name*. For example, if **Name** is set to **label1** for a user to be added to the default authentication domain, the actual tag name is **label1**; if **Name** is set to **label1** for a user to be added to the custom authentication domain **testdomain**, the actual tag name is **label1@testdomain**.
Description	User tag description.	N/A

Item	Description	Remarks
Parent Tag	Parent tag of the user tag.	● Click the drop-down list and select a created user tag in the current authentication domain. ● A single tag can be associated with up to four parent tags. ● Tags support a two-level structure of parent tags and child tags. A child tag cannot be used as a parent tag for other tags. For example, if **label2** is the parent tag of user tag **label1**, **label1** cannot act as a parent tag for any other user tags.
User	Users associated with the user tag.	Click the drop-down list and select created users. For details about user creation, see 5.8.2 User Management.

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

Follow-up Procedure

- Select one or more user tags and click **Delete** to delete the user tags. If a user tag has been referenced in a security policy, the user tag cannot be deleted. For details about security policies, see 4.1 Security Policy.
- Click **Refresh** to view the latest user tag information.
- Click **More** and select **Export User Tags in Current Domain** or **Export User Tags in All Domains** to export the corresponding user tag information to the local end in CSV format.
- Click **Edit** in the **Operation** column of a user tag to edit tag information.

5.8.4 User Import

1. Overview

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.

2. User Import

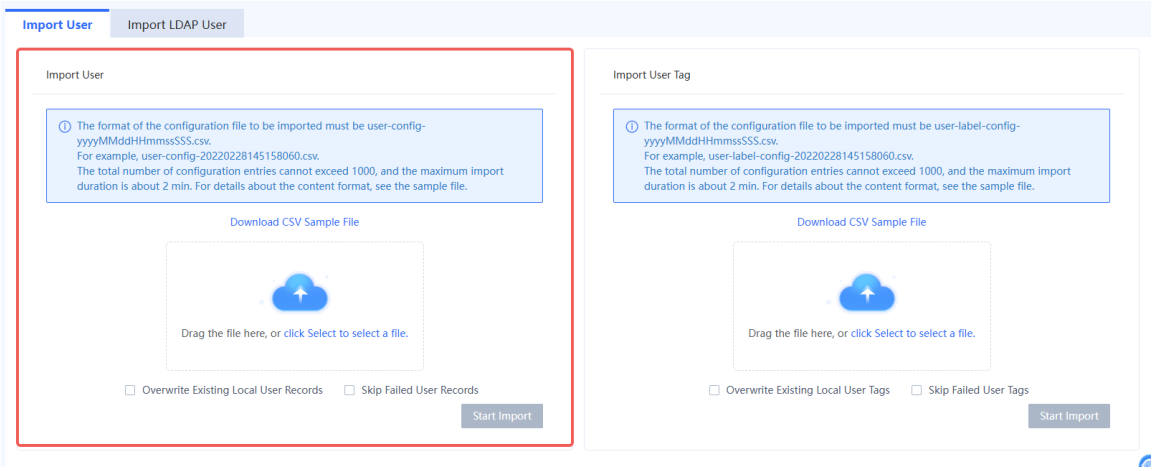
Procedure

(1) Choose **Object** > **User Authentication**> **Import User** > **Import User**.

(2) In the **Import User** area, 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.



(5) Click **Start Import**.

Follow-up Procedure

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

3. User Tag Import

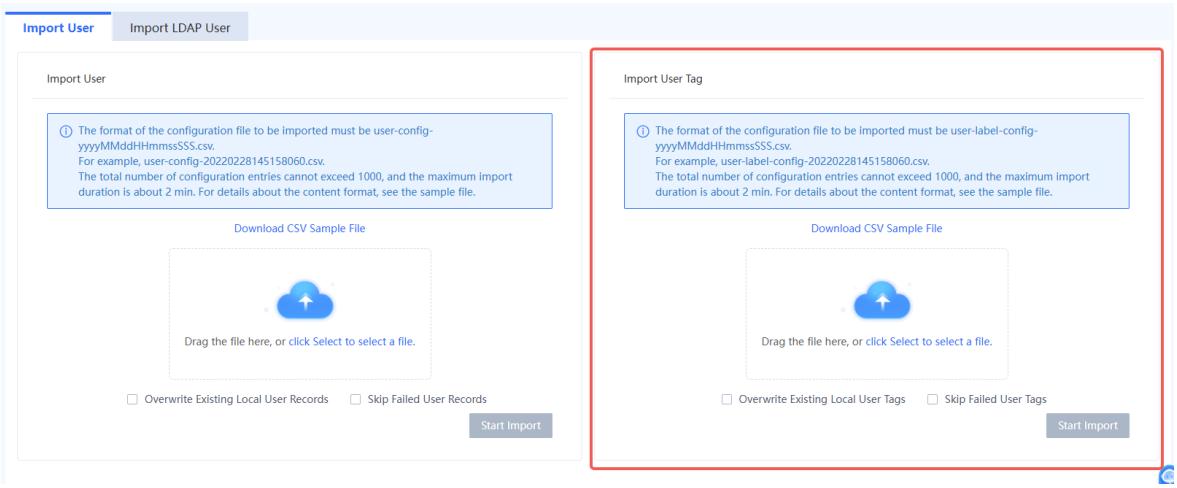
Procedure

(1) Choose Object > User Authentication > Import User > Import User.

(2) In the **Import User Tag** area, click **Download CSV Sample File** to download the import template. Fill in user tag information according to template requirements and examples.

(3) Click **click Select to select a file** and import the file of user tag information.

(4) (Optional) Select **Overwrite Existing Local User Tags** or **Skip Failed User Tags**. If neither is selected, a message is displayed upon repeated user tags or import failures.



(5) Click **Start Import**.

Follow-up Procedure

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

4. LDAP User Import

Precautions

When integrating with an AD domain server to synchronize user data, the device imports nodes with the **sAMAccountName** attribute as users and nodes with the **objectClass=organizationalUnit,objectClass=container** attribute as user groups by default. The following attributes are synchronously imported for users by default:

- When a user has the **userPrincipalName** attribute, their login name is imported as the username.
- When a user has the **memberOf attribute** attribute, the corresponding attribute value is imported as the user tag.
- When a user has the **telephoneNumber** attribute, the corresponding attribute value is imported as the user's mobile number.

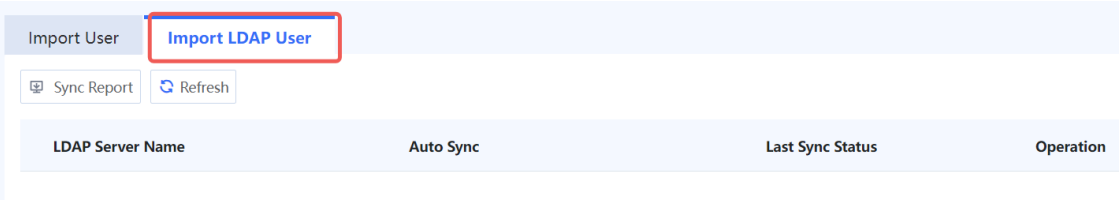
Note

To modify the attribute fields corresponding to users and user groups, choose **Object** > **User Authentication** > **Authentication Server** > **LDAP** to configure **Advanced Settings** for the LDAP server.

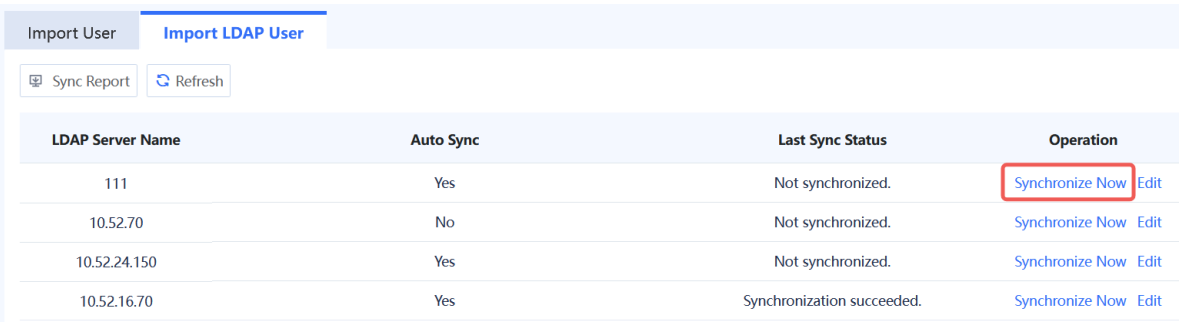
Procedure

(1) Choose **Object** > **User Authentication** > **Import User** > **Import LDAP User**.

(2) On the page that is displayed, check the configured LDAP server synchronization setting and the latest synchronization status.



(3) Click **Synchronize Now** to import user information from the LDAP server to the local device.



(4) (Optional) Click **Edit** to modify the LDAP server configuration.

Follow-up Procedure

- Each synchronization generates a synchronization report. Click **Sync Report** to view detailed synchronization information.

5.8.5 User Package Management

Application Scenario

A user package defines differentiated resources and services provided for different user groups. With user packages, the system can provide personalized service options for users, meeting diversified network access and resource usage requirements.

After an account is associated with a package, the package attributes will take effect. For example, limiting the number of terminals that can be connected per account concurrently.

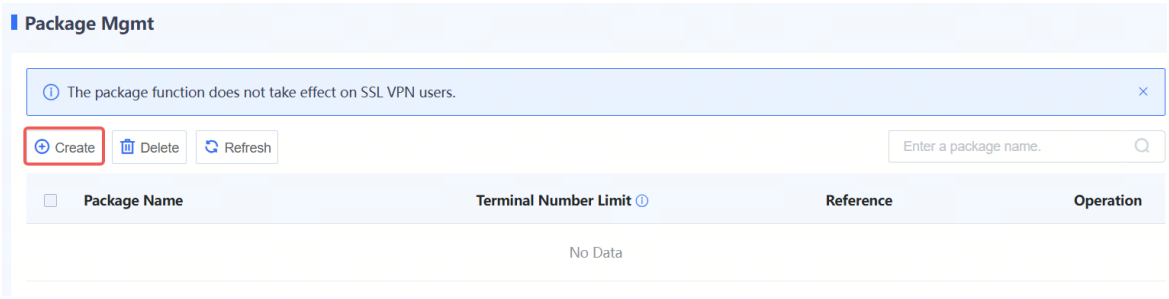
Caution

- A user package takes effect only after it is associated with a user. For details on how to configure a user package, see 5.8.2 2. Configuring Users.
- The user package function does not take effect for SSL VPN users.

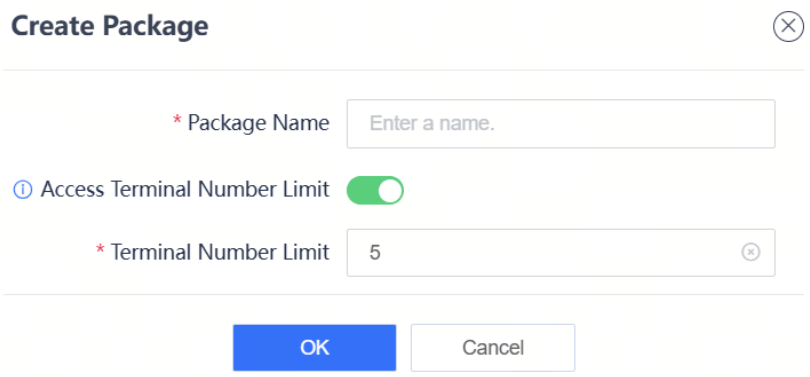
Procedure

(1) Choose **Object** > **User Authentication** > **User Package Mgmt**.

(2) Click **Create** to create a user package.



(3) Configure parameters for a user package.



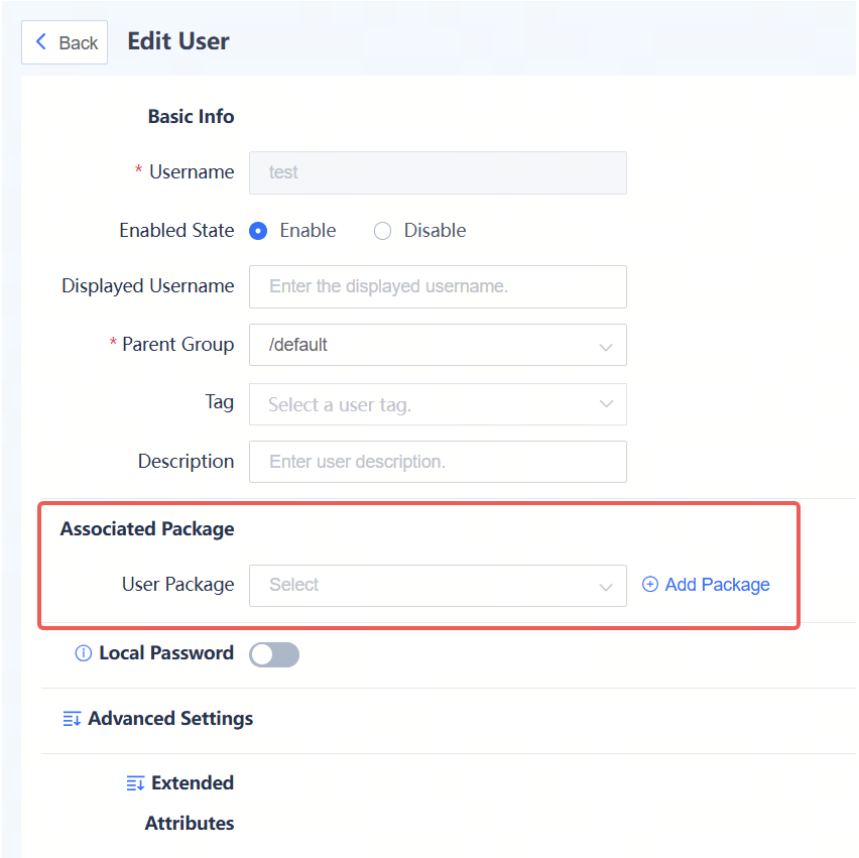
Item	Description	Remarks
Package Name	Package name.	[Example] plan_test

Item	Description	Remarks
Access Terminal Number Limit	Whether to limit the number of terminals that a user can use for access. If it is disabled, the number of terminals is not limited.	[Example] Enabled
Terminal Number Limit	Configure the maximum number of terminals that can be connected per account concurrently. Note that if an account can be used by different services concurrently (for example, an account can be used for both web-based authentication and PPPoE authentication), the access terminals used for these services will consume the capacity of access terminals in the package.	● This parameter needs to be configured when **Access Terminal Number Limit** is enabled. ● The value range is from 1 to 30. [Example] 5

(4) Click **OK**.

Follow-up Procedure

- Associate a user with the user package. For details, see 5.8.5 User Package Management.



- On the **User Package Mgmt** page, you can perform the following management operations:

- Click **Refresh** to obtain the latest configuration data.
- Click **Edit** in the **Operation** column to modify the package configuration.
- To delete a user package, click **Delete** in the **Operation** column. To batch delete user packages, select multiple packages and click **Delete** at the top of the page. A referenced user package cannot be deleted.
- Click **View** in the **Reference** column to view the package reference status.

5.8.6 Online User

1. Authenticated Online User

Application Scenario

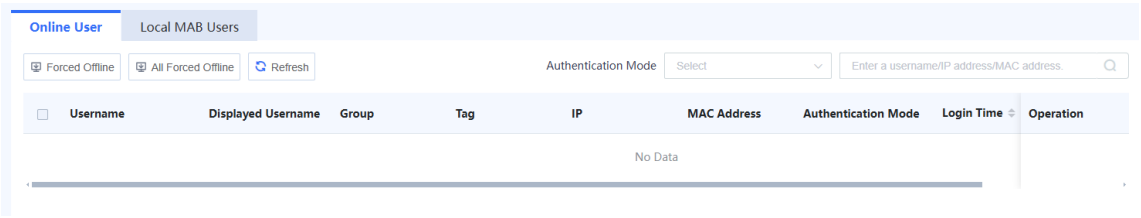
When a remote user accesses the intranet through SSL VPN or passes the web authentication, you can check online user information on the **Online User** page.

Procedure

(1) Choose **Object** > **User Authentication** > **Online User** > **Online User**.

You can filter online user information based on the authentication mode, user name, user IP address, or user MAC address.

(2) (Optional) Select one or multiple users and click **Forced Offline** to batch disconnect users. To disconnect all users, click **All Forced Offline**.



2. Local MAB User

Application Scenario

When local portal MAC Authentication Bypass (MAB) is enabled in the local authentication scenario, a user performs manual authentication and goes online. In this case, the system records the username and terminal MAC address into the binding list. When the terminal requests to access again, the system checks whether the terminal MAC address matches the local MAB user entry according to the binding list. If so, the user does not need to perform manual authentication again and can go online directly through the MAB process.

This tab page displays the binding information of local MAB users. The administrator can manually delete the MAC address in a user entry to prevent the user or terminal from accessing the network in MAB mode.

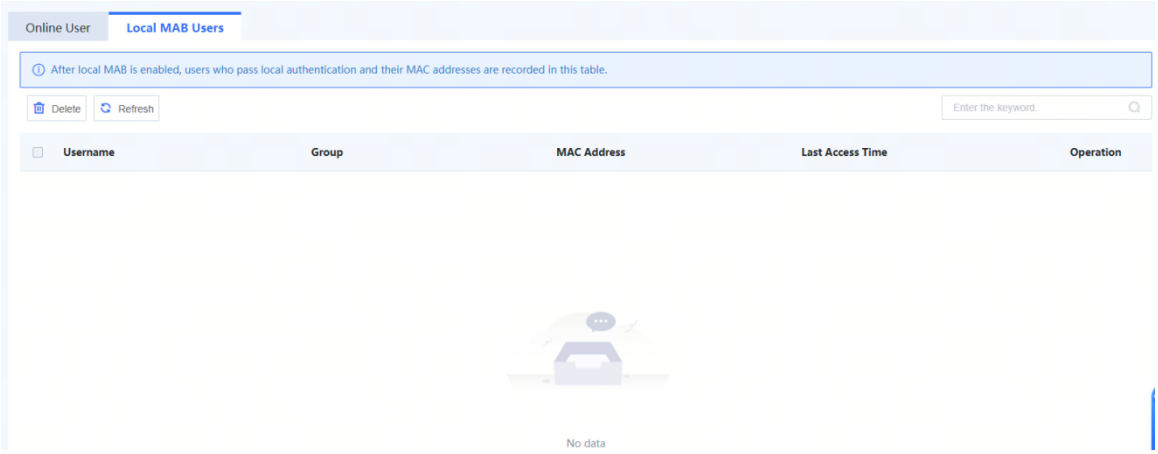
Note

- The number of MAC addresses recorded for each user is limited. If a terminal's MAC address is not authenticated again through the MAB process for a long time, the MAC address entry will be automatically aged out and deleted. For details on how to configure the maximum number of MAC addresses recorded for each user and MAB user idle aging time, see 5.8.9 Authentication Template - Local Portal Authentication.
- Local MAB takes effect only in Layer 2 environments.

Procedure

(1) Choose **Object** > **User Authentication** > **Online User** > **Local MAB Users**.

(2) Check information about local MAB users.



- In the **Operation** column of a user entry, click **Delete** to delete the local MAB user entry. After the deletion, the terminals that go offline and then access the network again using the corresponding username through local authentication need to be manually authenticated. To batch delete local MAB user entries, select them and click **Delete** at the top of the page.
- Click **Edit** in the **Operation** column of a user entry to view all MAC addresses recorded for the user.

  If a MAC address recorded for a user is deleted, the corresponding terminal cannot access the network in MAB mode. When the terminal goes offline and then accesses the network again, manual authentication is required. If all MAC addresses of a user are deleted, the user entry is also deleted.

5.8.7 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.

The system has three predefined authentication domains by default. Predefined authentication domains cannot be deleted.

Authentication Domain	Description	Default Configuration
default	Default authentication domain.	SSL VPN authentication and web-based authentication are enabled, and the user location information source is **Only Local Info**. You can manually configure and associate with an authentication server to use user information on the server for authentication.

Authentication Domain	Description	Default Configuration
pppoe	If the device functions as a PPPoE server, **pppoe** is used as the default authentication domain to manage PPPoE accounts and authenticate users that access through PPPoE.	PPPoE is enabled, and the user location information source is **Only Local Info**. You can manually configure and associate with an authentication server to use user information on the server for authentication.
vpn	This authentication domain applies to VPN access scenarios (such as PPTP VPN and L2TP VPN) and is used to manage VPN accounts and authenticate users that access through VPN tunnels.	SSL VPN and VPN are enabled, and the user location information source is **Only Local Info**. You can manually configure and associate with an authentication server to use user information on the server for authentication.

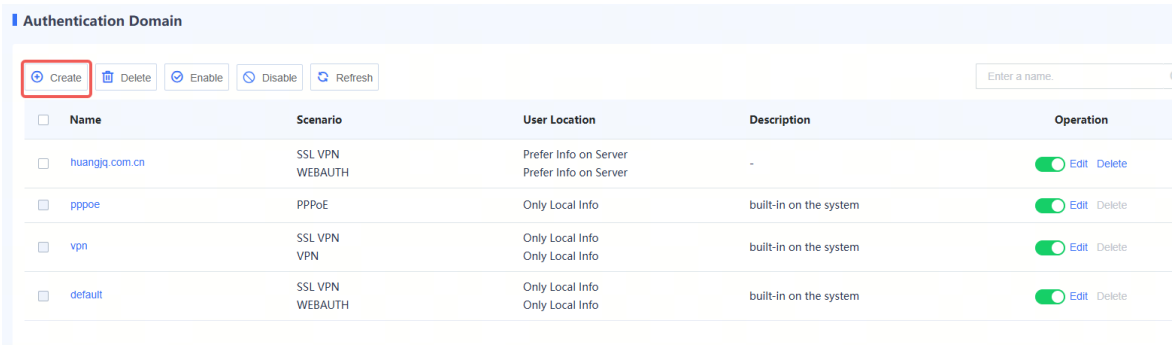
Prerequisites

You have configured user information on the firewall or authentication server. For details, see 5.8.2 User Management. For details on how to configure user information on the authentication server, see the **corresponding server manual.**

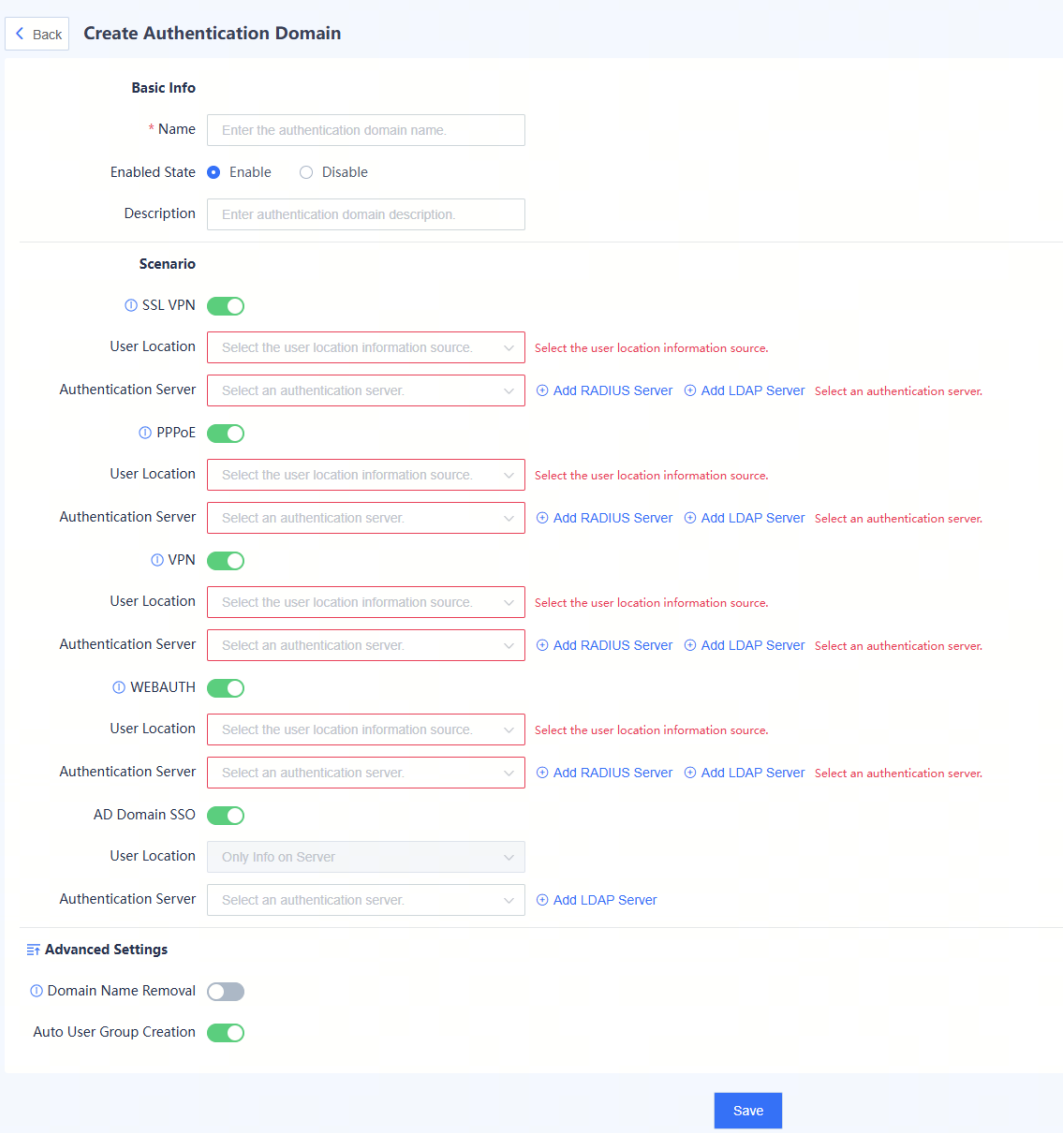
Procedure

(1) Choose **Object** > **User Authentication** > **Authentication Domain**.

(2) Click **Create**.



(3) Configure authentication domain information.



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
Scenario		

Item	Description	Remarks
SSL VPN	Whether to apply the authentication domain to the SSL VPN access scenario. After this function is enabled, you can view and select the current authentication domain when configuring the SSL VPN gateway. If an authentication server is configured in a non-default authentication domain, when an SSL VPN user logs in to the device, the username in the format of *Username@Domain name* is sent to the authentication server by default. *Domain* indicates the name of the current authentication domain. To remove the domain name in the username, enable **Domain Name Removal** in the **Advanced Settings** area.	[Example] Enabled
PPPoE	Whether to apply the authentication domain to the PPPoE access authentication scenario. After this function is enabled, PPPoE dial-up users can use user identity information in the current authentication domain for authentication. In PPPoE authentication scenarios, if the username entered does not contain **@**+*Domain name*, the user belongs to the PPPoE authentication domain by default. For example, the username **test** indicates that the authentication domain of the user is **pppoe**, and the username **test@123** indicates that the authentication domain of the user is **123**.	[Example] Enabled
VPN	Whether to apply the authentication domain to VPN authentication (non-SSL VPN) scenarios. After this function is enabled, VPN users can use user identity information in this authentication domain for authentication. In VPN authentication scenarios, if the username entered does not contain **@**+*Domain name*, the user belongs to the VPN authentication domain by default. For example, the username **test** indicates that the authentication domain of the user is **vpn**, and the username **test@123** indicates that the authentication domain of the user is **123**.	[Example] Enabled

Item	Description	Remarks
WEBAUTH	Whether to apply the authentication domain to the web-based authentication scenario. After this function is enabled, web-based authentication users can use user identity information in this authentication domain for authentication. In web-based authentication scenarios, if the username entered does not contain **@**+*Domain name*, the user belongs to the default authentication domain by default. For example, the username **test** indicates that the authentication domain of the user is **default**, and the username **test@123** indicates that the authentication domain of the user is **123**.	[Example] Enabled
User Location	Set the user authentication mode. The options are as follows: ● **Prefer Info on Server**: User identity information, including the username and password, is stored on the authentication server or local firewall. When the firewall is properly connected to the authentication server, only the authentication server is used for authentication. When the server network is unreachable, the user information on the firewall is 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. When no user information exists on the firewall, the user information on the server is 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
AD Domain SSO	Whether to enable AD domain Single Sign-on (SSO) for the authentication domain. If this function is enabled, user identity information must be available on the AD domain server, which is used for authentication.	-
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 and is authenticated. By default, the authentication domain name is not removed.	[Example] Disabled

Item	Description	Remarks
Auto User Group Creation	After this function is enabled, when the device receives user information synchronized from a server, the device identifies the user group to which the user belongs. If the user group already exists locally on the device, the user will be added to the local user group. Otherwise, a user group will be created automatically. If this function is disabled, the default user group of an online user authenticated by the server is specified by **Default Online User Group**.	[Example] Enable
Default Online User Group	Configure the default user group for users that go online through server authentication.	This parameter is available only when **Auto User Group Creation** is toggled off.

(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**.

5.8.8 Authentication Policies

Application Scenario

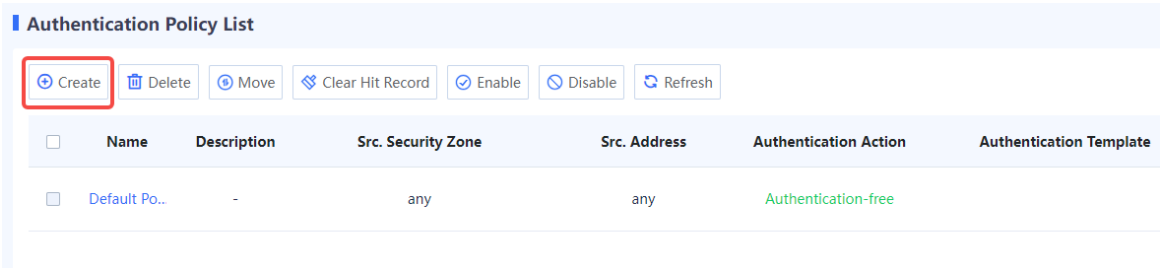
For scenarios where web authentication is required, you can configure authentication policies to execute specified authentication actions on user traffic from a specific source security zone or source IP address. On the device, a default policy is predefined to execute the authentication-free action 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.

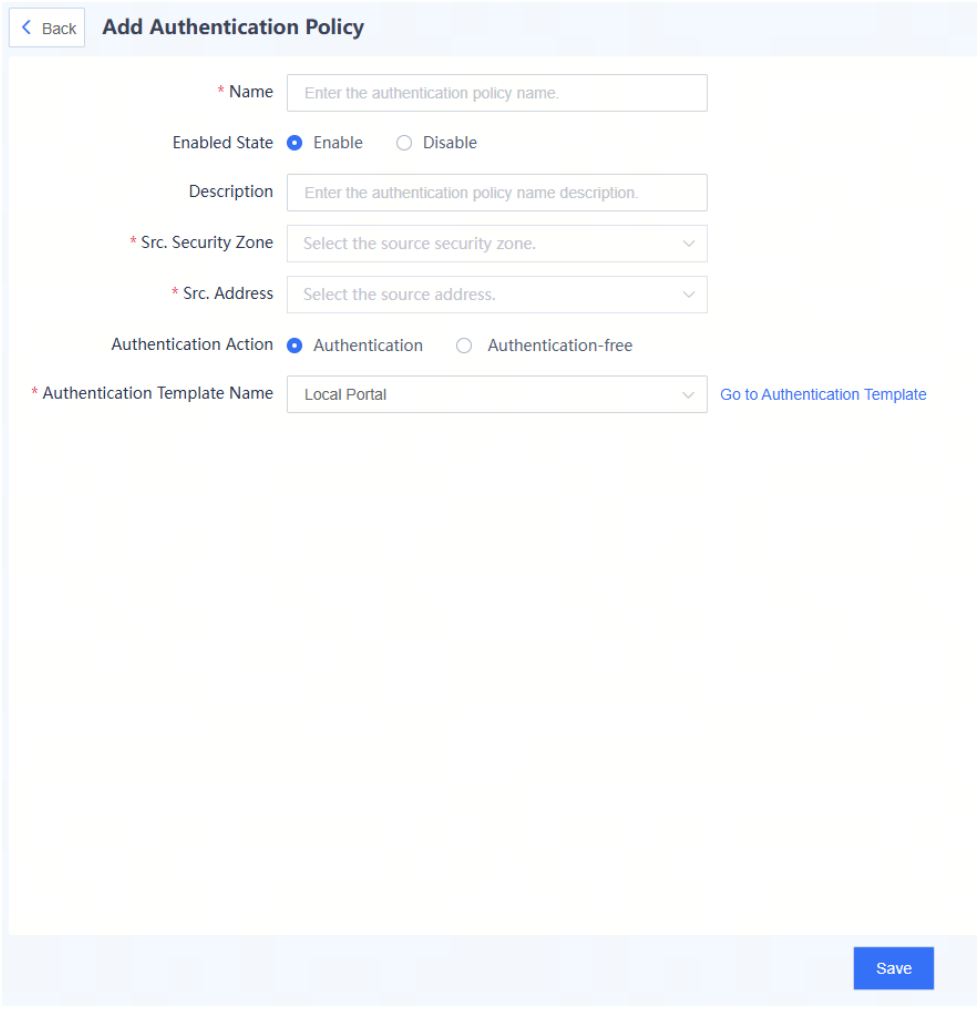
Procedure

(1) Choose **Object** > **User Authentication** > **Authentication Policy List**.

(2) Click **Create**.



(3) Configure an authentication policy.



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.	-

Item	Description	Remarks
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.	Any indicates all interfaces. [Example] trust
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 5.8.9 Authentication Template - Local Portal Authentication.	

(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 external network 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.

5.8.9 Authentication Template - Local Portal Authentication

1. Basic Configuration

Application Scenario

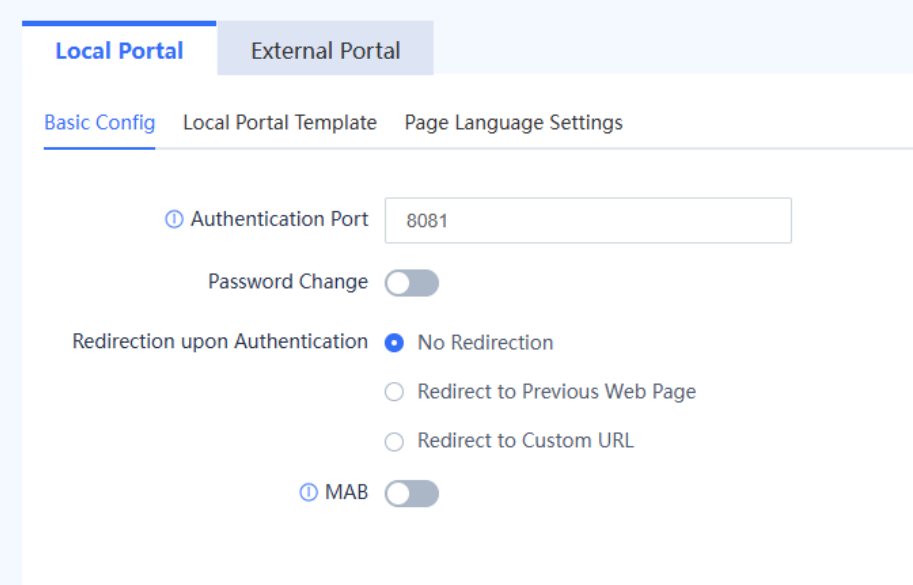
In a web authentication scenario where local portal authentication is selected, the firewall redirects the access page to the built-in portal authentication page when an unauthenticated user accesses the external network. The user can access external network resources only after being authenticated.

On the **Basic Config** page, you can set the global parameters including **Authentication Port**, **Redirection upon Authentication**, and **MAB** for the local portal authentication.

Procedure

(1) Choose **Object** > **User Authentication** > **Authentication Template** > **Local Portal** > **Basic Config**.

(2) Configure the authentication port based on actual services, configure whether to display the password change button on the authentication page, and configure the redirect page upon successful authentication.



Note

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

Item	Description	Remarks
Authentication Port	Port used by the device to push the authentication page.	The default authentication port is 8081. [Example] 8081
Password Change	Whether the password change button is provided on the portal authentication page.	[Example] Enabled
Redirection upon Authentication	Configure the redirect page upon successful authentication.	[Example] No Redirection
MAB ● After this function is enabled, the system records the MAC address of a terminal when the terminal completes local portal authentication for the first time. When the terminal accesses the network again, the MAB process is triggered. The system identifies the terminal and permits access. You do not need to enter the portal page for manual authentication again. ● The MAB function takes effect only for users who go online through the following authentication methods: o In the local portal template, set **Authentication Mode** to **Username/Password** so that users can go online only after entering the correct username and password. o In the local portal template, set **Authentication Mode** to **SMS Authentication** and toggle on **Bind Mobile Number for Authentication**. Users can use the mobile numbers configured on the **User Management** page to go online through SMS authentication. For details about the configuration of the local portal template, see 2. Local Portal Template. ● The MAB function takes effect only within Layer 2 broadcast domains and requires that no Layer 3 device exists between the device and the terminals.		

Item	Description	Remarks
MAB	Whether MAB is enabled.	[Example] Enabled
MAB User Idle Aging Time	If the terminal MAC address in an MAB user entry does not go online again within the idle aging time, the MAC address will be deleted. When the terminal accesses the network again, manual authentication is required.	[Example] 15 days
Max. MAC Number per User	Maximum number of MAC addresses that can be recorded for each user.	Click **View Binding List** to redirect to the **Local MAB User** page to view recorded MAC address information and manage binding entries. [Example] 5

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

2. Local Portal Template

Application Scenario

Configure a local portal template to set the authentication mode and authentication page style for local portal authentication.

- **Authentication Mode**: Supports **Username/Password** and **SMS Authentication**. Both authentication modes can be enabled simultaneously, and users can choose either mode for authentication.
- **Portal Page Style Settings**: Allows you to customize the local portal authentication page. When a user requests portal authentication, the device redirects the user request to the local portal authentication page. The authentication page allows you to customize the logo and background image to meet personalized page customization requirements.

The device provides a preset local portal template for configuration, and allows you to create a customized local portal template as required.

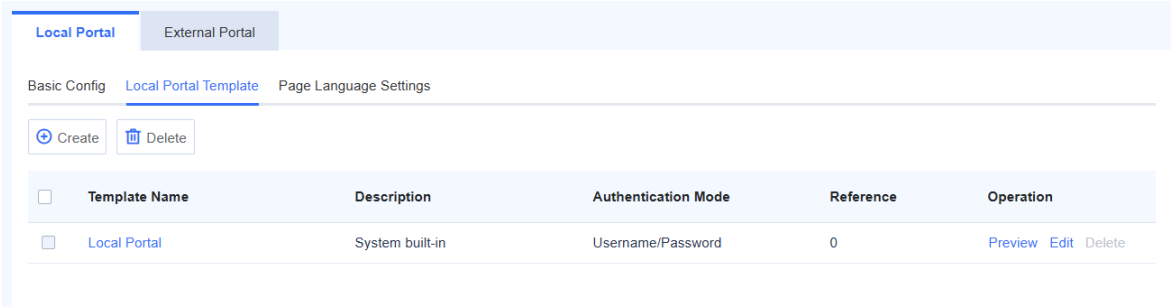
Precautions

- To enable SMS authentication, configure the SMS authentication server first. For details about the SMS authentication server, see 5.8.14 SMS Authentication Server.
- If username and password authentication is enabled, configure user names and local passwords on the **User Management** page in advance. For details about user management, see 5.8.2 User Management.
- After a local portal template is configured, it must be referenced by an authentication policy so that the local authentication configuration can take effect. For details about an authentication policy, see 5.8.8 Authentication Policies.

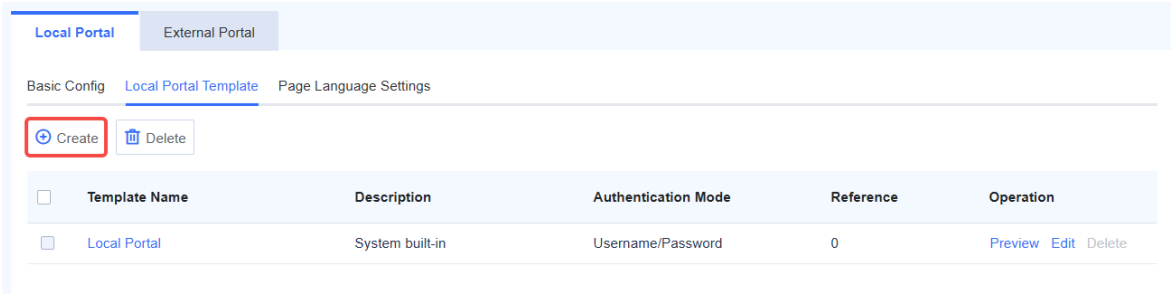
Procedure

(1) Choose **Object** > **User Authentication** > **Authentication Template** > **Local Portal** > **Local Portal Template**.

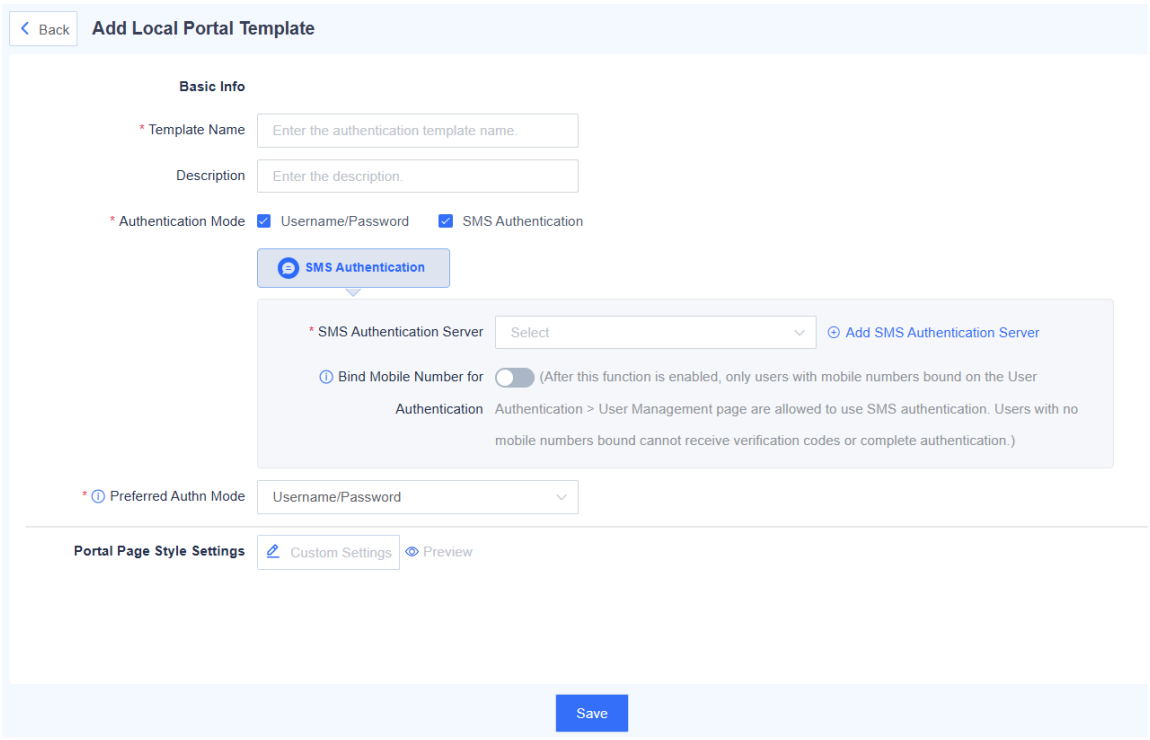
In the preset local portal template named **Local Portal**, **Authentication Mode** is set to **Username/Password** by default. You can edit and use the default template based on actual scenarios, or create a custom portal template. The default template cannot be deleted.



(4) Click **Create**.



(2) Configure parameters in the local portal template based on service requirements.



Item	Description	Remarks
Basic Info		

Item	Description	Remarks
Template Name	Authentication template name.	[Example] local_portal_1
Description	Authentication template description.	-
Authentication Mode	Authentication mode enabled in the authentication template: ● **Username/Password**: A user enters the username and password on the portal authentication page. The user can pass the authentication after the system verifies the credentials. ● **SMS Authentication**: A user receives a one-time SMS verification code through their mobile number. The user can pass authentication by entering the correct SMS verification code on the portal authentication page.	Both authentication modes can be selected, and users can select any one of them for authentication. [Example] SMS Authentication
Preferred Authn Mode	You can select a preferred authentication mode from the chosen modes to be displayed by default on the portal authentication page.	[Example] Username/Password
Authentication Mode: SMS Authentication		
SMS Authentication Server	You can select the SMS authentication server for SMS authentication. For details about the SMS authentication server, see 5.8.14 SMS Authentication Server.	Click **Add SMS Authentication Server** to add an SMS authentication server.
Bind Mobile Number for Authentication	After this function is enabled, choose **User Authentication** > **User Management** on which only users who have their mobile numbers bound are allowed to use SMS authentication. For details about how to configure a user's mobile number, see 5.8.2 User Management.	[Example] Disabled

(3) (Optional) Click **Custom Settings** next to **Portal Page Style Settings** to customize the portal page style.

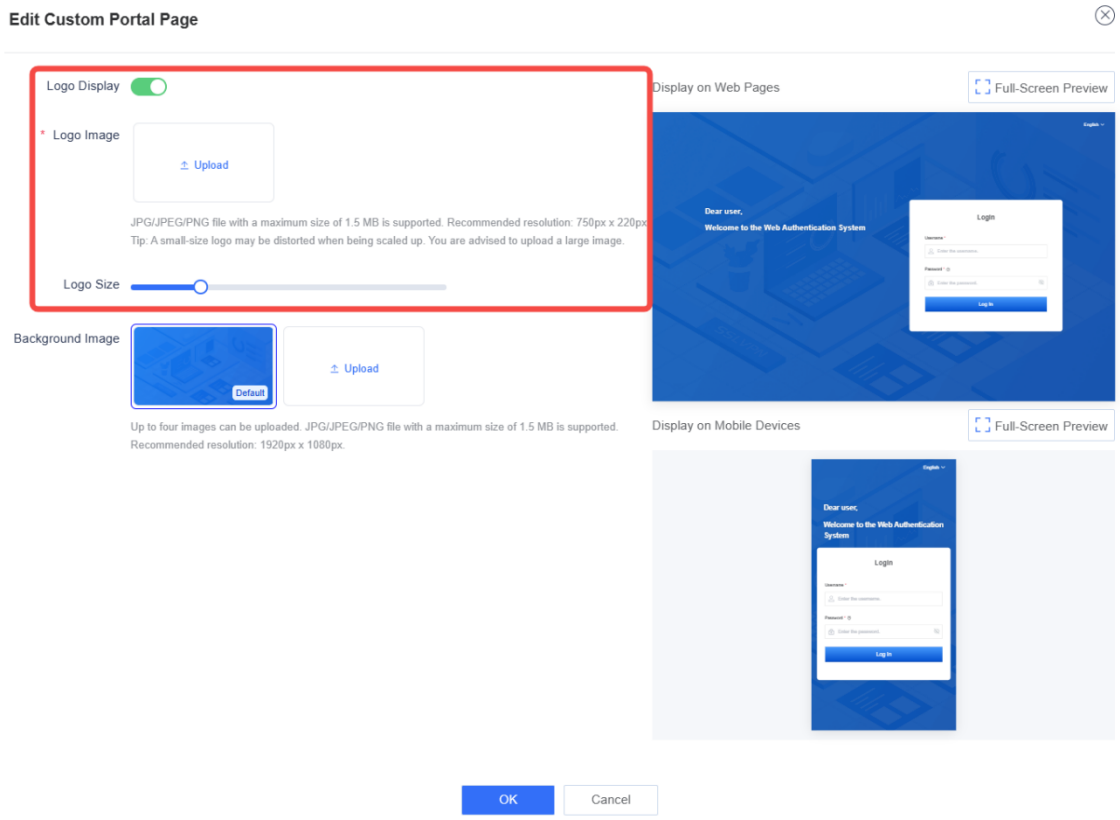
Note

Click **Preview** to preview the portal authentication page. If the custom portal authentication page is not required, retain the default style.

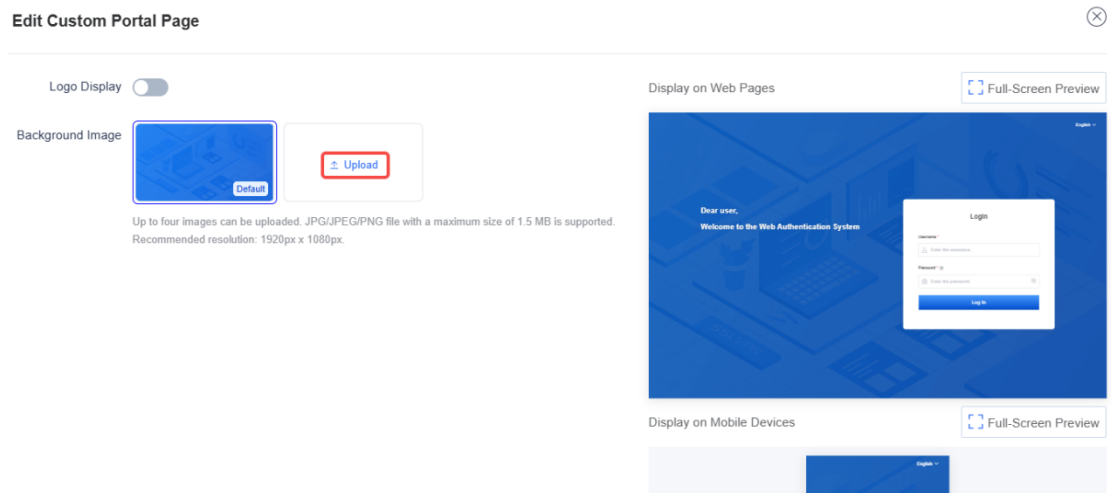
a To display a logo, toggle on **Logo Display**, upload a logo image, and adjust the logo size.

Note

- Only one logo image is supported. To change the logo image, click **Upload Again** to upload another image to overwrite the original image.
- If you do not want to display the logo, toggle off **Logo Display**.



a A default background image is provided. You can click **Upload** to customize the background image.



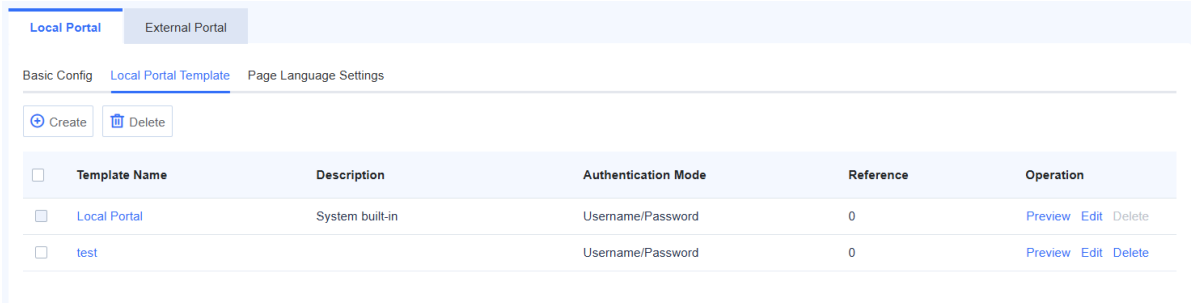
b Click **OK**.

Note

You can click **Full-Screen Preview** at any time during the configuration to view the visual style configuration in full-screen mode.

(5) After confirming that the configuration is correct, click **Save** to save the configuration of the local portal template.

Follow-up Procedure



- Click **Preview** to view the local authentication pages configured in a template, including the web and mobile authentication pages.
- Select a template to be deleted and click **Delete**. The built-in template cannot be deleted.
- If the **Reference** field is not set to 0 for a template, click **View** to view the authentication policy that references the template.
- A referenced template cannot be deleted. To delete the template, you need to remove the reference to this template in an authentication policy.

3. (Optional) Page Language Settings

Application Scenario

The device provides a page language configuration feature, which can be used to implement multi-language display for the local portal authentication module of the firewall. You can flexibly set languages as required. When users perform portal authentication, the device redirects the user's request to the built-in portal authentication page and replaces the language of the page with the configured language. The device has multiple built-in language packages and also supports the addition of custom language packages to meet the localization requirements of users in different regions.

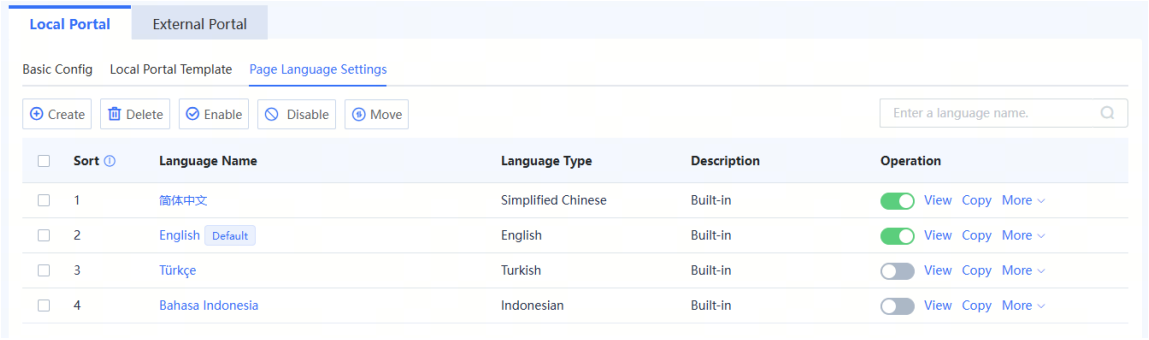
Precautions

- Up to five language packages can be enabled simultaneously on the device. The authentication page automatically loads the configured default language. Users can also select other enabled languages from the language switching list on the portal authentication page.
- Different versions support different built-in languages. If a language is not supported by the current version but is selected in language package configuration, the page content is displayed in English by default.

Procedure

(1) Choose **Object** > **User Authentication** > **Authentication Template** > **Local Portal** > **Page Language Settings**.

The device supports four built-in languages: English, Chinese, Turkish and Indonesian. The built-in languages of the system are for viewing only and cannot be edited or deleted.



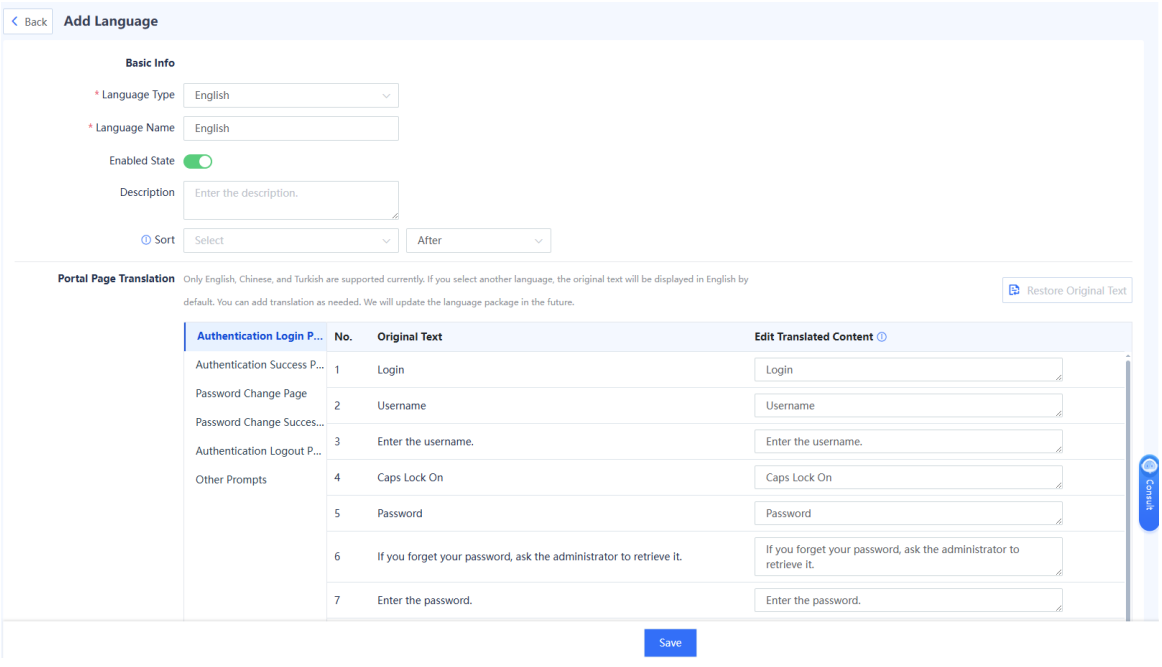
(2) Click **Create**.



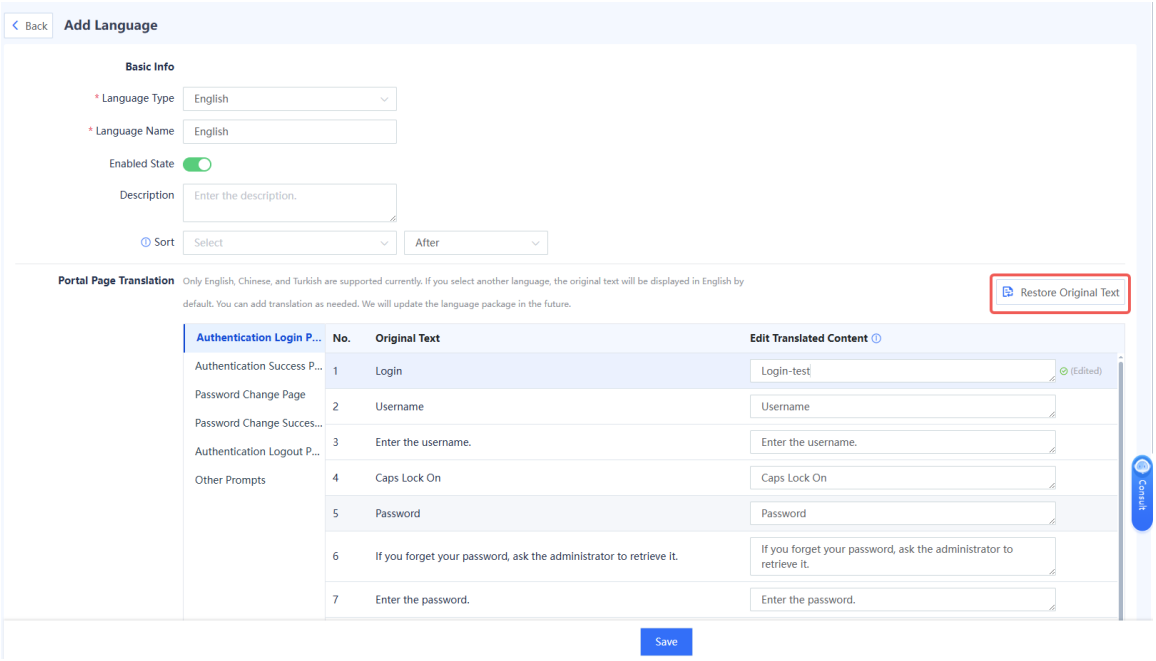
(3) Configure the language type, language name, enable state, sorting order, and portal page translation content based on actual services.

Note

- Portal authentication pages include the login page, authentication success page, password change page, password change success page, authentication logout page, and other prompts. The prompts and field names on the page are displayed based on the translation content of the language package.
- When editing translation content, ensure that the phrase length does not exceed 31 bytes and the sentence length does not exceed 255 bytes.

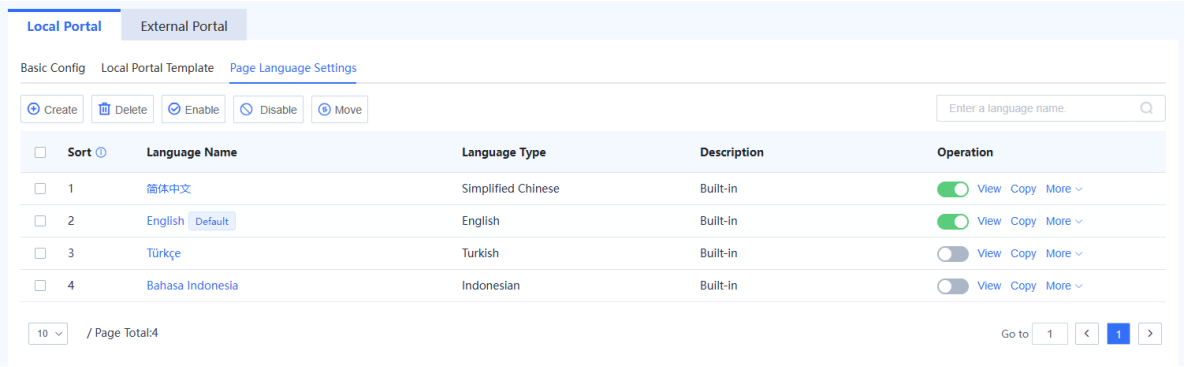


(4) (Optional) Click **Restore Original Text** to restore the translated content to the original text.



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

Follow-up Procedure



- Select the languages to be deleted and click **Delete** to delete the languages. Built-in languages cannot be deleted.
- Select languages and click **Enable** or **Disable** to enable or disable the languages on the authentication page. If a language is enabled, it is displayed in the language switching list for selection. If disabled, it is not displayed in the language switching list for selection.
- Click **Move** and select **Top**, **Move Up One Row**, **Move Down One Row**, or **Move to Specific Location** to change the display order of the languages in the language switching list on the portal authentication page.
- For a custom language, click **Edit** in the **Operation** column and modify parameters such as the language name, enabled state, description, and translation content.
- Click **Copy** in the **Operation** column of a language to copy its configuration. Then, you can modify other parameters to create a new language.

- Click **More** in the **Operation** column of a language and select **Set to Default** to configure the current language as the system default language.
- In the search box, enter a keyword to search for language names.

5.8.10 Authentication Template - WiFiDog Authentication

Application Scenario

The device can use the WiFiDog protocol to interact with external portal servers, such as the Ruijie Cloud server, to implement various authentication functions including SMS authentication and WeChat authentication. After WiFiDog authentication is enabled, users need to complete authentication operations for normal network access according to the instructions on the web page after connecting to Wi-Fi.

Prerequisites

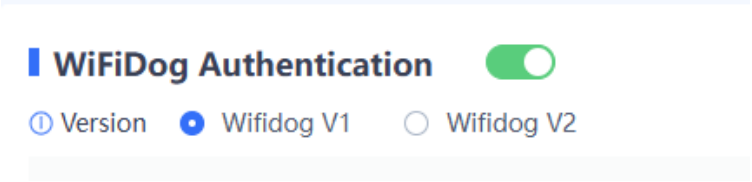
- Authentication rules and other configurations have been set on external portal servers.
- The DNS server has been correctly configured on the device to resolve the domain names of portal servers.

Procedure

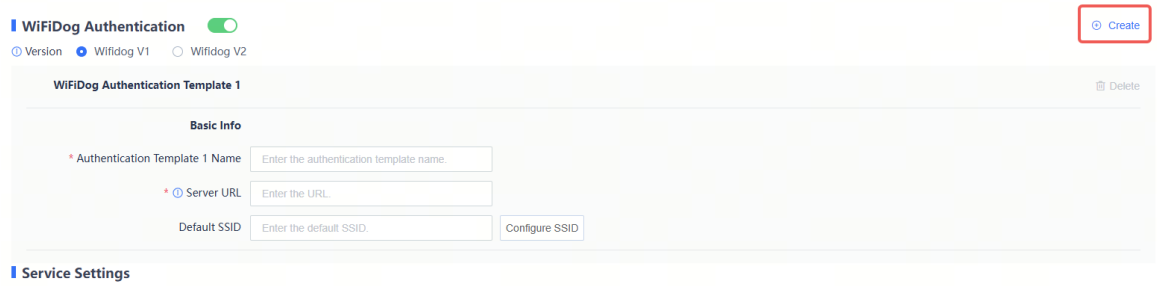
(1) Choose **Object** > **User Authentication** > **Authentication Template** > **External Portal**.

(2) Toggle on to enable WiFiDog authentication and select a WiFiDog protocol version.

The major difference between WiFiDog v1 and WiFiDog v2 is that the URL parameters of the redirected authentication page are encrypted by default in WiFiDog v2, but are not encrypted by default in WiFiDog v1 (unless a custom parameter that needs to be encrypted is specified).



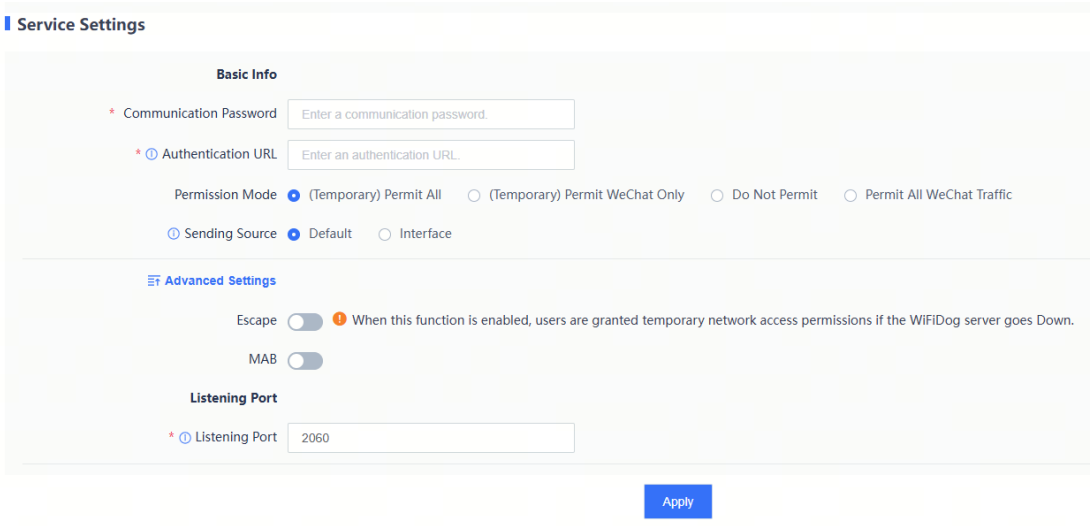
(3) Set authentication template parameters as required. Click **Create** in the upper right corner to create multiple authentication templates.



Item	Description	Remarks
Authentication Template 1 Name	Name of a WiFiDog authentication template.	[Example] wifidog
Server URL	URL of the authentication page on the	

Item	Description	Remarks
	authentication server.	[Example] http://maccauth.ruijie.com.cn/auth/servlet/standardAuthServlet/portal/
Default SSID	SSID carried in the redirect URL by default. On the portal server, if the authentication rules are configured to take effect based on SSIDs, the redirect URL accessed by terminals must carry the corresponding SSID parameter. Otherwise, the terminals cannot be redirected to the authentication page. When constructing the redirect URL, the device first searches for the SSID that corresponds to the IP address of the terminal that initiates the authentication request. (Click **Configure SSID** to view and configure the mappings between the network segments of terminal addresses and SSIDs.) If no SSID is matched, the default SSID value is carried in the URL. If no default SSID is specified, the SSID in the URL is empty.	The value must be the same as the SSID associated with the authentication rule configured on the portal server. [Example] test1

(4) Configure service parameters.



Item	Description	Remarks
Basic Info		

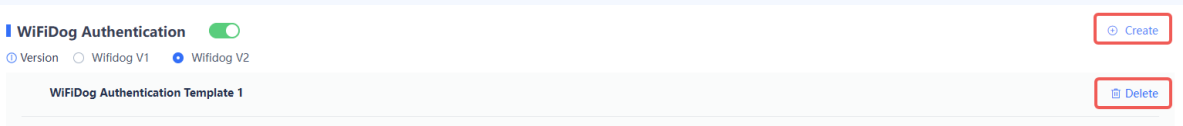
Item	Description	Remarks
Communication Password	Password for the device to communicate with the WiFiDog server.	The value must be the same as the password configured on the server. Otherwise, authentication fails. [Example] ruijie
Authentication URL	URL for the device to communicate with WiFiDog server during WiFiDog authentication (for example, to obtain the user authentication result).	[Example] http://maccauth.ruijie.com.cn/auth/servlet/standardAuthServlet/
Permission Mode	Configure a mode for the device to permit user traffic. ● **(Temporary) Permit All**: During terminal authentication, when the device receives a temporary permit request from the terminal, it temporarily permits all traffic from the terminal to allow Internet access. If the user fails to be authenticated during the temporary permit period, the user cannot continue to access the Internet. ● **(Temporary) Permit WeChat Only**: During terminal authentication, when the device receives a temporary permit request from the terminal, it temporarily permits WeChat traffic to allow the terminal to access the WeChat application. If the user fails to be authenticated during the temporary permit period, the user cannot continue to access the WeChat application. This mode applies to WeChat-based authentication scenarios and allows users to access the WeChat application to complete authentication operations. ● **Do Not Permit**: The device blocks all traffic from unauthenticated users. ● **Permit All WeChat Traffic**: The device permits the traffic of the WeChat application in any period to allow terminals to access the WeChat application even if the terminals are unauthenticated.	[Example] Do Not Permit
Sending Source	Source IP address for the device to communicate with the WiFiDog server. Click **Interface** to specify an interface for the device to communicate with the server. If **Default** is selected, the outbound interface determined according to the routing result is used as the sending source.	[Example] Default
Advanced Settings		

Item	Description	Remarks
Escape	After this function is enabled, if an exception occurs on the WiFiDog server (the device detects that the server status is Down), temporary network access permissions are granted to users. That is, users can directly access network resources without authentication. When the server recovers, users who were allowed to access are forced to go offline, and users need to be re-authenticated to go online.	[Example] Enabled
MAB	After this function is enabled, a user only needs to be authenticated once, and can subsequently go online without authentication.	[Example] Enabled
Listening Port	Port number for the device to listen on WiFiDog packets.	The value must be the same as that on the server. You are advised to keep the default value unless otherwise specified. [Example] 2060

(5) Verify that the configuration is correct and click **Apply**.

Follow-up Procedure

Click **Create** in the upper right corner to add a WiFiDog authentication template or click **Delete** to delete a specific template. If only one authentication template exists, it cannot be deleted.



5.8.11 Authentication Settings

1. 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

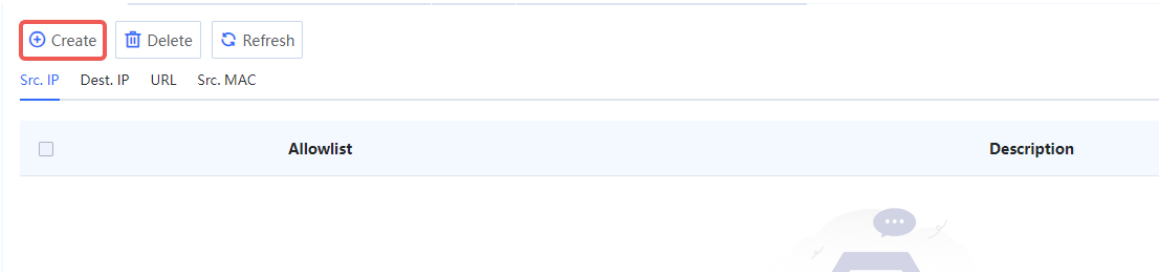
go online without being authenticated.

- **URL**: After a URL allowlist is configured, all users can access URLs in the allowlist without being authenticated.

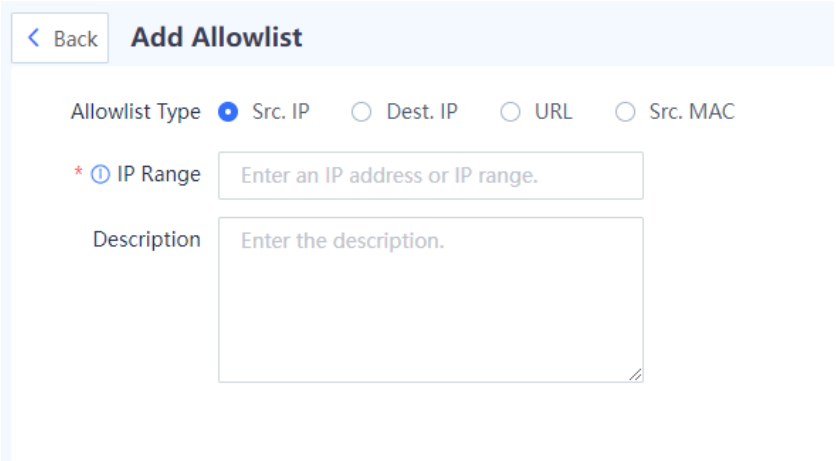
Procedure

(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 external network.

2. SSO

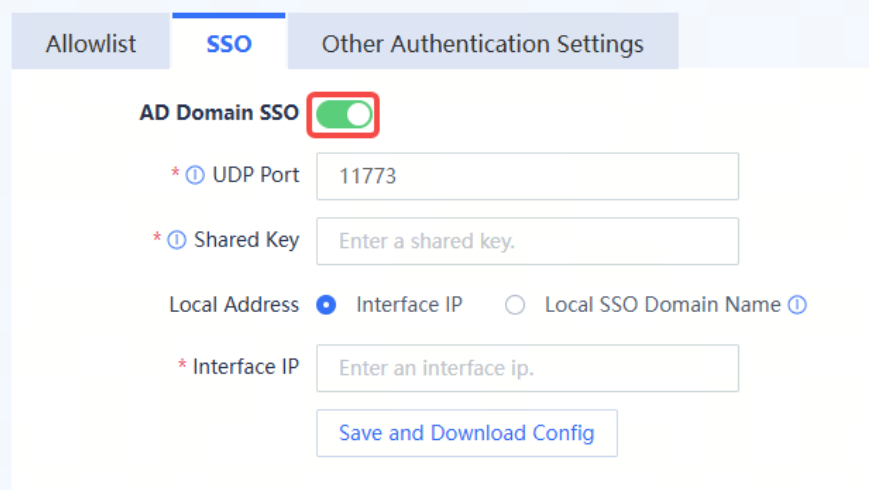
Application Scenario

SSO allows a user to access multiple application systems that require authentication and trust each other after the user logs in to one of the systems once. In a typical AD domain scenario, an LDAP server (AD domain server) is deployed to manage and authenticate user identity information. In this case, you can configure the AD domain SSO function for the device to authenticate user login information and PC users can go online on the device and access network resources after being authenticated by the AD domain server without any secondary authentication such as web authentication.

Procedure

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

(2) Toggle on to enable AD domain SSO.



Item	Description	Remarks
UDP port	Service port for the firewall to receive user login and account cancelation information.	[Example] 11773
Shared Key	Key used by the firewall and the user PC to encapsulate exchange information.	[Example] Test12
Local Address	Local address used by the device to connect to the PC and receive user information. ● **Interface IP**: The device uses the interface IP address to communicate with the PC. When this option is selected, the script deployed on the AD domain server becomes invalid if the interface IP address of the device changes. In this case, user login in SSO mode may fail. ● **Local SSO Domain Name**: The device uses the local SSO domain name to communicate with the PC. Using the domain name as the local address can prevent script invalidation caused by the interface IP address change, reducing the risk of SSO login failures. Ensure that DNS packets from terminals pass through the local device or the mapping between the domain name and local device IP address is configured on the external DNS server. Ensure that the user's PC can resolve the AD domain name and local SSO domain name.	[Example] sso.device.local

(3) Click **Save and Download Config** to save the configuration and download it to the local device. Deploy the downloaded configuration script to the AD domain authentication server.

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

3. 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.
- Privacy Statement: Choose whether to enable privacy statement. After this function is enabled, you must select **User Data Processing Policy** in the user authentication system. After this function is enabled, you need to upload a privacy statement file (only the TXT file in UTF-8 format is supported and the file size cannot exceed 64 KB).
- Single/Dual Stack: Specify whether to enable the function of permitting IPv6 packets when IPv4 authentication is performed (also known as IPv4/IPv6 dual-stack authentication). The IPv4 authentication and IPv6 bypass mode applies to scenarios where the authentication client supports IPv4/IPv6 dual stack and needs to access both IPv4 and IPv6 networks. After this function is enabled, IPv6 users can reuse authentication results of IPv4 users for the same terminal. That is, if a user gets online through IPv4 address authentication, the IPv6 request corresponding to the MAC address will also be allowed to pass through (both the user's IPv4 address and IPv6 address are in online state). The user terminal needs to be authenticated only once to access network resources of both IPv4 and IPv6 protocols.

  Caution
  - The IPv4 authentication and IPv6 bypass features are not supported in Layer 3 environments.
  - Real-name synchronization users do not support IPv6 users reusing IPv4 authentication results, and after IPv4 user login information is synchronized to the device, the corresponding IPv6 user will not go online.
  - After you enable Allow IPv6 Address for IPv4 Authentication, ensure that the IPv6 address of the user is included in the authentication policy with the action set to Authentication; otherwise, the online status of the user is not displayed in the online user list.

- IP-MAC binding mode: After this function is enabled, the system automatically records the IP address and MAC address of a terminal (that is, the IP-MAC binding record) when the terminal is successfully authenticated and goes online. When processing Internet access traffic of users, the system checks the validity of the traffic based on the recorded information. Only when the source IP address and source MAC address of the traffic match the information of the authenticated terminal (IP-MAC binding record), the traffic is considered as the valid traffic of the authenticated user and is released. This function prevents unauthorized terminals from bypassing authentication by changing IP addresses of authenticated terminals to those of unauthorized terminals.

  Caution
  - IP-MAC binding can be enabled only on Layer 2 networks. Otherwise, network exceptions may occur on clients.
  - Traffic of authentication-free users is directly permitted without being affected by the IP-MAC address binding mode.
  - When an end user goes offline, the system automatically unbinds the IP address and MAC address and deletes the binding record.

- HTTPS authentication redirect: enables or disables HTTPS traffic redirection. During user authentication, the system by default redirects HTTP and HTTPS traffic of users through a proxy. However, due to the encryption feature of HTTPS traffic, the HTTPS proxy process may generate large performance metrics. You can disable this function to redirect only HTTP traffic but not HTTPS traffic.
- Configure SSID: Configure the mapping between terminal address network segments and SSIDs. During WiFiDog web-based authentication, the NAS searches for the SSID matching the IP address of a terminal requesting authentication and uses the SSID as the SSID in the redirection URL. If no matching SSID is found, the default SSID preset in the authentication template is carried in the URL.

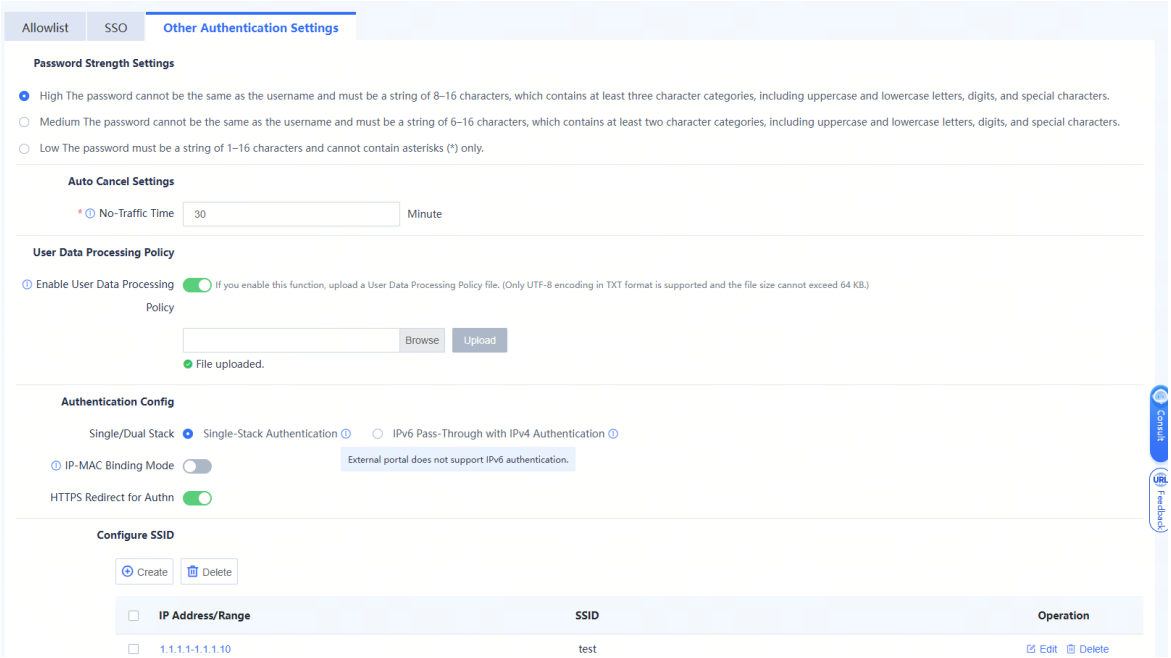
Note

If no network segment SSID is configured and no global default SSID is specified in the authentication profile, the SSID in the URL is empty. For details about WiFiDog authentication configuration, see 5.8.10 Authentication Template - WiFiDog Authentication.

Procedure

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

(2) Configure the password complexity as required, and set the automatic logout function for MAB traffic and privacy statement.



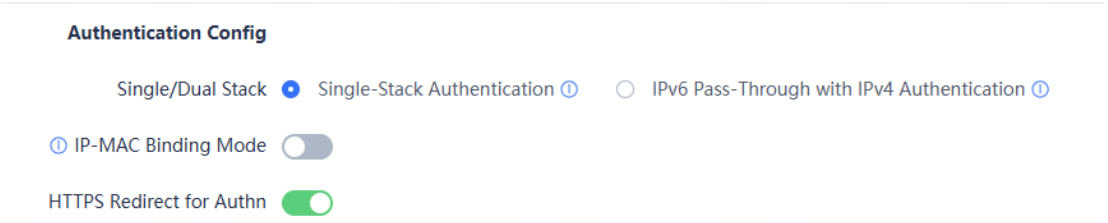
Note

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 5.8.2 2. Configuring Users.

(3) In Authentication Settings, configure whether to enable dual-stack authentication (IPv4 authentication and IPv6 bypass), whether to enable IP-MAC binding mode, and whether to enable HTTPS authentication redirect.

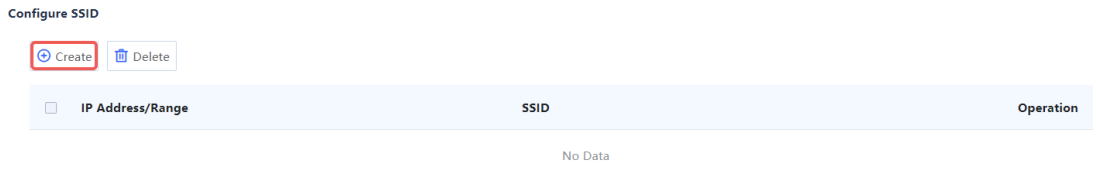
Caution

- In single-stack authentication mode, the external portal server does not support IPv6 authentication. If you need to use the external portal server to implement IPv6 user authentication, enable the dual-stack authentication function.
- If a dual-stack user goes offline through the IPv4 stack, the IPv6 stack of the user also goes offline. If IPv6 users go online through non-dual-stack authentication (they go online separately), the status of IPv4 users will not affect the online status of IPv6 users.
- For authentication clients that support IPv4/IPv6 dual stack, ensure that the IPv6 user addresses are included in the authentication scope when configuring an authentication policy. Otherwise, IPv6 access traffic of the clients will be directly released because it cannot match the authentication policy (that is, it matches the default authentication-free policy), and there is a risk that clients bypass authentication.

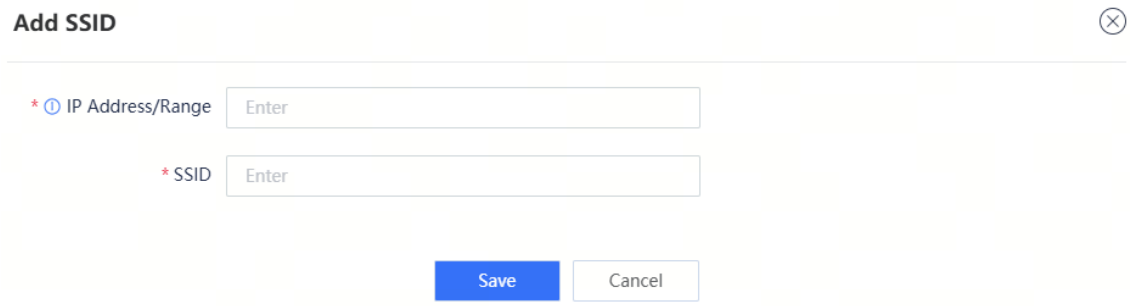


(4) (Optional) Configure the mapping between terminal address network segments and SSIDs.

a Click **Create**.



b Enter the IP address and SSID.



Item	Description	Remarks
IP Address/Range	Specify the IP address range of addresses to be assigned to terminals.	The following three formats are supported: ● Single IP address: 192.168.1.1 ● IP address range: 192.168.1.1–192.168.1.10 ● IP network segment: 192.168.1.0/24
SSID	SSID to which the terminal connects.	[Example] Test

c Click **Save**.

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

5.8.12 RADIUS Authentication Server

Application Scenario

In a scenario where a firewall functions as an SSL VPN gateway or web authentication is performed, when server authentication is required, you need to configure user identity information on the RADIUS server and add the RADIUS server on the firewall first.

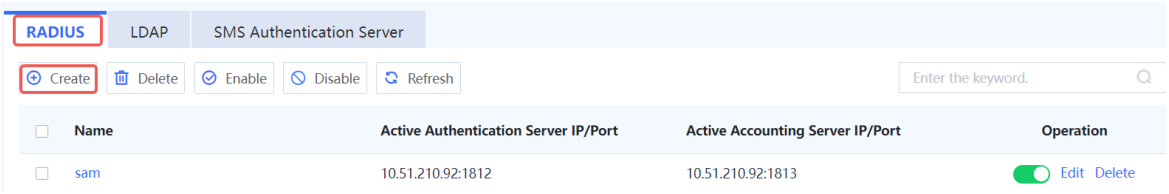
Precautions

- Ensure that the firewall can communicate with the authentication server. Otherwise, authentication may fail.
- Currently, accounting is not supported.
- In PPTP, L2TP, and PPPoE authentication scenarios where user information authentication is preferentially performed by the RADIUS server, if the primary RADIUS authentication server is offline, adjust the timeout duration of the RADIUS authentication server to ensure that the detection duration is less than 15 seconds. That is, the value of "Response timeout duration (seconds)" + "retransmission times" x "Response timeout duration (seconds)" on the RADIUS server must be less than 15 seconds. Otherwise, authentication may fail.

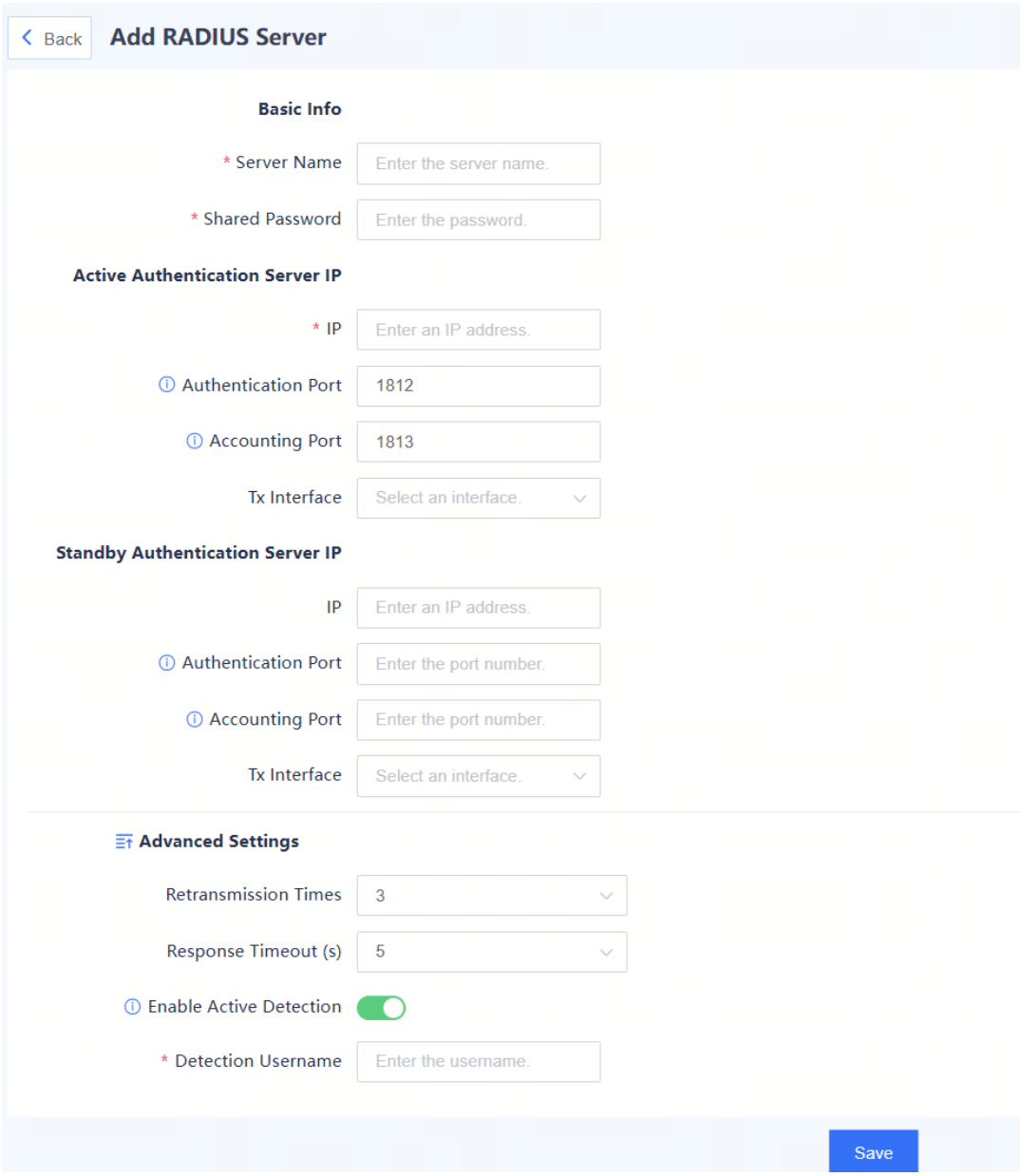
Procedure

(1) Choose **Object** > **User Authentication** > **Authentication Server** and click the **RADIUS** tab.

(2) Click **Create**.



(3) Configure the server.



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

Item	Description	Remarks
Active Authentication Server	Authentication server that performs authentication. ● **IP**: IP address of the authentication server. ● **Authentication Port**: Port on the authentication server that provides the authentication service. ● **Accounting Port**: Port on the authentication server that provides the accounting service. ● **Tx Interface**: Interface on the firewall for sending authentication packets.	N/A
Standby Authentication Server	When the active authentication server fails or has no user information, the standby authentication server performs authentication. ● **IP**: IP address of the authentication server. ● **Authentication Port**: Port on the authentication server that provides the authentication service. ● **Accounting Port**: Port on the authentication server that provides the accounting service. ● **Tx Interface**: Interface on the firewall for sending authentication packets.	N/A
Advanced Settings		
Retransmission Times	Maximum times of resending authentication request packets when the firewall does not receive a reply packet from the authentication server. If the retransmission times configured for both the active and standby servers are reached, the server is deemed as unreachable and the authentication fails.	[Example] 3
Response Timeout	Timeout period in seconds for the firewall to receive a reply packet from the authentication server. When the timeout period expires, the firewall sends a request packet again.	[Example] 5
Enable Active Detection	After this function is enabled, the device sends a RADIUS packet every 10 minutes to detect whether the server can be connected.	-
Detection Username	Username carried in the RADIUS packet. You are advised to set it to the active detection username provided by the server. Otherwise, the server will generate a large number of authentication failure logs.	-

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

Follow-up Procedure

- To delete authentication servers in a batch, select the servers and click **Delete**.
- To disable authentication servers in a batch, select the servers and click **Disable**.
- To enable authentication servers in a batch, select the servers and click **Enable**.

5.8.13 LDAP Authentication Server

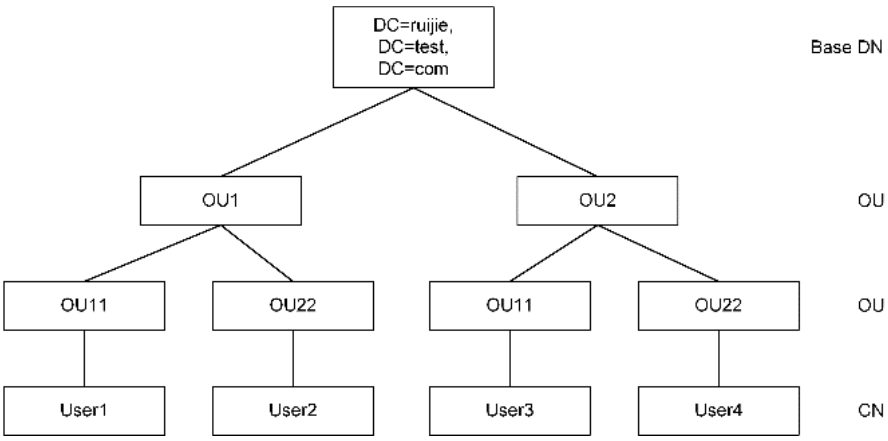
1. Overview

The Lightweight Directory Access Protocol (LDAP) is a TCP/IP-based protocol that does not support accounting. LDAP is based on the server/client structure, and all directory information is stored on the LDAP server. The LDAP server stores user data in a hierarchical directory structure.

As shown in Figure 5-1, the LDAP directory has a tree structure, and each entry has a unique Distinguished Name (DN).

- Domain Controller (DC): indicates the domain to which an object belongs.
- DN: indicates the path of an object on the server. In Figure 5-1, the DN of User 1 in the directory is CN=User1, OU=OU11, OU=OU1, DC=ruijie, DC=test, DC=com.
- Base DN: indicates the root DN. In Figure 5-1, the base DN is DC=ruijie, DC=test, DC=com.
- Organization Unit (OU): indicates the organization to which an object belongs. In Figure 5-1, the OU to which User 1 belongs to is OU=OU11, OU=OU1.
- Common Name (CN): indicates the object name.

Figure 5-1 LDAP Directory Structure



2. Configuring the LDAP Server

Application Scenario

In scenarios where server authentication is required (for example, a firewall functions as an SSL VPN gateway or web authentication is performed), you need to configure user identity information on the LDAP server and add the LDAP server on the firewall first.

Precautions

- Ensure that the firewall can communicate with the authentication server. Otherwise, authentication may fail.
- If a security group has been associated with users on the LDAP server, the security group is configured as the user tag during import to the device, and the users in the security group are also imported to the device. If a security group is not associated with users, the security group is ignored and is not imported to the device.

For example, a security group **group1** exists on the LDAP server and a user **user1** exists in the security group. During import to the device, **group1** is added as a user tag on the **User Tag** page, and **user1** is added as a user (with the user tag of **group1**) on the **User Management** page.

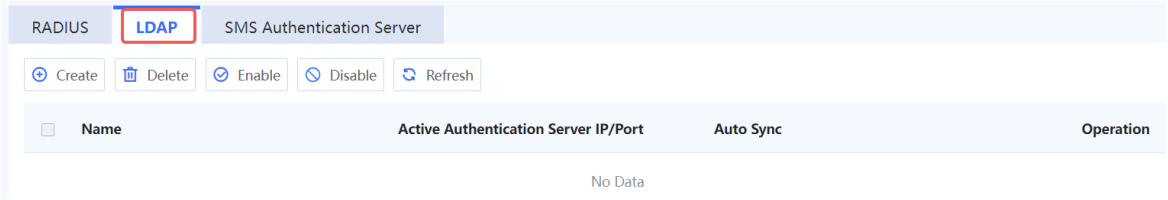
Prerequisites

- You have obtained the administrator account and password of the authentication server.

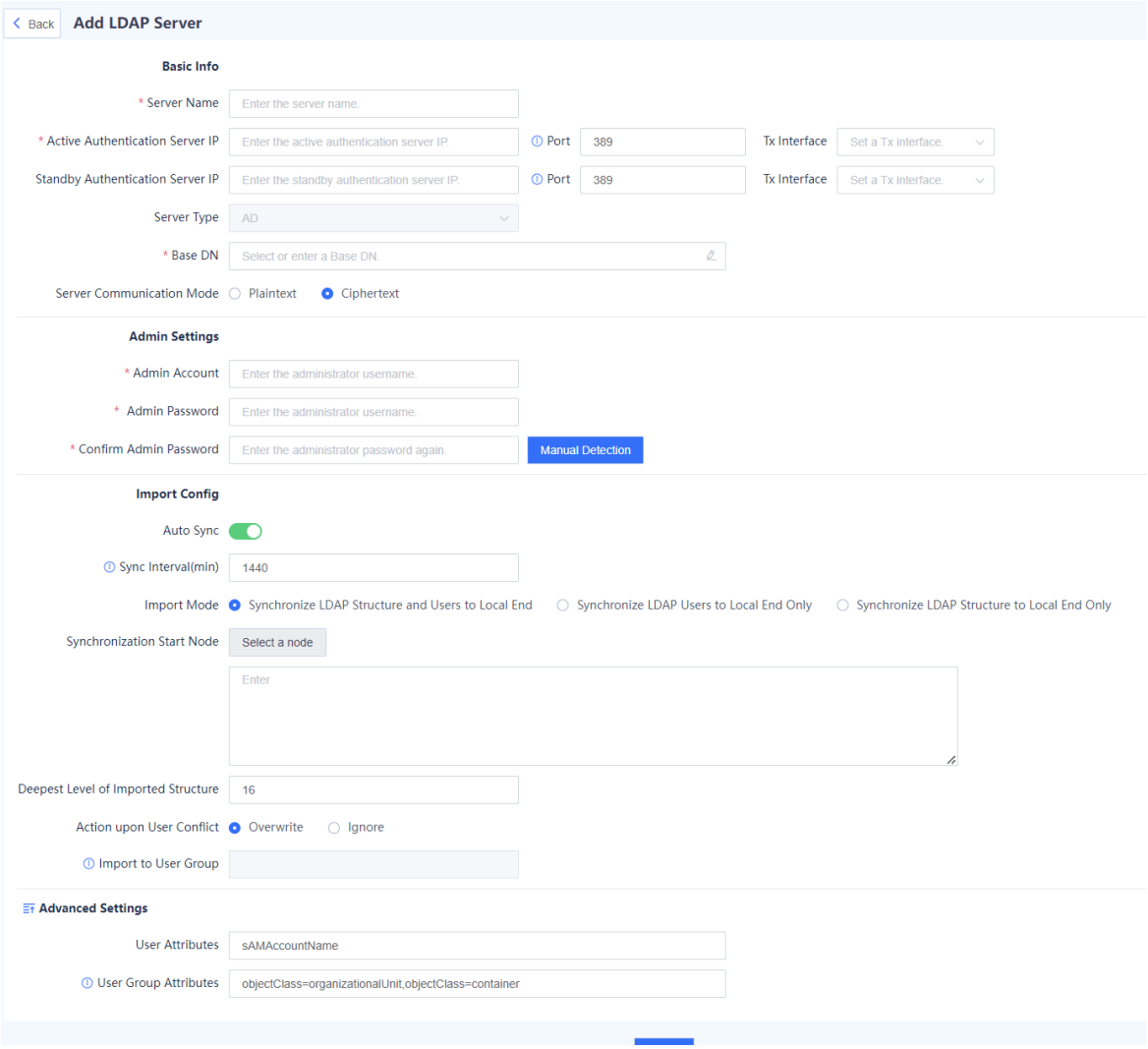
Procedure

(1) Choose **Object** > **User Authentication** > **Authentication Server** and click the **LDAP** tab.

(2) Click **Create**.



(3) Configure the server.



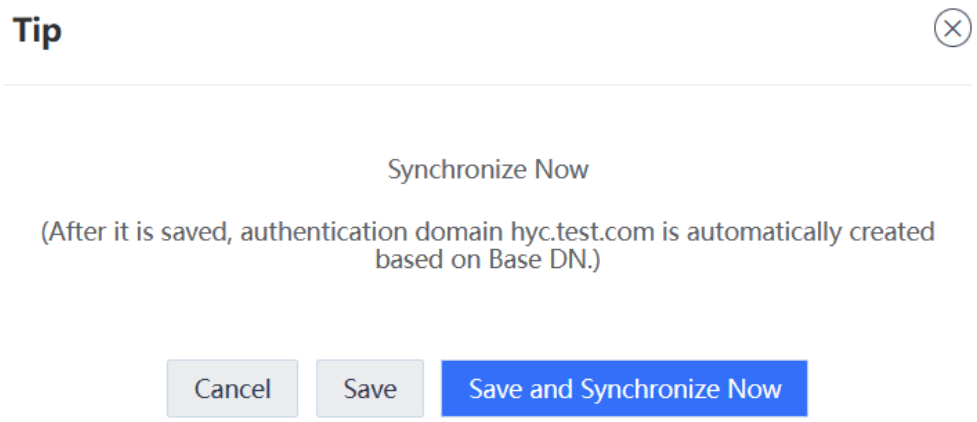
Item	Description	Remarks
Basic Info		
Server Name	LDAP server name.	[Example] server_1
Active Authentication Server	Authentication server that performs authentication. ● **IP**: IP address of the authentication server. ● **Port**: Port on the authentication server that provides the authentication service. ● **Tx Interface**: Interface on the firewall for sending authentication packets.	N/A
Standby Authentication Server	When the active authentication server fails or has no user information, the standby authentication server performs authentication. ● **IP**: IP address of the authentication server. ● **Port**: Port on the authentication server that provides the authentication service. ● **Tx Interface**: Interface on the firewall for sending authentication packets.	N/A
Server Type	Type of the LDAP server. Currently, only the Active Directory (AD) type is supported.	N/A
Base DN	Root node (base directory) of the LDAP server. The LDAP server searches for entries from this node downwards.	Select a value from the drop-down list or enter a value.
Server Communication Mode	Whether to encrypt data carried in LDAP packets during communication between the device and LDAP server. ● **Plaintext**: Data is not encrypted and is transmitted in plaintext. ● **Ciphertext**: Data is encrypted and transmitted in ciphertext.	[Example] Plaintext
Admin Settings		
Admin Account	Administrator account of the LDAP server.	[Example] Administrator@test.com.cn
Admin Password	Administrator password of the LDAP server.	[Example] ruijie@123

Item	Description	Remarks
Confirm Admin Password	Confirm the administrator password. Click **Manual Detection** to check whether the authentication server can be successfully connected.	N/A
Import Config		
Auto Sync	Whether to enable automatic data synchronization from the LDAP server to the local device at an interval.	[Example] Enable
Sync Interval (min)	Interval between two consecutive LDAP user information synchronizations.	[Example] 1440
Import Mode	Mode of data synchronization from the LDAP server to the firewall: ● **Synchronize LDAP Structure and Users to Local End**: Synchronize the organization structure (user groups) and users from the LDAP server to the local device. ● **Synchronize LDAP Users to Local End Only**: Synchronize users from the LDAP server to the local device and do not synchronize the organization structure. ● **Synchronize LDAP Structure to Local End Only**: Synchronize the organization structure (user groups) from the LDAP server to the local device and do not synchronize users. Users can be imported only to the authentication domain with the same name as the authentication server. Choose **Object** > **User Authentication** > **User Management,** select the authentication domain, and check imported user information.	[Example] Synchronize LDAP Structure and Users to Local End
Synchronization Start Node	Start node for synchronization, indicating the directory level from which the server starts to synchronize data.	Click **Select a node** to select a node or enter node information.
Deepest Level of Imported Structure	Deepest structure level that can be imported from the server. The device imports data from top to bottom. For example, if the directory structure is **/111/222/333**, the device imports data at the **/111** level first.	[Example] 16

Item	Description	Remarks
Action upon User Conflict	If the imported user information already exists on the local device, you can choose to overwrite or ignore it. ● **Overwrite**: User information on the server overwrites the original user information. For example, if User 1 has been configured on the local device and information on User 1 is imported, the original configuration is overwritten. ● **Ignore**: Existing configuration on the local device prevails, and user information on the server is ignored.	[Example] Overwrite
Import to User Group	When you create an LDAP server, the device automatically creates an authentication domain with the same name. When you import user information, the information is automatically imported to the authentication domain with the same name.	It is automatically configured based on the base DN.
Advanced Settings		
User Attributes	Attributes that identify usernames on the server. For example, if **sAMAccountName** is set, the value of **sAMAccountName** of a user is deemed as the username, and data on users without **sAMAccountName** is not imported.	The default value is **sAMAccountName**. Use the default value unless otherwise specified.
User Group Attributes	Attributes for filtering the nodes of which the user group information needs to be imported.	[Example] objectClass=XXX,objectClass=XXX Use the default value unless otherwise specified.

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

The system prompts you to synchronize user information from the LDAP server immediately. You can click **Save and Synchronize Now** to start synchronization immediately, or click **Save** to save the configuration only.



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**.

5.8.14 SMS Authentication Server

Application Scenario

When the device is used for web authentication or acts as an SSL VPN virtual gateway, it can work with an SMS authentication server to implement SMS authentication on users, reducing the risk caused by username and password leaks and protecting intranet resources.

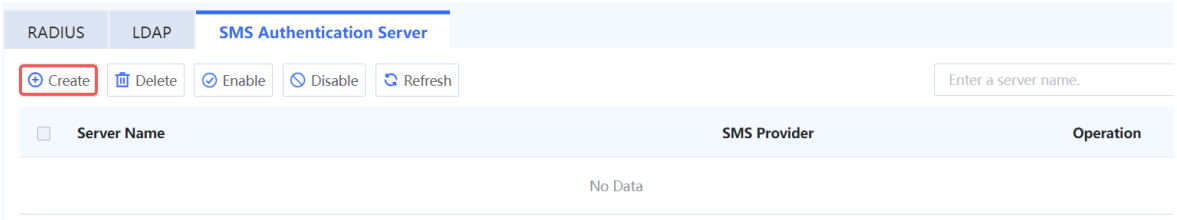
Prerequisites

- If the SMS service provider is Twilio, you need to register and configure your account on the Twilio SMS platform, including obtaining the account SID and authentication token and purchasing a mobile number.
- To enable SMS authentication, create a mobile phone user on the **User Management** page on the firewall web UI first. When SMS authentication is performed, Twilio sends SMS messages to the mobile number entered by the user.

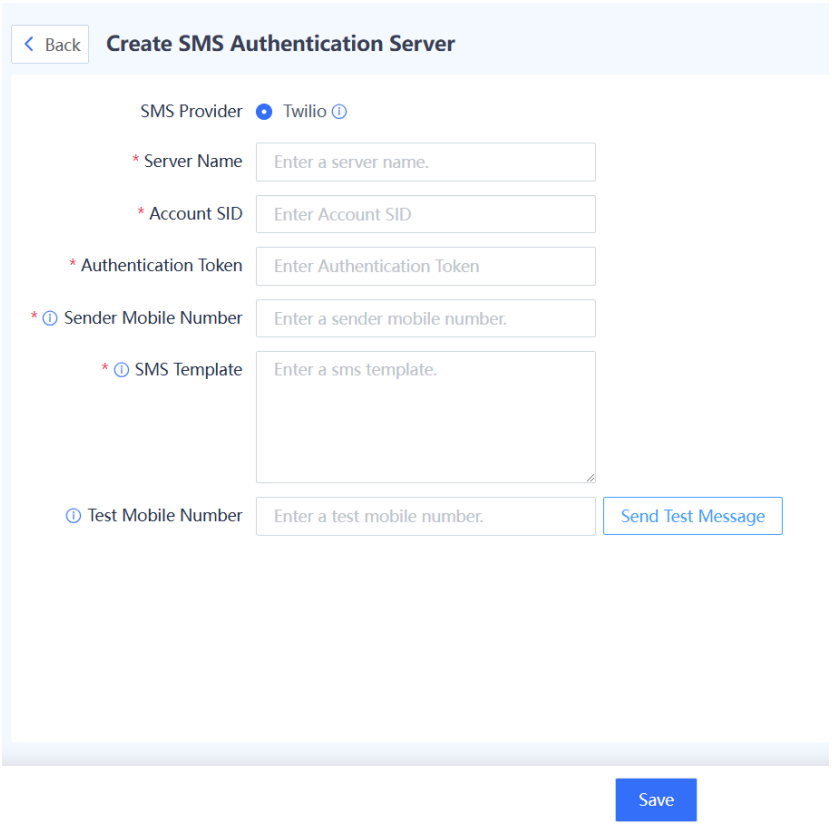
Procedure

(1) Choose **Object** > **User Authentication** > **Authentication Server** and click the **SMS Authentication Server** tab.

(2) Click **Create**.



(3) Configure interconnection parameters for the SMS authentication server.



Item	Description	Remarks
Twilio		
Server Name	SMS authentication server name.	[Example] server_1
Account SID	Account SID obtained from Twilio.	-
Authentication Token	Authentication token obtained from Twilio.	-
Sender Mobile Number	Mobile number purchased from Twilio.	-
SMS Template	You can configure custom content in the SMS message without application. The verification code will be attached to the end of the SMS content when the SMS message is sent.	-
Test Mobile Number	Mobile number used to check whether SMS messages can be properly received.	-

(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**.

5.9 Certificate Management

5.9.1 Overview

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

Local certificate: 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.

SSL 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.

5.9.2 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 and exchange the key with the SSL VPN gateway based on the digital certificate. If a non-CA certificate is provided, the client reports a certificate security alarm. To avoid such an alarm, import a trusted certificate issued by a CA.

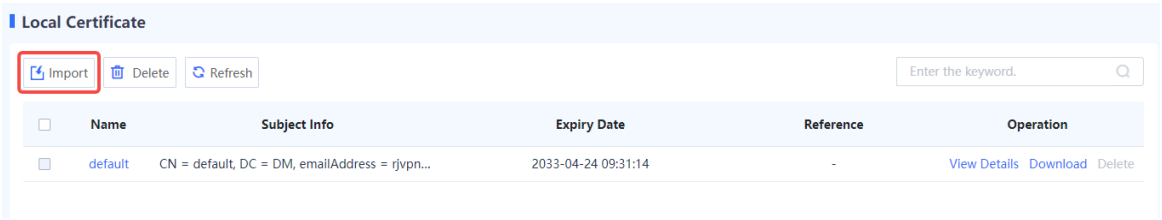
A firewall provides an untrusted self-signed certificate **default**. You can import a new local certificate as required.

For details about the SSL VPN gateway, see 6.9 SSL VPN.

Procedure

(1) Choose **Object** > **Certificate** > **Local Certificate**.

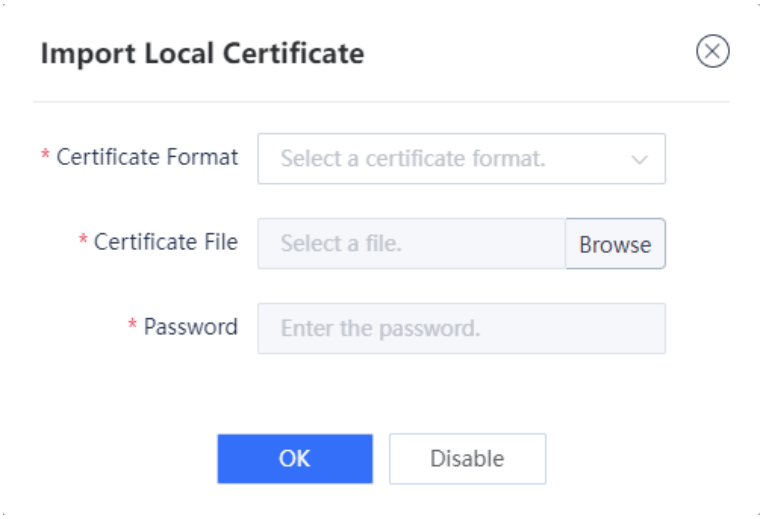
(2) Click **Import**.



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

Note

Up to 20 local certificates are supported.



Follow-up Procedure

- Click **Download** to download the corresponding certificate in .pem format.
- After certificate import, you can reference the local certificate when creating the virtual gateway.
- Click **View Details** to view details about the certificate.
- To delete a newly imported certificate, click **Delete**. The default certificate cannot be deleted.
- You can enter the certificate name in the search box in the upper right corner of the page to search for a certificate.

5.9.3 SSL Certificate

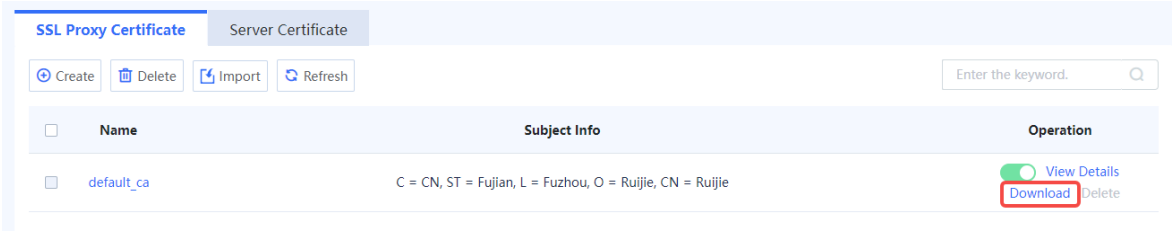
1. Configuring an SSL Proxy Certificate

Application Scenario

If HTTPS encrypted traffic needs to be decrypted and the SSL proxy mode is set to **Decrypt Internet access packets of terminals**, 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.

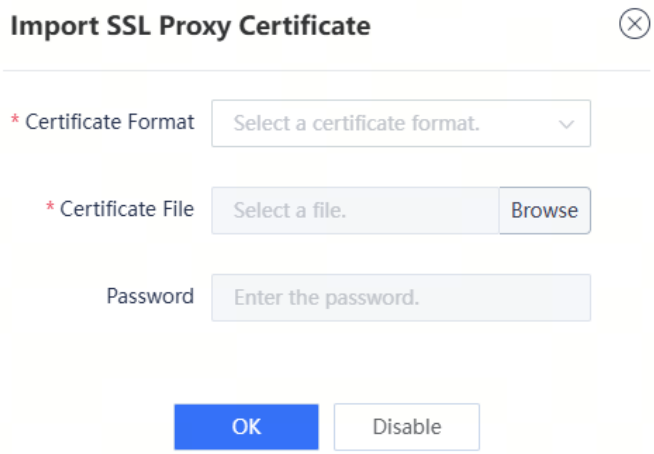


2. Importing an SSL Proxy Certificate

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



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



(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.	● The certificate with the .p12 or .pem suffix already contains the key. You need to specify the password of the certificate when importing the certificate. ● The certificate with the .crt suffix does not contain a key and a separate key file is required. When you import the certificate, specify the key file and password of the key file. [Example] P12

Certificate File	Imported SSL proxy certificate file.	Click **Browse** to select a certificate file to be uploaded from the local device.
Key File	Separate key file attached with the certificate.	The certificate file with the .crt suffix does not contain a key. You need to upload the key file and specify the password for the key file when importing the certificate.
Password	Password of the key file.	● Certificate with the .p12 or .pem suffix: You need to specify the password of the certificate when importing the certificate. ● Certificate with the .crt suffix: When you import the certificate, specify the key file and password of the key file.

Follow-up Procedure

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

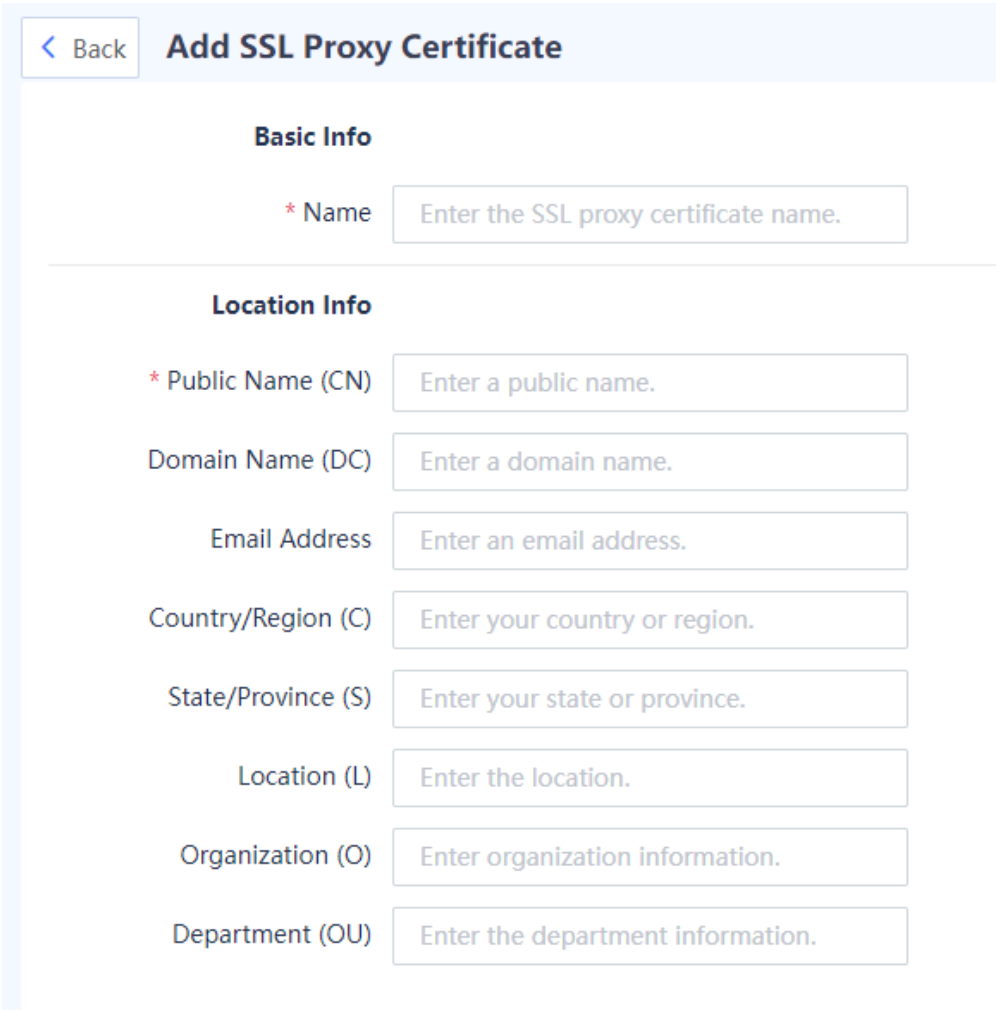


- Click **View Details** to view details about the SSL proxy certificate.
- To delete a newly imported SSL proxy certificate, click **Delete**. The default SSL proxy certificate cannot be deleted.
- You can enter the certificate name in the search box in the upper right corner of the page to search for 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.



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

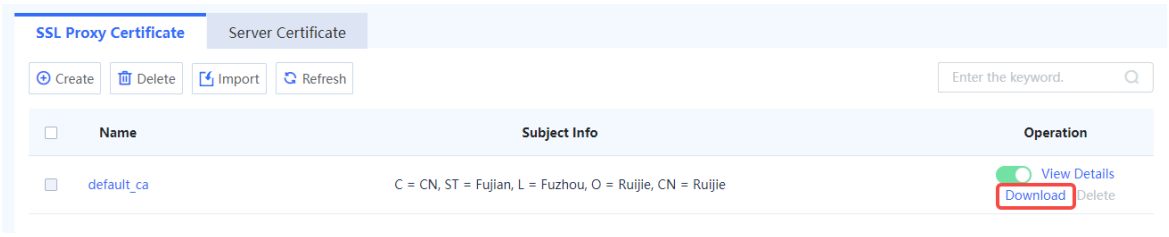
Item	Description	Remarks
Name	Name of the SSL proxy certificate.	[Example] local_ca
Public Name (CN)	Common name of the SSL proxy certificate.	[Example] Ruijie
Domain Name (DC)	Domain name of the certificate applicant.	[Example] www.abc.com.cn
Email Address	Email address of the certificate applicant.	[Example] test@ruijie.com.cn

Item	Description	Remarks
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.	[Example] Fujian
Location (L)	Location of the certificate applicant.	[Example] Fuzhou
Organization (O)	Organization of the certificate applicant.	[Example] Ruijie
Department (OU)	Department of the certificate applicant.	[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.

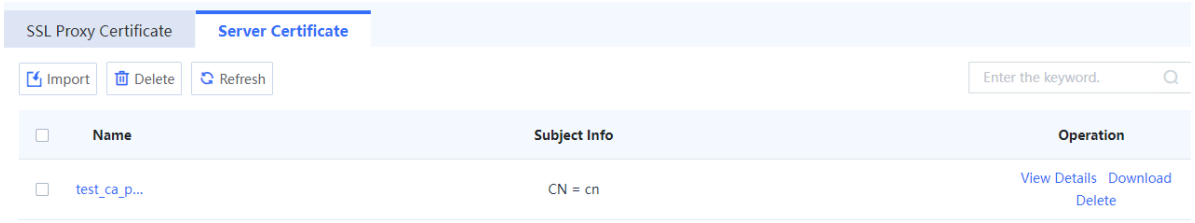
4. Importing a Server Certificate

Application Scenario

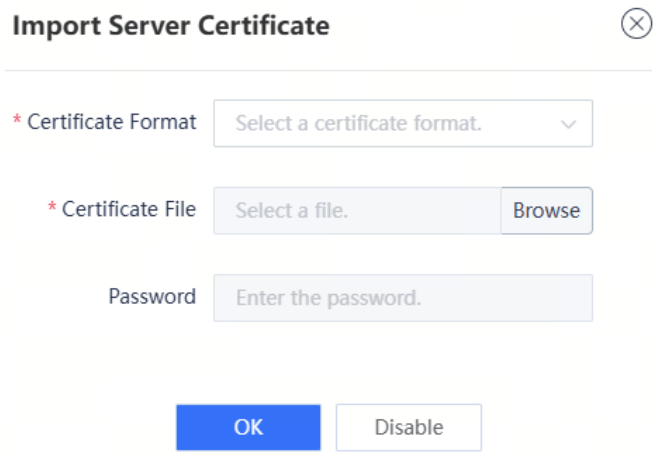
If HTTPS encrypted traffic needs to be decrypted and the SSL proxy mode is set to **Decrypt packets destined for LAN servers**, you must import a server certificate.

Procedure

(1) Choose **Object** > **Certificate** > **SSL Certificate** > **Server Certificate**.



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



(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.	● 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.

Item	Description	Remarks
Password	Password of the key file.	• Certificate with the .p12 or .pem suffix: You need to specify the password of the certificate when importing the certificate. • Certificate with the .crt suffix: When you import the certificate, specify the key file and password of the key file.

Follow-up Procedure

- Reference the imported server certificate in an SSL proxy policy for which the SSL proxy mode is set to **Decrypt packets destined for LAN servers**. For details, see 4.11 SSL Proxy.
- 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.

5.10 Content Template

5.10.1 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, POP3, SMB, IMAP and NFS.

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.

Note

RG-CF10S and RG-CF10S-LTE do not support the deep scan mode.

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 7.2.4 Activating the License.

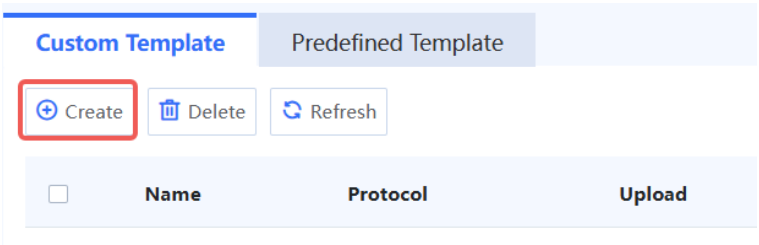
Note

- If the antivirus function is unauthorized, the virus protection function is unavailable.
- 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.

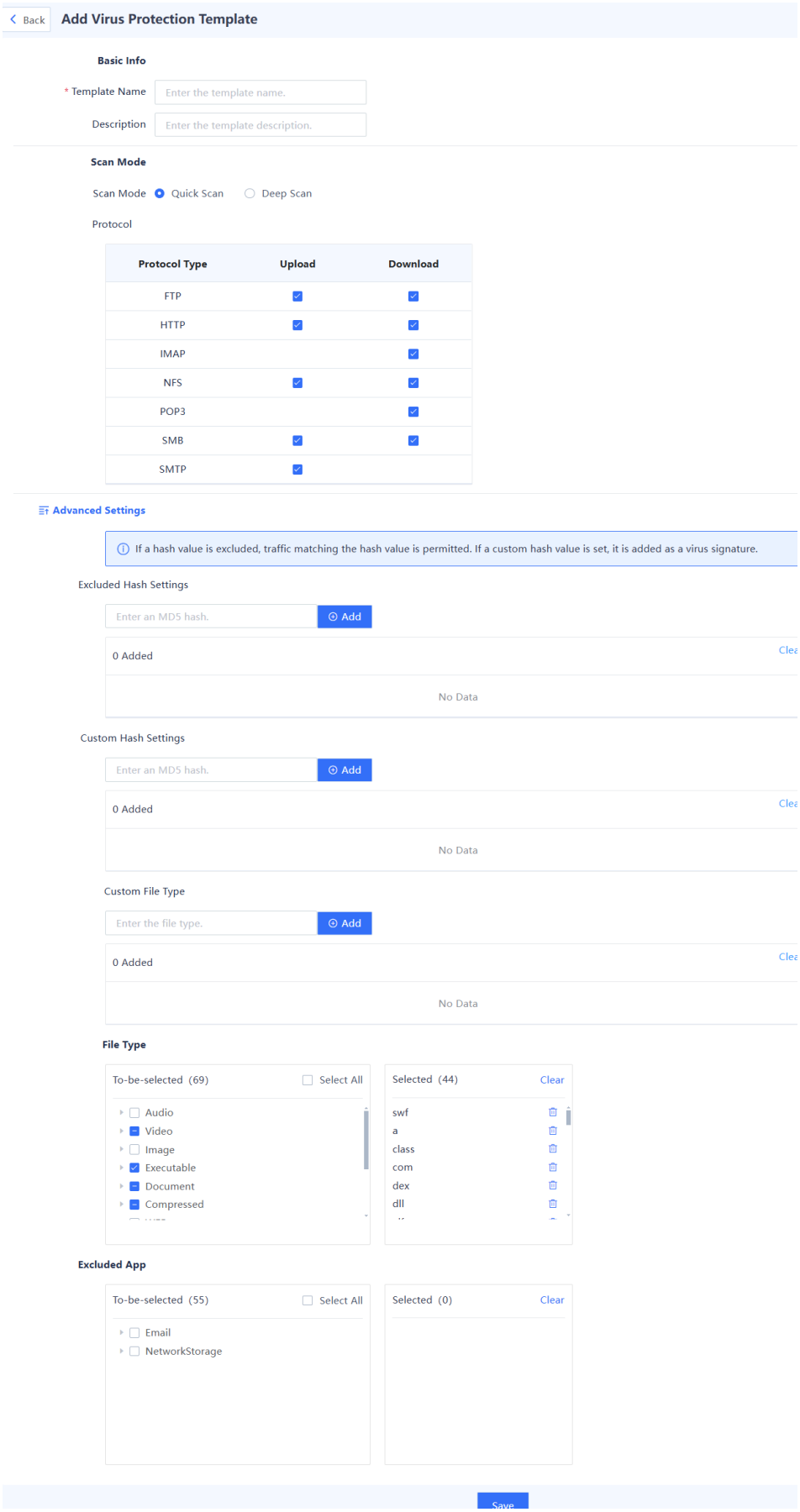
Procedure

(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
Enter the template name.
Description
Enter the template description.
Scan Mode
Scan Mode
Quick Scan
Deep Scan
Protocol
Protocol Type
Upload
Download
FTP
HTTP
IMAP
NFS
POP3
SMB
SMTP
Advanced Settings
If a hash value is excluded, traffic matching the hash value is permitted. If a custom hash value is set, it is added as a virus signature.
Excluded Hash Settings
Enter an MD5 hash.
Add
0 Added
No Data
Custom Hash Settings
Enter an MD5 hash.
Add
0 Added
No Data
Custom File Type
Enter the file type.
Add
0 Added
No Data
File Type
To-be-selected (69)
Select All
Audio
Video
Image
Executable
Document
Compressed
Selected (44)
Clear
swf
a
class
com
dex
dll
Excluded App
To-be-selected (55)
Select All
Email
NetworkStorage
Selected (0)
Clear
Save

Item	Description	Remarks
Basic Info		
Template Name	Name of the virus protection template.	[Example] Template_1
Description	Description of the virus protection template.	[Example] Only for detection of network-wide HTTP traffic
Scan Mode		
Scan Mode	The firewall supports two scan modes: quick scan and deep scan. Different modes use different virus protection signature libraries: ● 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.	[Example] Quick Scan
Protocol	Virus detection is performed on traffic of the specified protocols and directions. Traffic of the other protocols is directly permitted without being detected.	N/A
Advanced Settings Click to expand advanced settings		
Excluded Hash Settings	If a hash is added as an excluded hash, the firewall permits the packets that match the hash.	The supported hash algorithm depends on the hash algorithm used by the virus protection signature library (quick scan). Enter the hash value in the corresponding format.
Custom Hash Settings	After a hash value is added as a custom hash value, the device determines that a packet contains viruses when detecting that the packet matches the hash value.	The supported hash algorithm depends on the hash algorithm used by the virus protection signature library (quick scan). Enter the hash value in the corresponding format.
Custom File Type	Enter file suffixes to add file types for virus detection.	N/A

Item	Description	Remarks
File Type	Select file types (based on file suffixes) for virus detection. If the file type to be detected is unavailable, you can add the file type by setting **Custom File Type**.	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 4.1 Security Policy.

3. Viewing the Predefined Virus Protection Template

Application Scenario

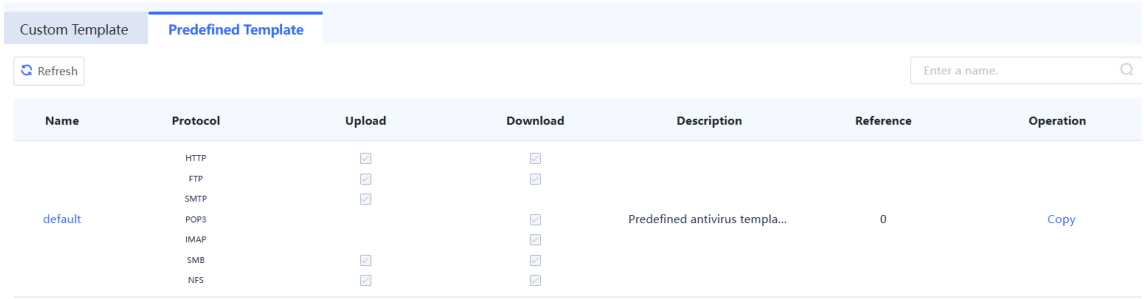
View the predefined content template to check the protocol traffic to be detected for subsequent configuration.

Prerequisites

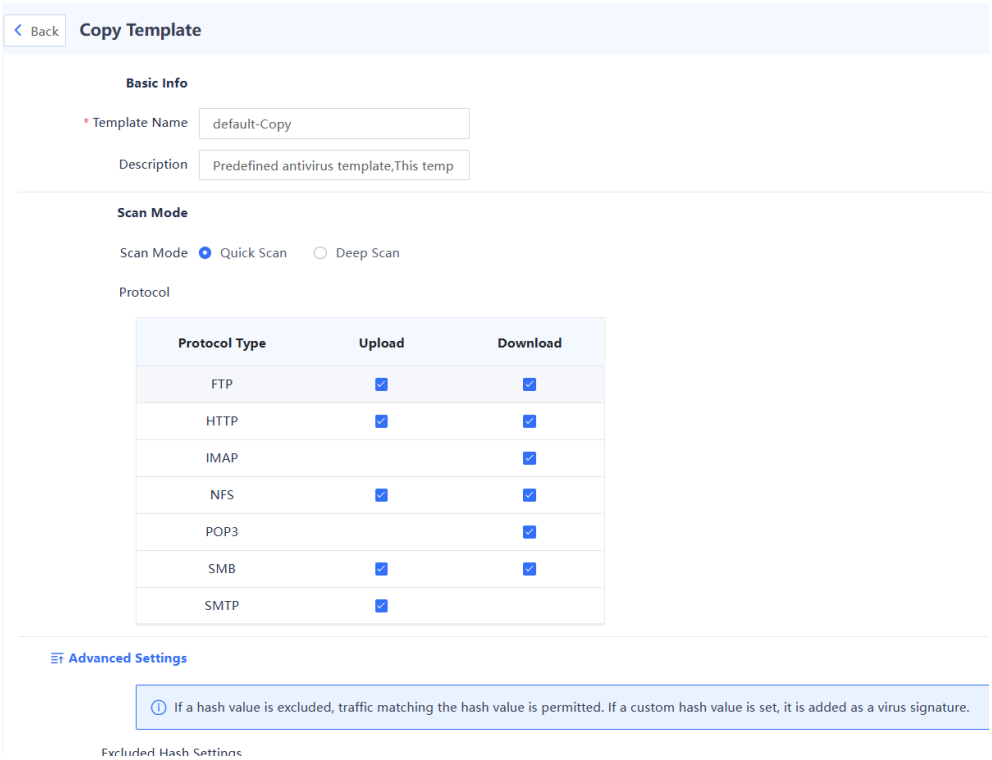
A predefined template cannot be deleted or edited, but you can copy it and then edit it as a custom template.

Procedure

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



(2) (Optional) 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 predefined virus protection template is referenced by a security policy. For details about security policies, see 4.1 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 7.5 Signature Library Upgrade.

5.10.2 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.

Note

If the IPS function is unauthorized or the license of the IPS function expires, the IPS function can be used normally, but the IPS signature library cannot be upgraded.

2. Creating a Custom IPS Content Template

Application Scenario

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

Procedure

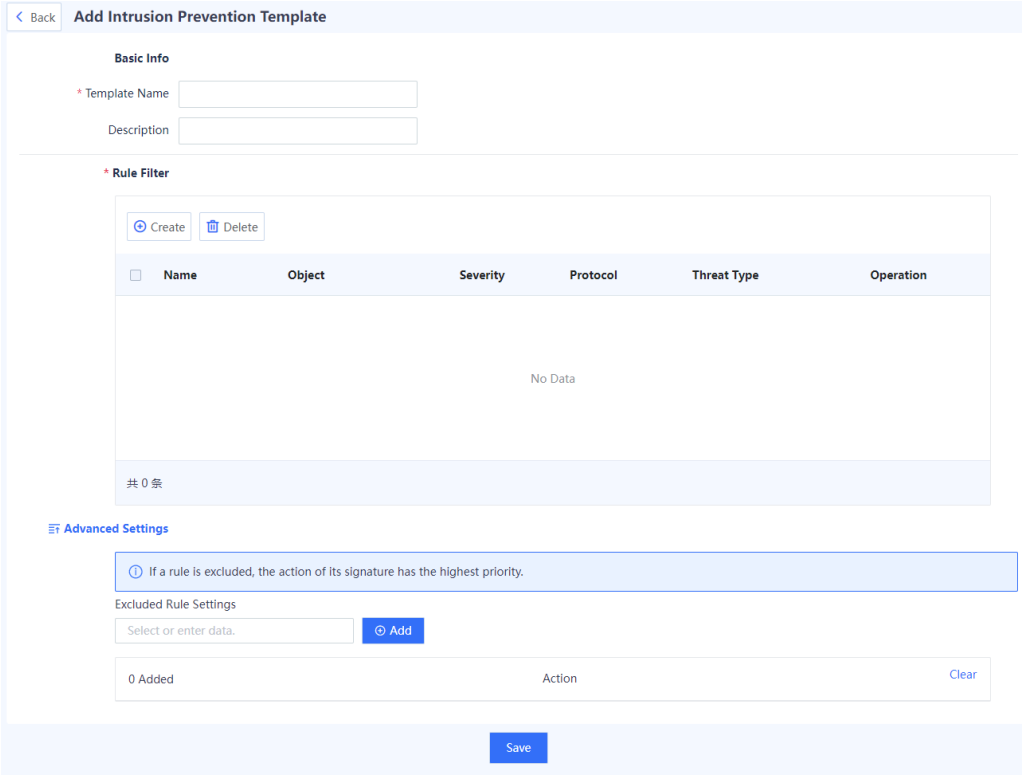
(1) Access the **Add Intrusion Prevention Template** page.

a Choose **Object** > **Content Template** > **Intrusion Prevention** > **Custom Template**.

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

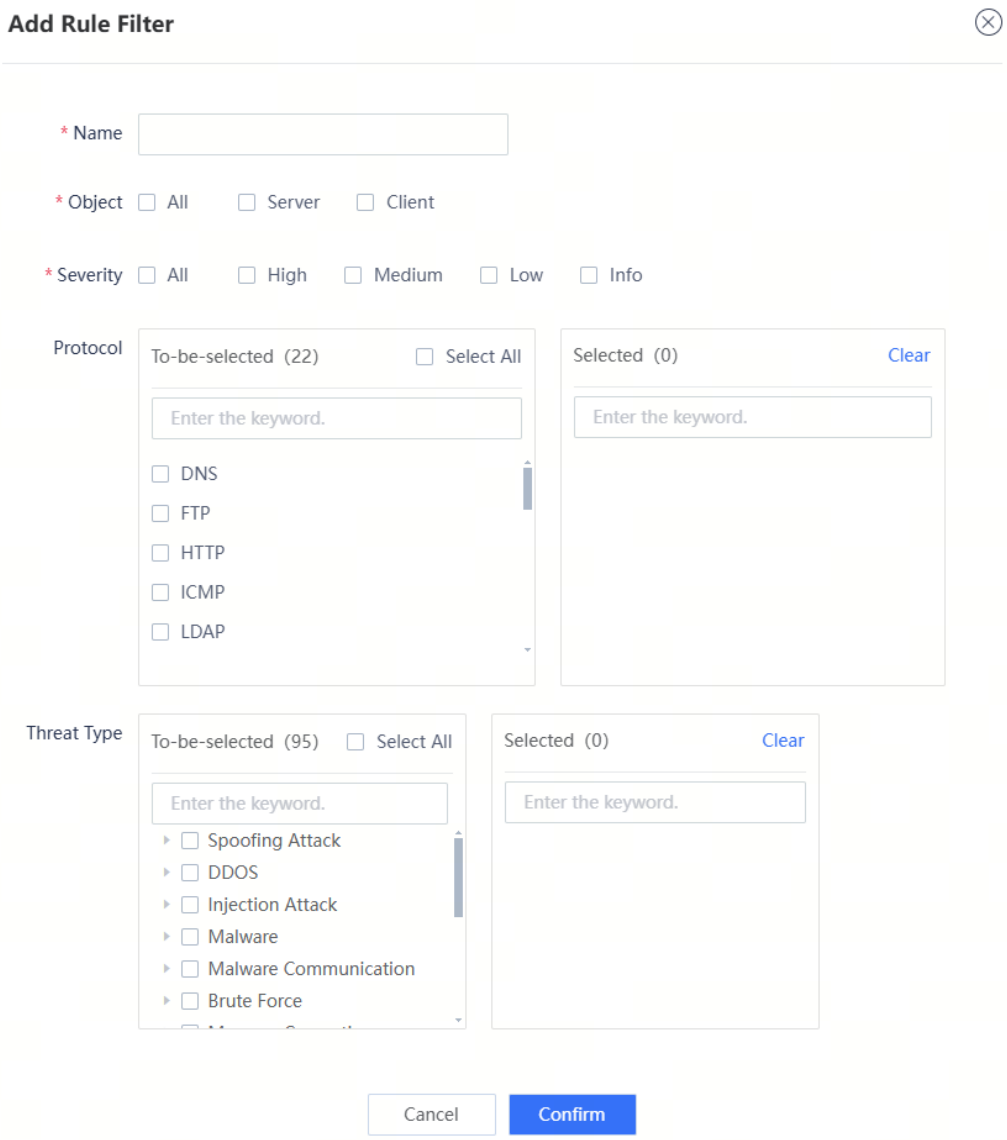


(2) Set parameters for the intrusion prevention template.



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**.

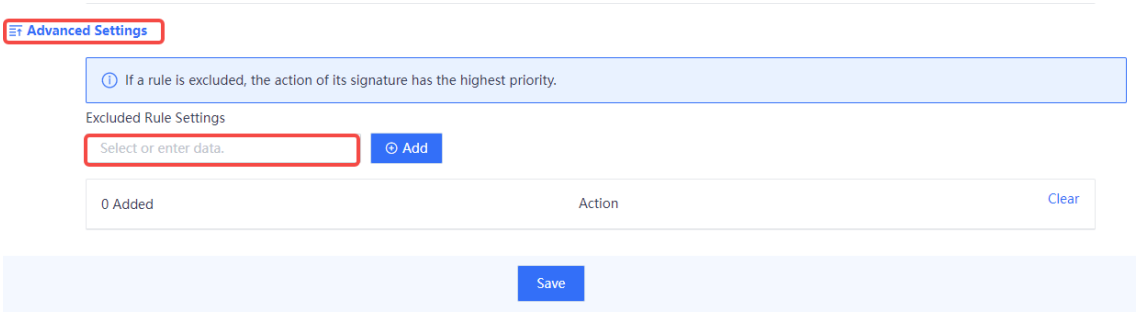


Item	Description	Remarks
Name	Name of the new rule filter.	You are advised to configure a name that can describe the filter function. [Example] Filter1
Object	Objects to be protected.	[Example] All

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.



(3) Click **Save**.

Follow-up Procedure

- A custom IPS template must be referenced by a security policy before the detection mechanism is triggered. For details about the security policy, see 4.1 Security Policy.

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.

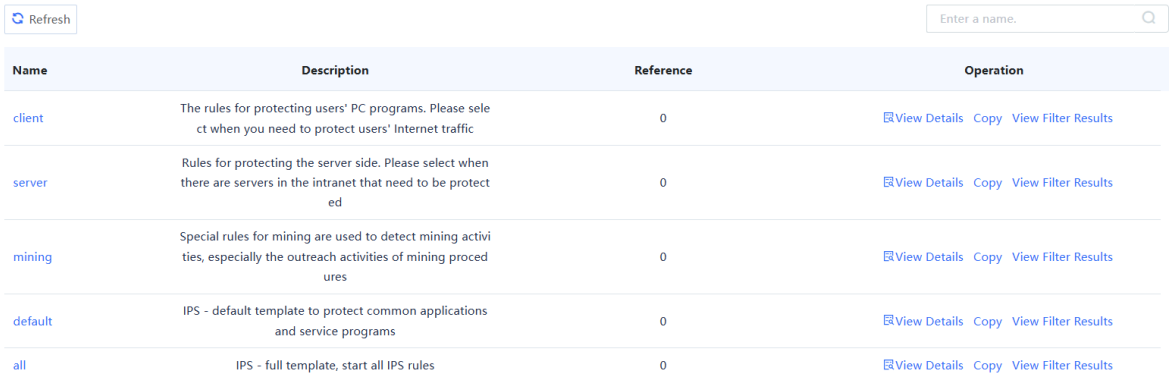
View the predefined content templates to check the features of intrusions to be detected for subsequent configuration.

Prerequisites

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

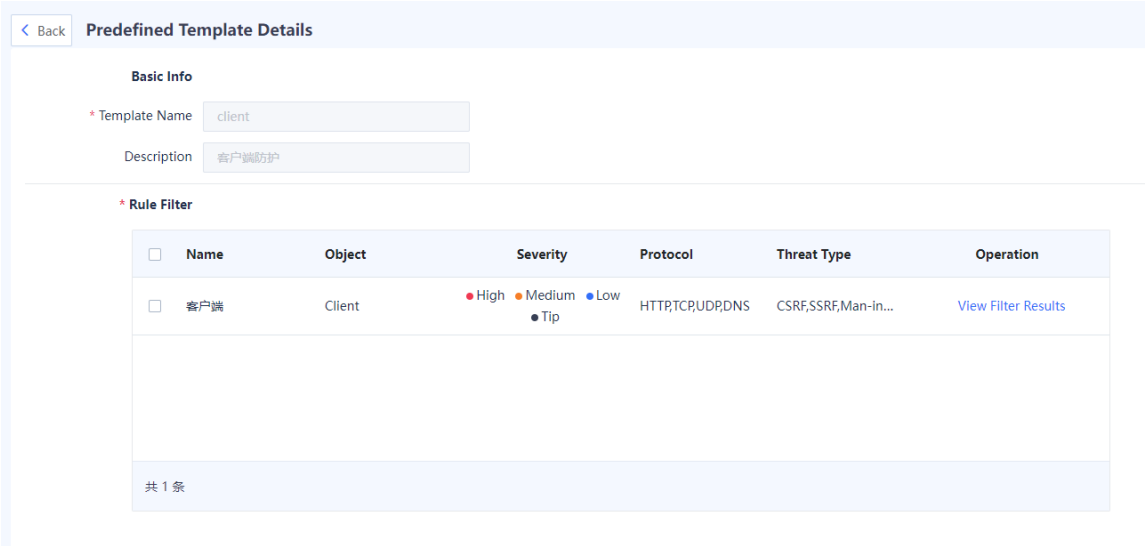
Procedure

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



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

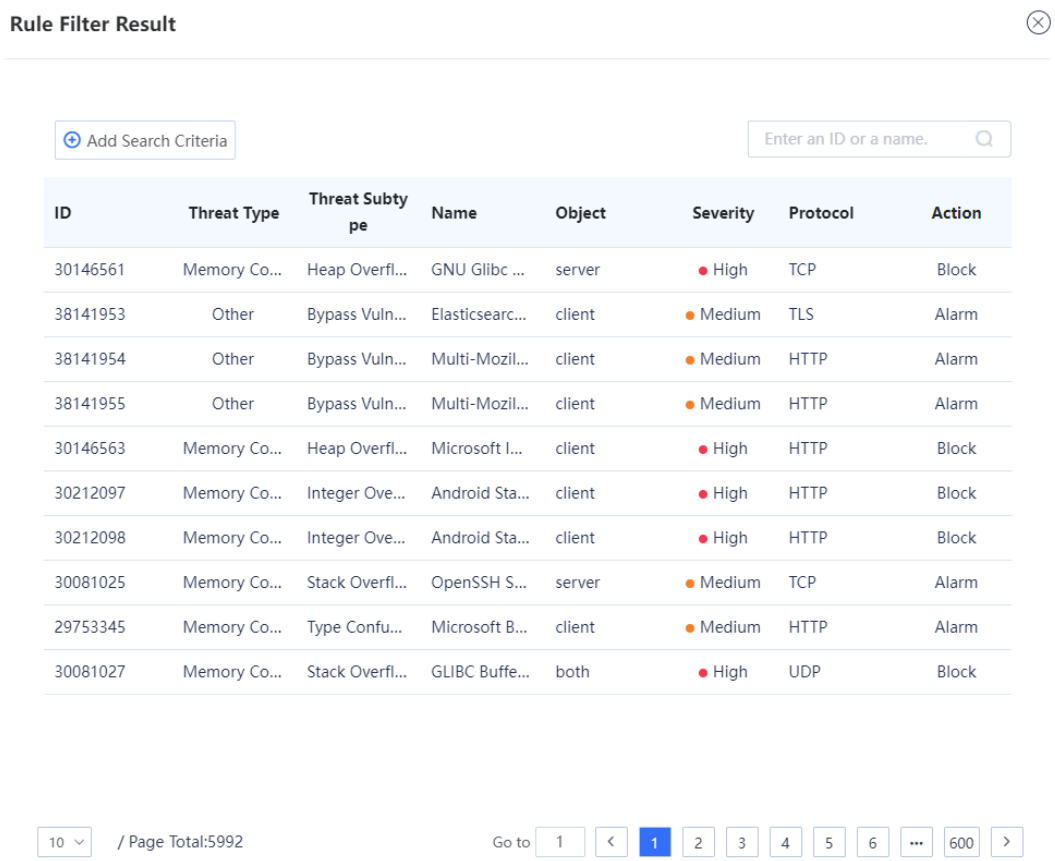
- Click **View Details** to view details about the predefined template, including the name, description, and rule filter information.



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	Attack object of network threats. ● 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	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.
Protocol	Protocol types of network threats to be detected by the predefined content template.
Threat Type	Types of network threats.

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



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. ● 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.

Follow-up Procedure

- A predefined IPS template must be referenced by a security policy before the detection mechanism is triggered. For details about the security policy, see 4.1 Security Policy.

4. IPS Advanced Settings

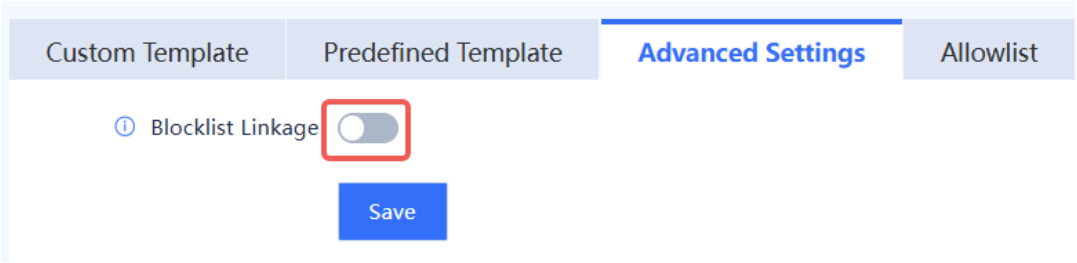
Application Scenario

The IPS technology of the device supports blocklist linkage. If blocklist linkage is enabled, a temporary blocklist can be automatically generated when traffic hits a brute-force IPS policy. The blocking duration is 10 minutes by default and the temporary blocklist is automatically deleted after the blocking duration expires. If blocklist linkage is disabled, a temporary blocklist cannot be automatically generated. You can enable the blocklist linkage function as required. If traffic hits a temporary blocklist, it is directly blocked without IPS detection.

Procedure

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

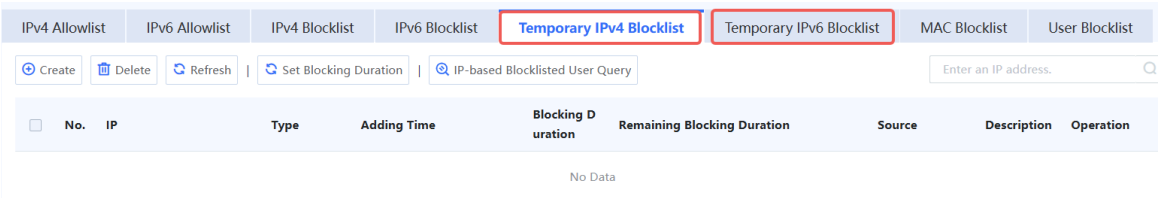
(2) Toggle on to enable blocklist linkage.



(3) Click **Save**.

Follow-up Procedure

- Choose **Policy** > **Blocklist and Allowlist**. On the page that is displayed, click the corresponding temporary blocklist tab to view blocklists added by IPS.



5. Creating IPS Allowlist

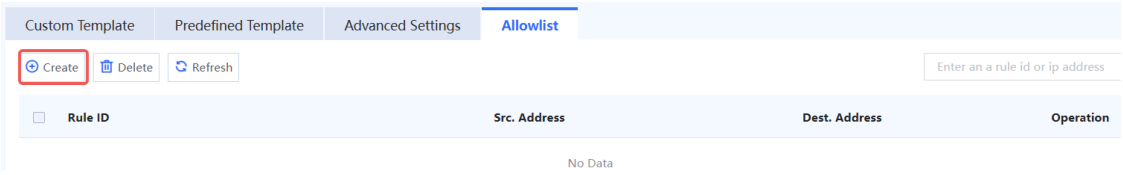
Application Scenario

In some defense scenarios (such as false positives), you can create an IPS allowlist to permit the traffic that matches the allowlist without security log generation.

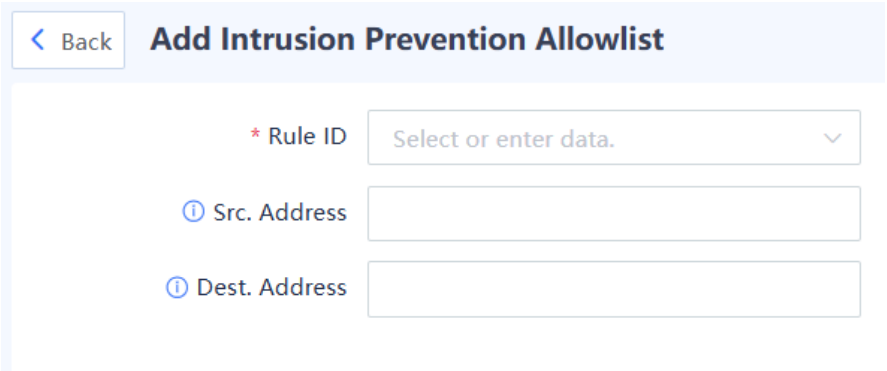
Procedure

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

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



(3) Add an IPS allowlist.



Item	Description	Remarks
Traffic is permitted only when all of the following three parameters are matched.		
Rule ID	Rule ID allowlist.	Select a value from the drop-down list.
Src. Address	Source IP address allowlist.	● Enter a valid IPv4 or IPv6 address. Example: 192.168.1.1 or 1234::100 ● If this parameter is not set, it indicates any IP address.
Dest. Address	Destination IP address allowlist.	● Enter a valid IPv4 or IPv6 address. Example: 192.168.1.1 or 1234::100 ● If this parameter is not set, it indicates any IP address.

(4) Click **Save**.

6. Viewing Intrusion Prevention Logs

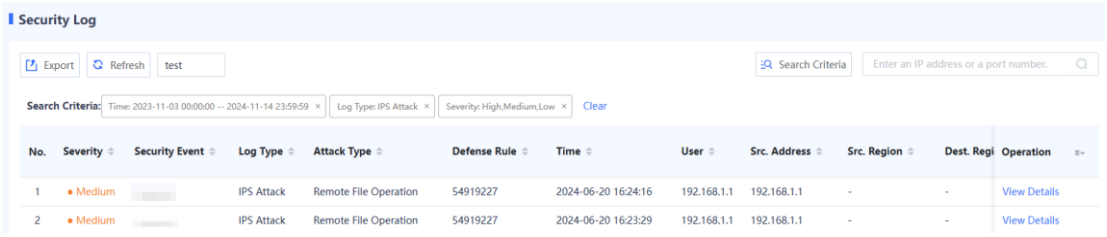
Application Scenario

When malicious traffic matches the conditions of intrusion prevention, a security log is generated, and the log type is IPS attack. By checking the logs, you can view the specific attack information and matched attack type, helping you determine whether to block or permit the traffic.

Procedure

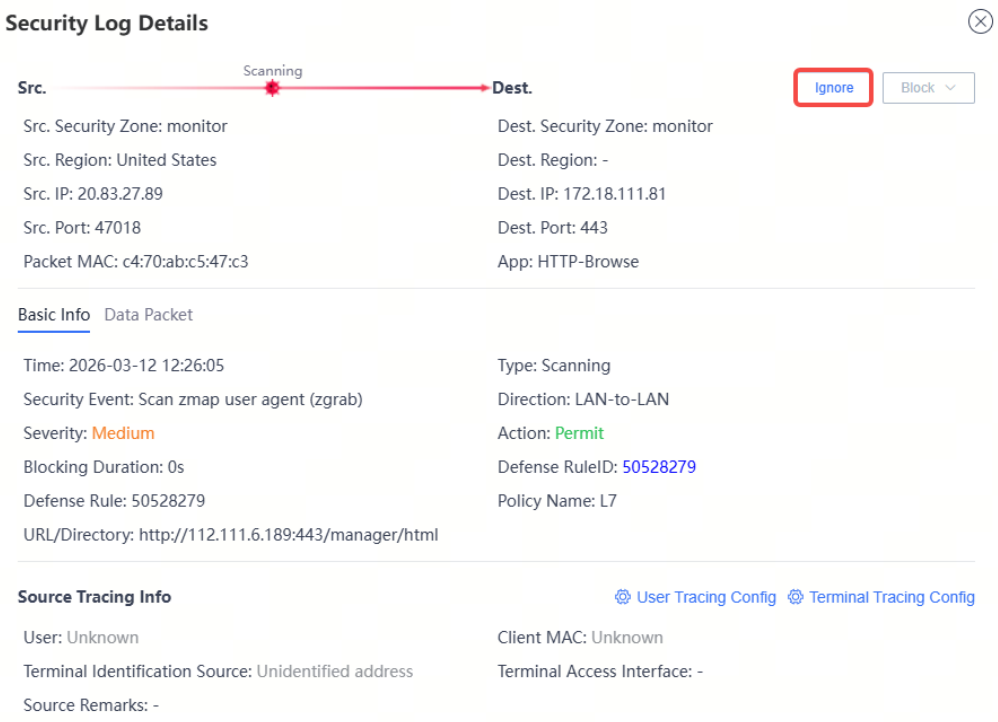
(1) Choose O&M > Logs > Security Log.

(2) Intrusion prevention log information is displayed.



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

- If you confirm that an attack is a false positive, click **Ignore** to add the IPS information in this security log to the IPS allowlist and permit subsequent traffic. To remove the IPS information from the IPS allowlist, click **Unignore**.



- Click **Defense Rule ID** to view the defense rule details.

Note

For more information and configurations about the fields in security logs, see 8.3.2 2. Querying Security Logs.

7. 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 7.5 Signature Library Upgrade.

5.10.3 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 4.1 Security Policy.

Precautions

- If URL filtering is configured for the first time and the client browser has cached a URL that is prohibited from access, the device cannot block traffic accessing the URL before the cache expires. Clear the browser cache or wait for the cache to expire for the configuration to take effect.
- For HTTPS-based URL detection, if the URL only contains the domain name (such as **https://www.example.com**), you do not need to configure an SSL proxy policy. If the URL contains both the domain name and path (such as **https://www.example.com/path/to/resource**), you need to configure an SSL proxy policy. For details about SSL proxy, see 4.11 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.
- When a client browser uses DNS queries to retrieve the ECH configuration, the SNI information in subsequent HTTPS packets is encrypted. As a result, URL filtering fails. To ensure normal URL filtering, you are advised to disable ECH.

1. Custom URL Filtering Template

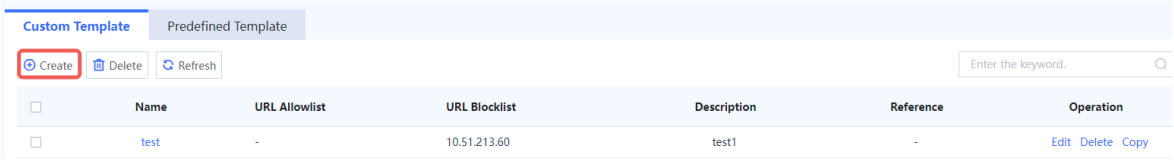
Prerequisites

A custom template can be deleted or edited. You can also copy it and then edit it as a new custom template.

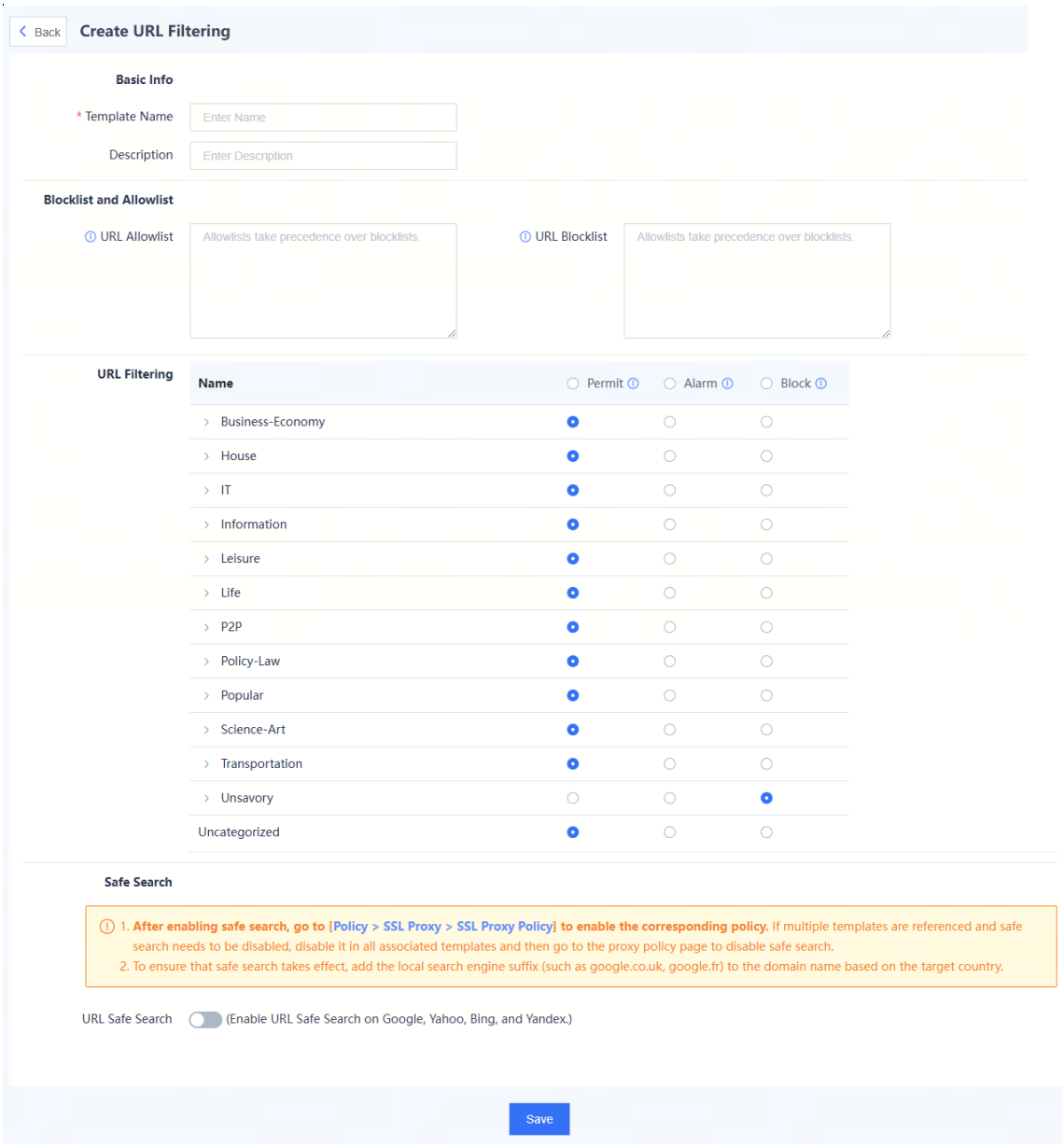
Procedure

(1) Choose **Object** > **Content Template** > **URL Filtering** > **Custom Template**.

(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	After a URL is added to an allowlist, the device directly permits traffic that accesses the URL. URL allowlists take precedence over URL blocklists. Note: Multiple URLs can be entered. A URL can contain the wildcard character (*). Enter one URL per line. Press **Enter** to separate lines. 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
URL Blocklist	After a URL is added to a blocklist, the device directly blocks traffic that accesses the URL. The input format is the same as that for the URL allowlist.	[Example] www.abc2.com
URL Filtering		
URL Filtering	Set processing actions for different URL categories: ● **Permit**: Permit traffic that accesses the URLs of the specific categories. ● **Alarm**: Permit traffic that accesses the URLs of the specific categories and generate an alarm log. ● **Block**: Block traffic that accesses the URLs of the specific categories and generate an alarm log. When a URL matches multiple URL categories, the actions in descending order of priority are as follows: **Block**, **Alarm**, **Permit**.	N/A

(4) Configure the URL safe search function.

Safe search is a safety defense function provided by the search engine to automatically filter unauthorized content or high-risk content (such as adult content and malicious websites). You can enable safe search in the URL filtering template to enable the safe search function for all the Internet access users in a unified manner to standardize user online behavior.

Caution

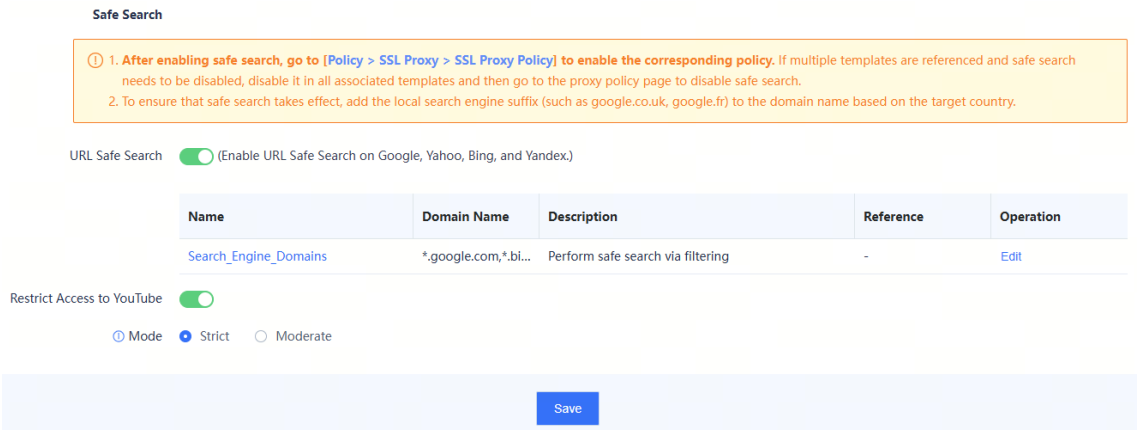
An SSL proxy policy (**default_search_engine**) using the domain name of the corresponding search engine as the destination address exists in the system, and the policy is disabled by default. After you enable the URL safe search function, you need to manually enable this SSL proxy policy to ensure that

URL safe search takes effect. For details about how to configure an SSL proxy policy, see 4.11 SSL Proxy.

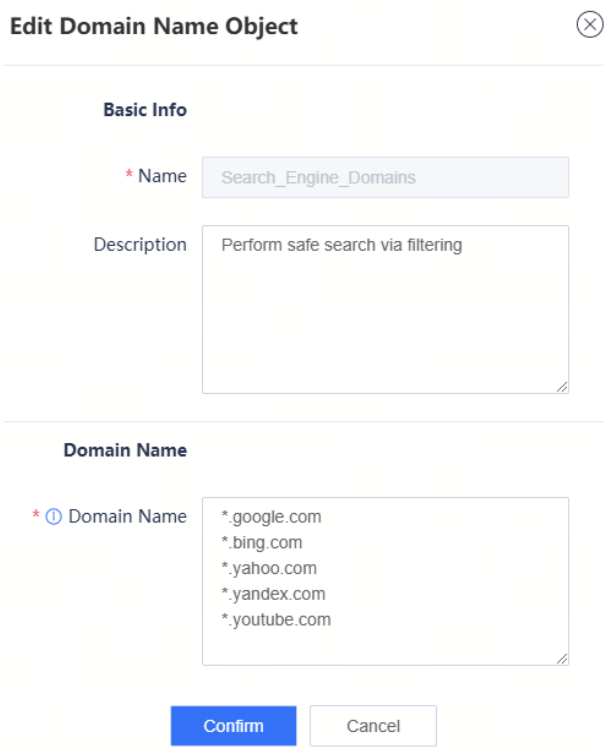
Note

You are advised to enable URL safe search and DNS safe search at the same time to provide more comprehensive security filtering. For details about the DNS safe search configuration, see 4.7.6 DNS Protection.

a Toggle on the **URL Safe Search** switch.

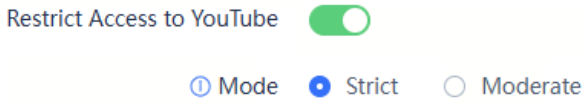


b Click **Edit** and configure the domain names of search engines for which the safe search function is to be enabled. Add the suffixes of the local search engines (such as google.co.uk and google.fr) in the domain names based on the country or region of the Internet access users to ensure that safe search takes effect.



c Specify whether to enable **Restrict Access to YouTube** and select a restriction mode based on management and control requirements.

In strict mode, an automated system is used to filter out a large number of videos while leaving some videos available for users to watch. Compared with the strict mode, the number of videos available for users to watch is significantly increased in moderate mode.



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

Follow-up Procedure

- A custom URL filtering template must be referenced by a security policy before the detection mechanism is triggered. For details about the security policy, see 4.1 Security Policy.
- After enabling URL safe search, you must enable the predefined SSL proxy policy (**default_search_engine**) that uses domain names of search engines as destination addresses to ensure that URL safe search takes effect. For details about SSL proxy policy, see4.11 SSL Proxy.

2. Predefined URL Filtering Template

Prerequisites

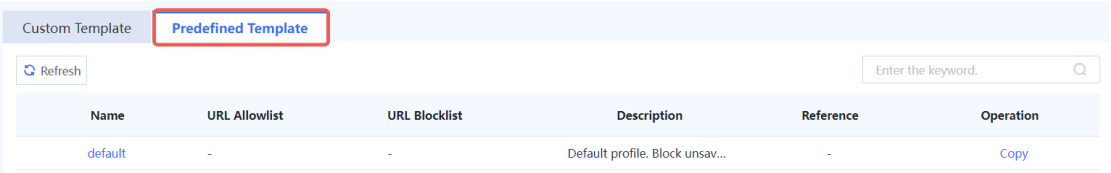
After a license is activated for the device, a default filtering template is displayed on the **Predefined Template** tab page. For details about license activation, see 7.2.4 Activating the License.

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

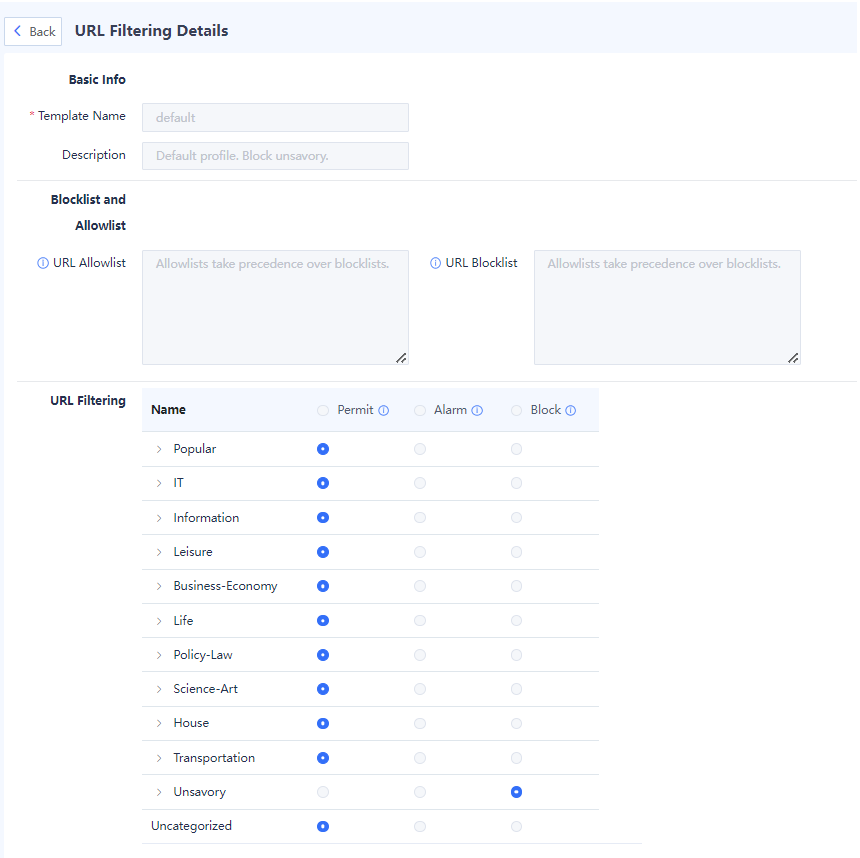
Procedure

(1) Check the predefined URL filtering template.

a Choose **Object** > **Content Template** > **URL Filtering** > **Predefined Template**.

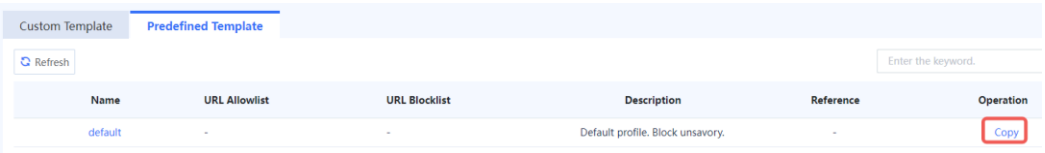


b Click a template name to view URL filtering details.



(2) Modify the parameters of a predefined URL filtering template.

a Click **Copy** in the **Operation** column to copy a template and then modify the parameters as required to quickly create a custom template.



b After the configuration is completed, click **Save**.

Follow-up Procedure

- Refer to a URL filtering template in a security policy. For details about security policies, see 4.1 Security Policy.

5.10.4 Web App Protection

1. Overview

Web app protection is a security defense technology for websites. You can configure a filtering template to analyze access traffic to websites to identify hidden risks and generate alarms or block the traffic, protecting web services. A web app protection template must be referenced in a security policy to trigger the detection mechanism. For details about security policies, see 4.1 Security Policy.

The web app protection function detects traffic by using the web app protection signature library and web semantic detection engine library.

- The web app protection signature library contains built-in features of application-layer attack packets such as website scanning, WebShell, cross-site request forgery, remote file manipulation attacks, and information leakage attacks. When these attack packets pass through the device, the device identifies and blocks them to protect websites based on the web app protection signature library.
- The semantic detection engine library mainly performs semantic analysis against SQL injection, command injection, and code injection. It identifies attack strings through steps including lexical analysis, syntactic analysis, and semantic analysis on the input text.

2. Customizing a Web App Protection Template

Application Scenario

The device provides predefined templates. You can also customize templates for different protection scenarios.

Precautions

- You must remove a custom template from its reference in a security policy before you can delete the template.

Prerequisites

You have installed and activated the web app protection license. For details about how to activate the license, see 7.2.4 Activating the License.

Note

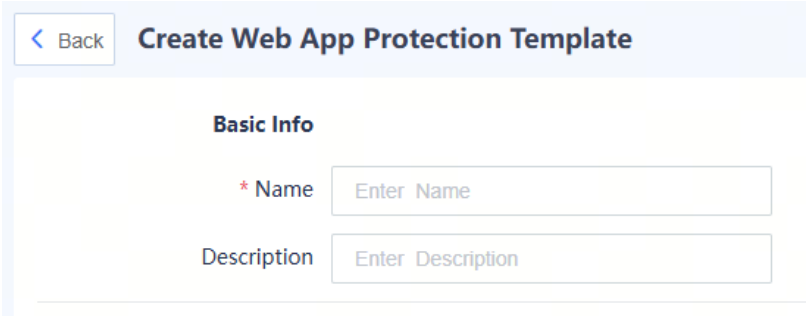
A dedicated license is available for the web app protection function. If the web app protection license is not installed or activated or the license has expired, the existing web app protection signature library can still be used but the semantic detection engine library cannot. Both libraries cannot be upgraded.

Procedure

(1) Choose **Object** > **Content Template** > **Web App Protection** > **Custom Template**.

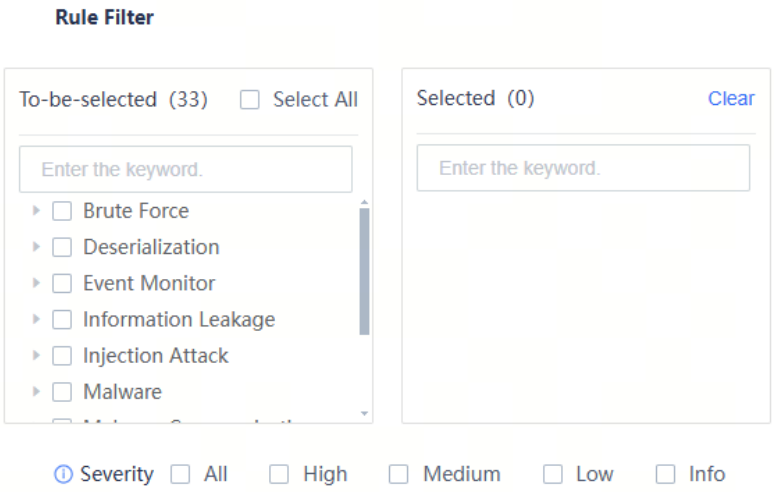
(2) Above the operation area, click **Create**.

(3) Configure basic template information.



Item	Description	Remarks
Basic Info		
Name	Name of the web app protection template.	[Example] Template_1
Description	Description of the web app protection template.	-

(4) Configure a rule filter.



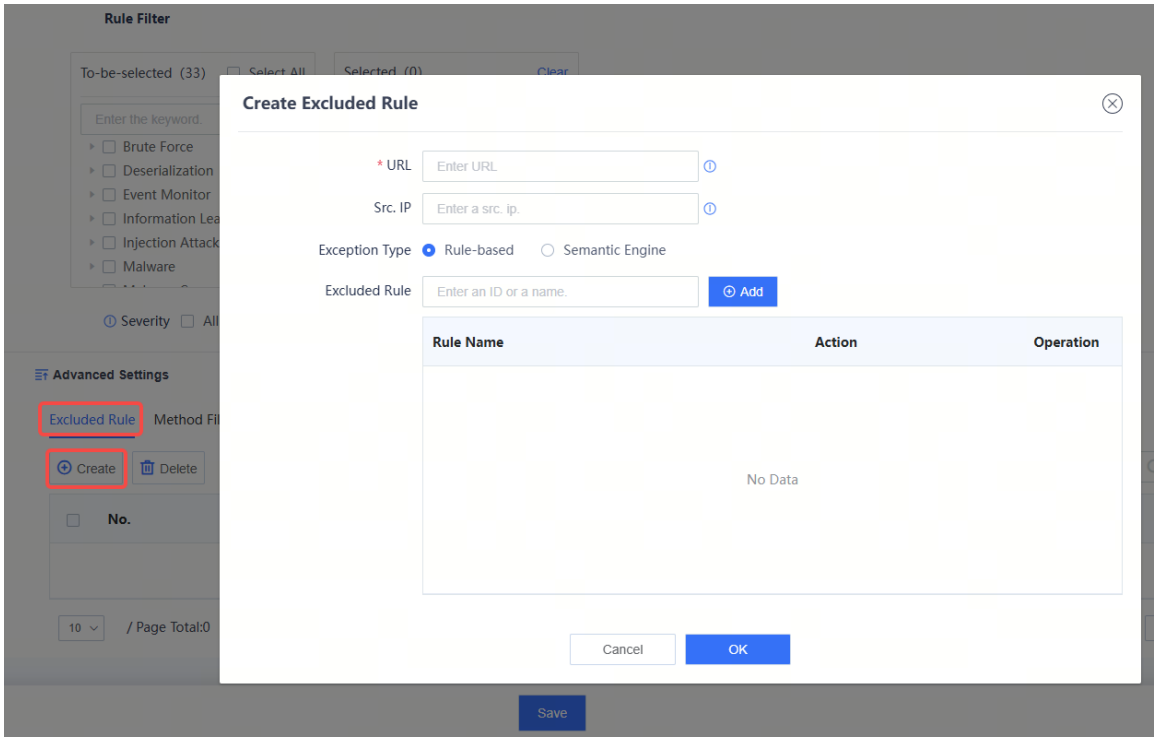
Item	Description	Remarks
Rule Filter	Web app protection rule selected to filter threat categories defined in the rule. Traffic not of the specified threat categories does not match this filter.	Select a rule in the **To-be-selected** column. The selected rule is displayed in the **Selected** column, indicating that the rule is effective.

Item	Description	Remarks
Severity	Severity of the attack result. The options are **High**, **Medium**, **Low**, and **Info**. For example, if you select **High**, only web app protection rules of high severity match the filter. If you leave the parameter empty, the template rule engine does not take effect.	Select an option. [Example] All

(5) Configure advanced parameters.

All parameters in this step are optional. Configure the parameters based on actual needs.

- **Excluded Rule**: After you create an excluded rule, the device takes the action defined in the rule on packets matching the rule, regardless of the action defined in the template.



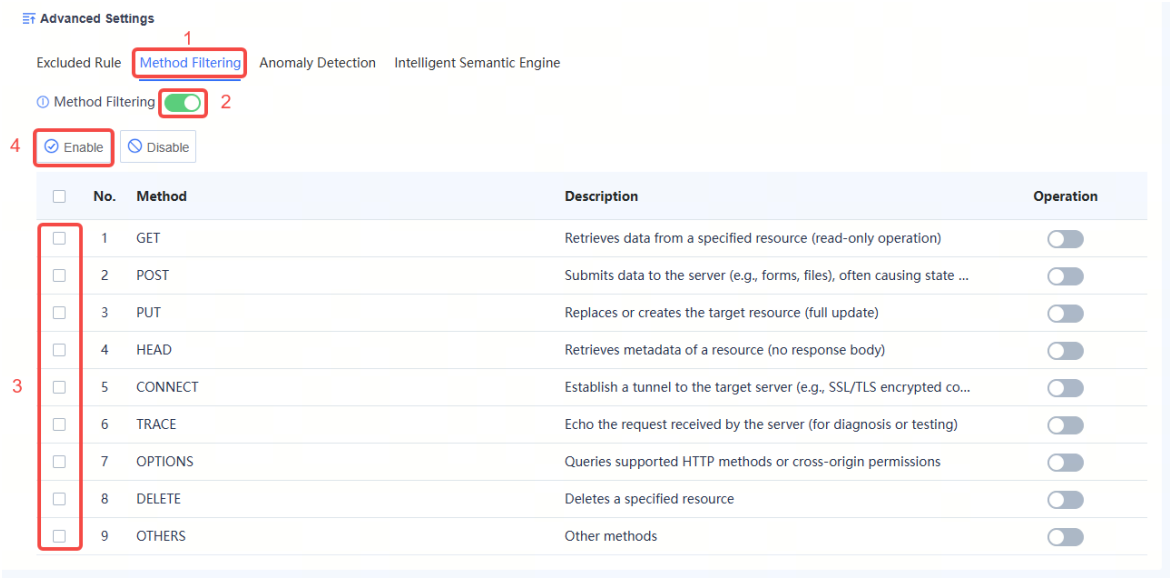
Item	Description	Remarks
URL	URL to be added to the excluded rule list. The device takes the action defined in the excluded rule for traffic matching the list. Do not add URLs of the same exception type.	[Example] http://www.test.com/

Item	Description	Remarks
Src. IP	Source IP address to be added to the excluded rule list. The device takes the action defined in the excluded rule for traffic matching the list.	Enter a valid IPv4 or IPv6 address. [Example] 192.168.1.1 or 1234::100
Exception Type	Type of exception. The options are **Rule-based** and **Semantic Engine**. Select threat categories under the corresponding type and click **Add** to add rule-based exceptions and exceptions defined by the semantic engine to the excluded rule list. You can specify an action for rule-based exceptions and exceptions defined by the semantic engine in the excluded rule list. Then, the device takes the action defined in the excluded rule for traffic matching the list.	-

- **Method Filtering**: Toggle on to enable method filtering. Select HTTP request methods based on actual needs and click **Enable** (or toggle on in the **Operation** column. After that, the device blocks HTTP packets using the selected request methods.

Caution

If HTTPS packets are detected, you need to configure an SSL proxy first. For details about SSL proxy, see 4.11 SSL Proxy.



- **Anomaly Detection**: The device supports protocol anomaly detection and HTTP header overflow detection.

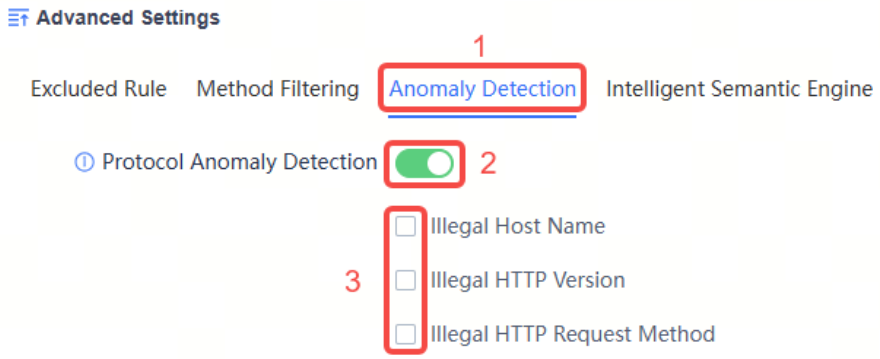
> **Caution**
>
> If HTTPS packets are detected, you need to configure an SSL proxy first. For details about SSL proxy, see 4.11 SSL Proxy.

Toggle on to enable protocol anomaly detection and select an exception type. Then, the device blocks HTTP requests of the selected type.

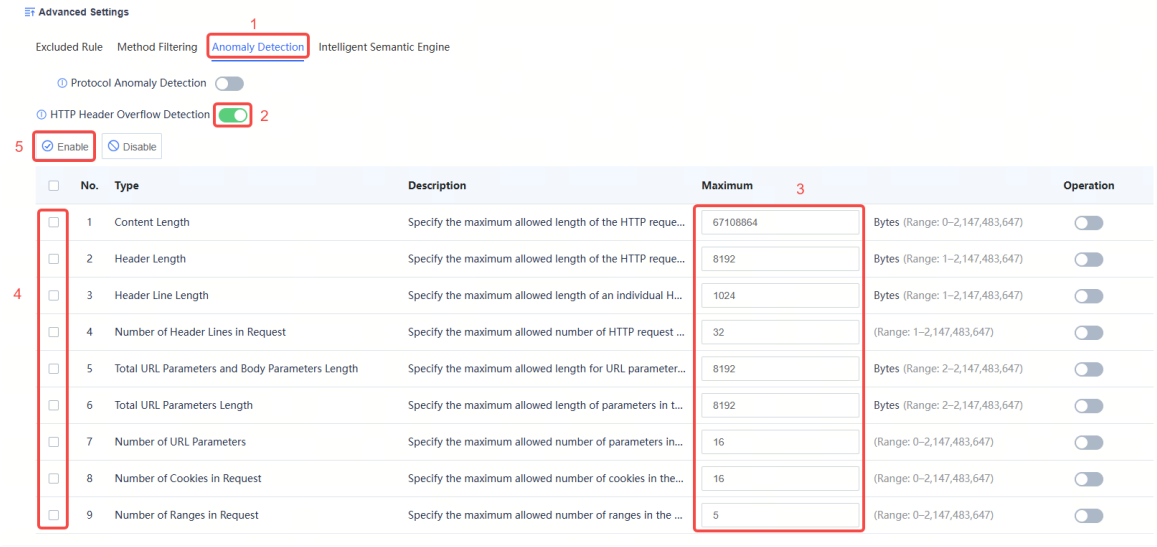
Illegal Host Name: After this option is selected, the device blocks HTTP requests that contain invalid characters such as null string or encoded characters in the **Host** field.

Illegal HTTP Version: After this option is selected, the device blocks HTTP requests not of the following versions: HTTP 0.9, HTTP 1.0, and HTTP 1.1.

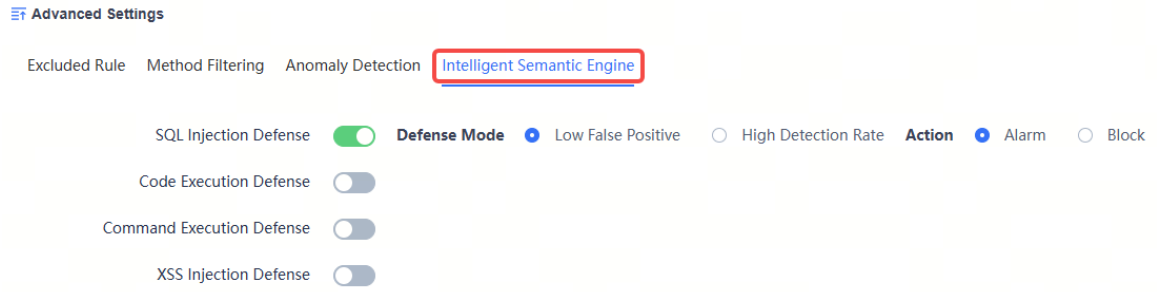
Illegal HTTP Request Method: After this option is selected, the device permits HTTP requests of the following methods: HEAD, GET, PUT, POST, DELETE, CONNECT, OPTIONS, TRACE, PATCH, PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, UNLOCK, VERSION-CONTROL, CHECKOUT, UNCHECKOUT, CHECKIN, UPDATE, LABEL, REPORT, MKWORKSPACE, MKACTIVITY, BASELINE-CONTRODL, MERGE and blocks HTTP requests of other methods.



Toggle on to enable HTTP header overflow detection, select detection types, set the maximum value for each type, and then click **Enable** (or toggle on in the **Operation** column). Then, the device blocks HTTP packets with the maximum value exceeded for the corresponding fields.



- Intelligent Semantic Engine:



Item	Description	Remarks
Defense Mode	Defense mode of the semantic engine. The options are as follows: ● **Low False Positive**: strict detection rule with low error rate ● **High Detection Rate**: loose detection rule with high error rate	[Example] Low False Positive
Action	Action defined by the semantic engine. The options are as follows: ● **Alarm**: Permits traffic matching the filter rule and records a log. ● **Block**: Discards packets matching the filter rule and records a log.	[Example] Alarm

(6) Click **Save**.

Follow-up Procedure

- A custom web app protection template must be referenced in a security policy to trigger the detection mechanism. For details about security policies, see 4.1 Security Policy.

3. Viewing the Predefined Web App Protection Template

Application Scenario

Multiple predefined web app protection templates are built in the device, covering various defense requirements in typical application scenarios. You can directly reference predefined web app protection templates in security policies based on actual defense requirements to further detect and filter the traffic.

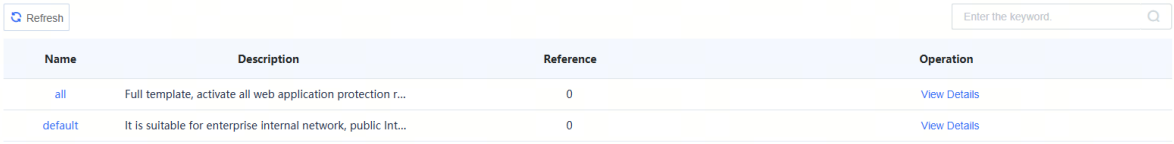
Before configuring security policies, you can view the content of predefined templates to understand the detected threat categories, facilitating subsequent configurations.

Precautions

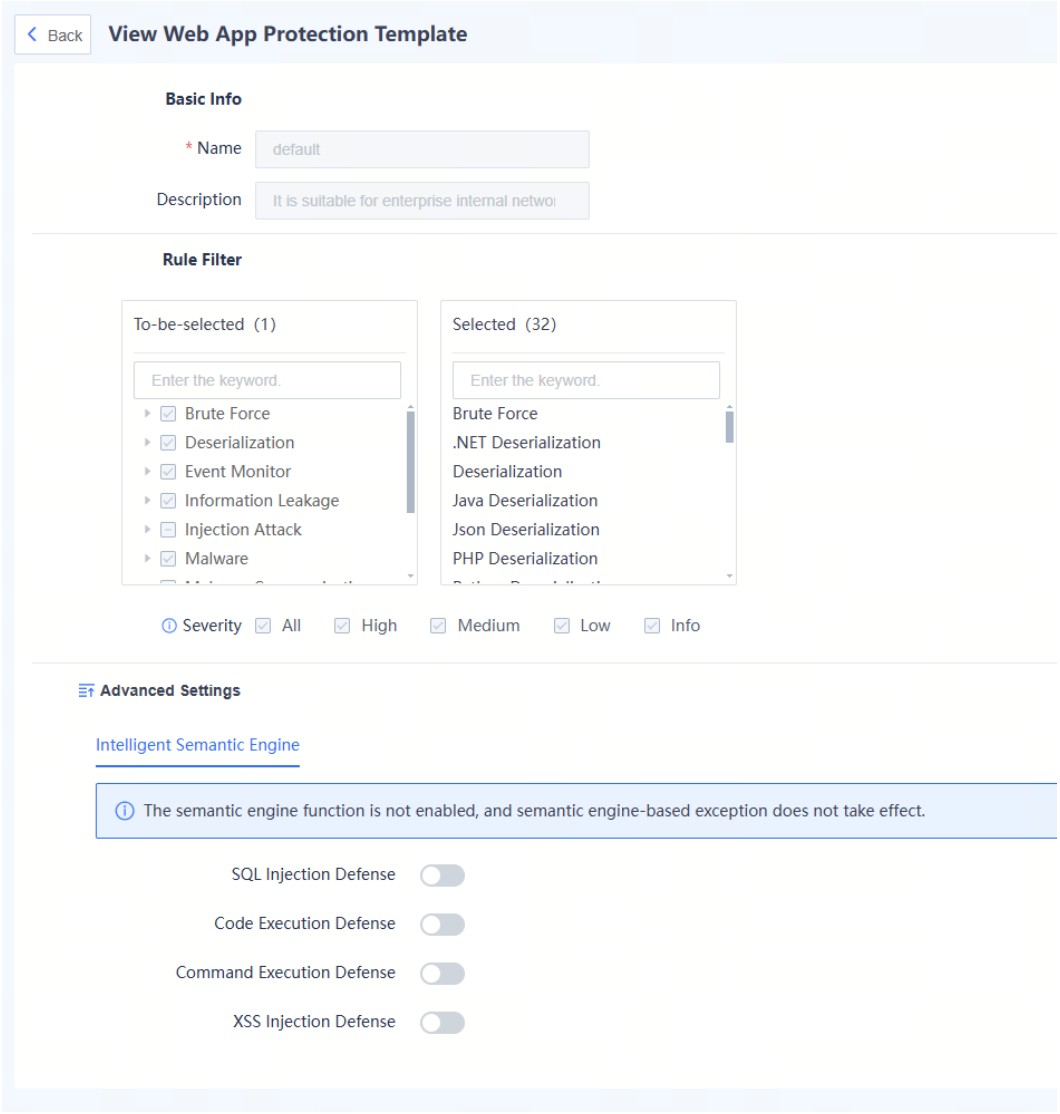
- Predefined templates cannot be deleted or modified.

Procedure

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



(2) Click a template name or **View Details** in the **Operation** column to view the template details.



Follow-up Procedure

- A predefined web app protection template must be referenced in a security policy to trigger the detection mechanism. For details about security policies, see 4.1 Security Policy.

4. Advanced Settings of Web App Protection

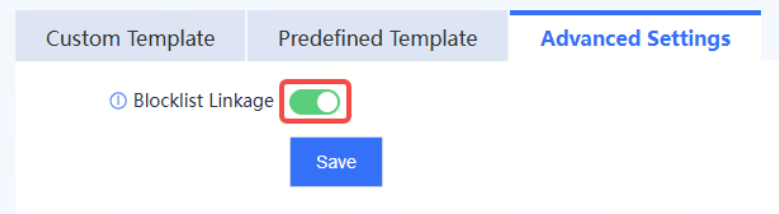
Application Scenario

The device supports blocklist linkage for web app protection. When blocklist linkage is enabled, the device automatically generates a temporary blocklist if the traffic matches a web app protection policy of the brute force attack type. The blocklist has a default blocking duration of 10 minutes and is automatically deleted after expiration. When blocklist linkage is disabled, the device does not automatically generate a temporary blocklist. You can enable blocklist linkage based on actual defense requirements. If traffic matches the temporary blocklist, the device directly blocks the traffic and does not apply web app protection.

Procedure

(1) Choose **Object** > **Content Template** > **Web App Protection** > **Advanced Settings**.

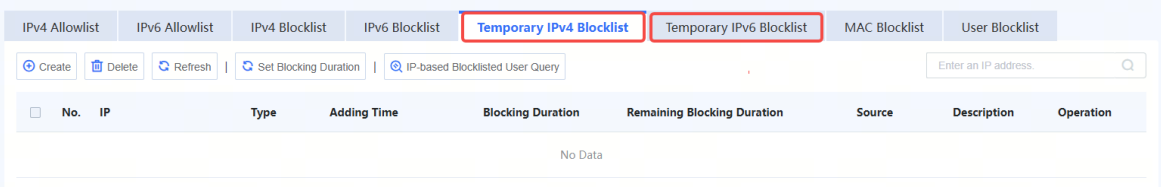
(2) Toggle on to enable blocklist linkage.



(3) Click **Save**.

Follow-up Procedure

- Choose **Policy** > **Blocklist and Allowlist** to view the temporary blocklist added for web app protection.



5. Upgrading the Web App Protection Signature Library and Semantic Detection Engine Library

The web app protection signature library and semantic detection engine library are continuously updated to maintain security of the highest level. You can upgrade the web app protection signature library and semantic detection engine library to detect more types of web app services and web semantics. For details about signature library upgrade, see 7.5 Signature Library Upgrade.

5.10.5 Keyword Filtering

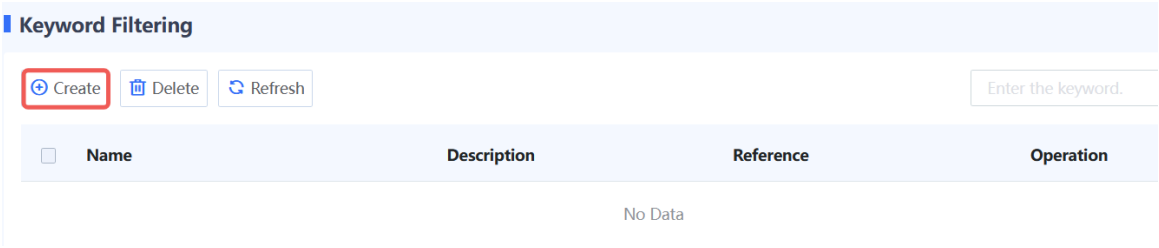
Application Scenario

Configure a keyword filtering template to block or report alarms for traffic containing keywords. Detection can be triggered only after a keyword filtering template is referenced by a security policy. For details about security policies, see 4.1 Security Policy.

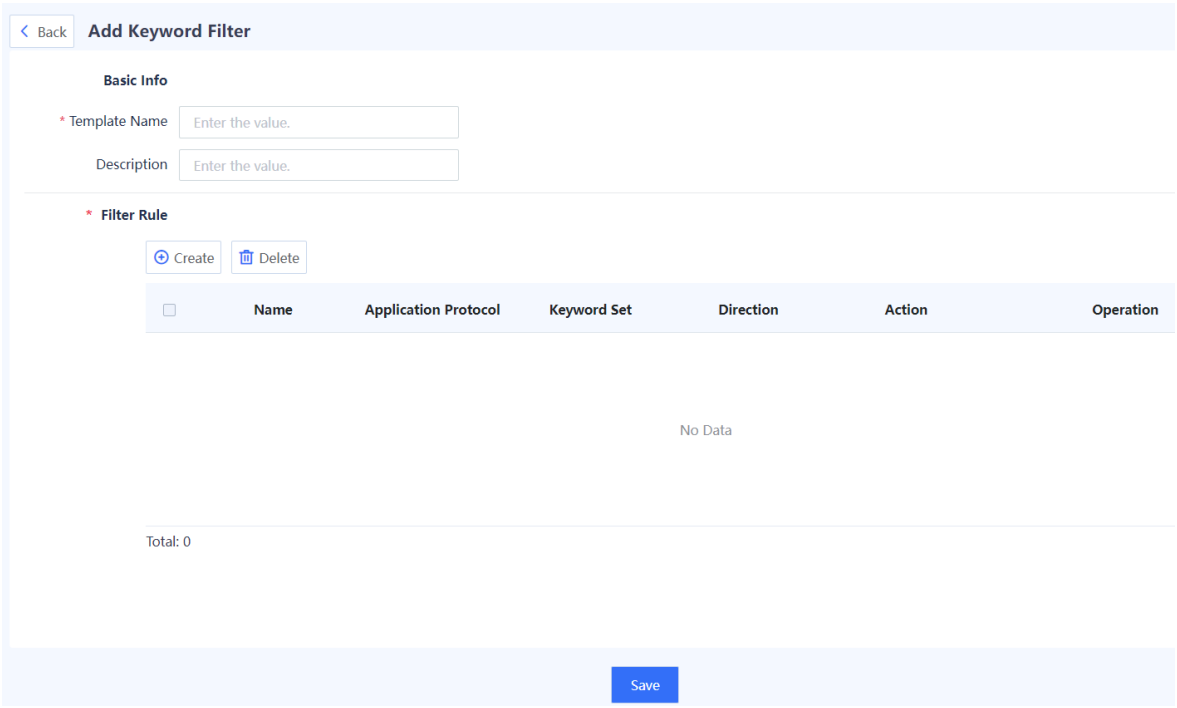
Procedure

(1) Choose **Object** > **Content Template** > **Keyword Filtering**.

(2) Click **Create**.



(3) Enter keyword filtering template information.



Item	Description	Remarks
Basic Info		
Template Name	Name of the keyword filtering template.	[Example] Template_1
Description	Description of the keyword filtering template.	[Example] Template_1
Filter Rule		
Rule Name	Name of the filter rule.	[Example] RULE_1

Item	Description	Remarks
Application Protocol	Application protocol for matching.	Select a value from the drop-down list. [Example] All
Keyword Set	Select the keyword text to be filtered. For details about how to configure a keyword set, see 5.3.1 Configuring a Keyword .	Select a value from the drop-down list.
Direction	Direction of the traffic to be detected. ● **Upload**: Upload traffic is detected. ● **Download**: Download traffic is detected. ● **Bidirectional**: Both upload and download traffic are detected.	Select a value from the drop-down list. [Example] Bidirectional
Action	Action defined for the filtering rule. ● **Alarm**: When traffic hits this rule, it is allowed to pass through but a log is recorded. ● **Block**: When traffic hits this rule, it is discarded and a log is recorded.	Select a value from the drop-down list. [Example] Block

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

Follow-up Procedure

- The keyword filtering template must be referenced by a security policy before the detection mechanism is triggered. For details about the security policy, see 4.1 Security Policy.
- To delete a filtering template, you need to delete the reference to the template in the security policy first.

5.10.6 File Filtering

1. Creating a File Filter Template

Application Scenario

Configure a file filter template to block or generate alarms on the transmission of files of specific types to reduce the risks of internal information leakage and intranet virus infection. A file filter template must be referenced by a security policy to trigger the detection mechanism. For details about security policies, see 4.1 Security Policy.

Precautions

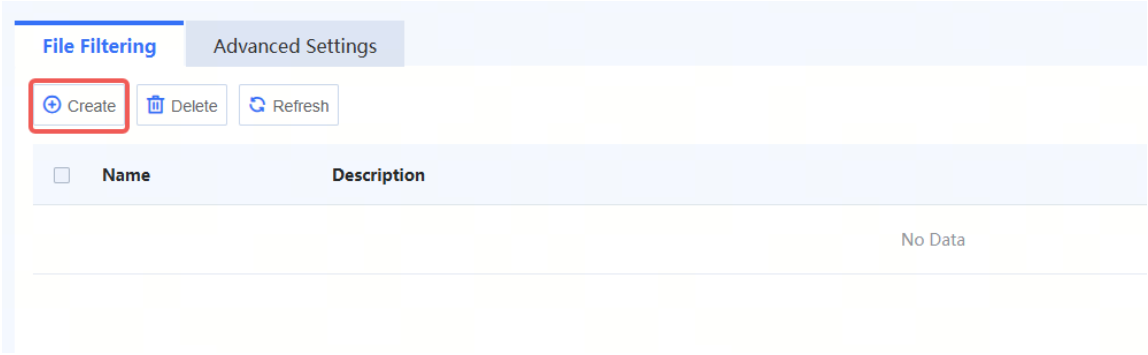
- Only HTTP and FTP packets can be filtered, that is, only files transmitted via HTTP or FTP can be filtered.
- To filter files in HTTPS traffic, configure the SSL proxy function. For details about SSL proxy, see 4.11 SSL Proxy.
- If the first file in a flow is blocked, subsequent traffic (files) in the flow will also be blocked.
- The system does not detect or filter the embedded files (for example, .exe files inserted in Word documents).

- The system does not detect or filter files in a compressed package.

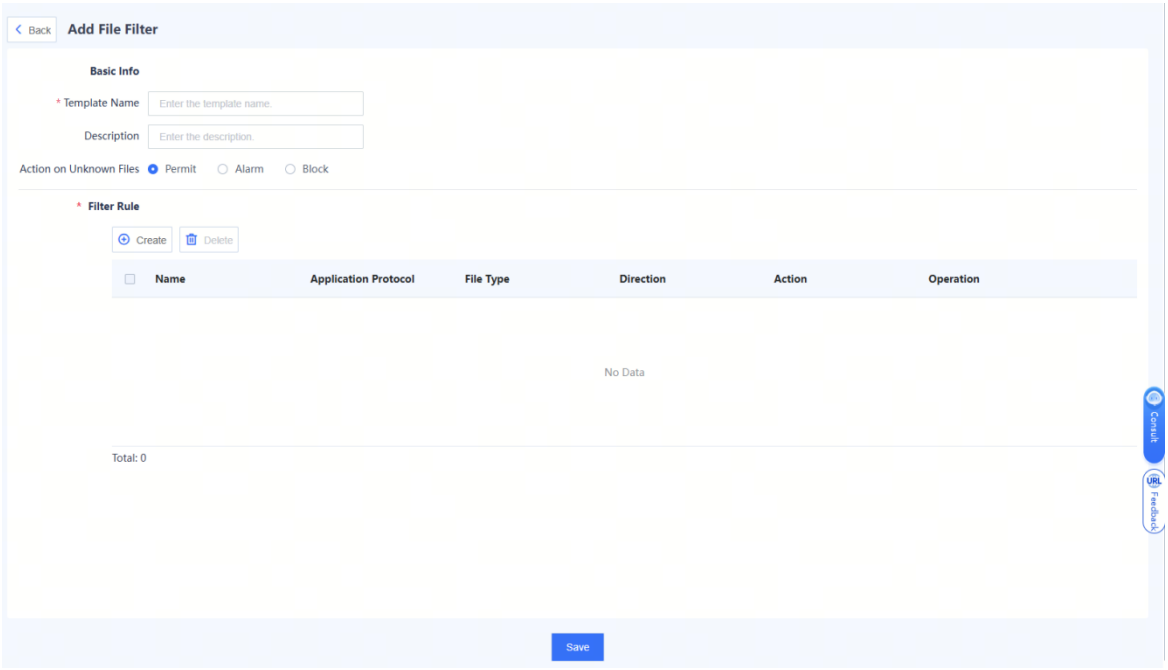
Procedure

(1) Choose **Object** > **Content Template** > **File Filtering** > **File Filtering**.

(2) Click **Create**.



(3) Configure parameters for the file filter template.



Item	Description	Remarks
Basic Info		
Template Name	Name of a file filter template.	[Example] Template_1
Description	Description of a file filter template.	[Example] Prohibits the download of.exe executable files.

Item	Description	Remarks
Action on Unknown Files	Processing action for files that cannot be identified: ● **Permit**: Permit file transfer, but not record logs. ● **Alarm**: Permit file transfer, and record logs. ● **Block**: Block file transfer, and record logs.	[Example] Alarm
Filter Rule ● Click **Create** to create a filter rule. ● If a file matches multiple filter rules, the action with the highest priority is performed. The priority of **Block** is higher than that of **Alarm**.		
Name	Name of a filter rule.	[Example] RULE_1
Application Protocol	Select the application protocols to be filtered. For example, to filter only files transmitted via FTP, select FTP.	● Click the drop-down list and select application protocols. Multiple choices are supported. ● The default value is **All**. That is, all application protocols that support file filtering are detected and filtered. [Example] FTP
File Type	Select the file types to be filtered. The drop-down list contains predefined and custom file type groups.	● Click the drop-down list and select file type groups. Multiple choices are supported. ● The default value is **All**. That is, all file types in the predefined and custom file type groups are detected and filtered. ● Click **Add File Type Group** to add a file type group. For details about file type groups, see 5.3.3 File Type Group. [Example] Executable File
Direction	File transfer direction to be detected. ● **Upload**: Detect uploaded files. ● **Download**: Detect downloaded files. ● **Bidirectional**: Detect both uploaded and downloaded files.	Click the drop-down list and select a value. [Example] Bidirectional
Action	Action performed by the device when a file matches filter rules. ● **Alarm**: Permit file transfer, and record logs. ● **Block**: Block file transfer, and record logs.	Click the drop-down list and select a value. [Example] Block

(4) Click **Save**.

Follow-up Procedure

- A file filter template must be referenced by a security policy to trigger the file detection and filtering mechanism. For details about security policies, see 4.1 Security Policy.
- If a file filter template is referenced by a security policy, the template cannot be deleted. To delete the template, dereference the template in the security policy first.

2. Advanced Settings

Application Scenario

During file transfer, storage, and backup, file extensions (file suffixes) may be modified, resulting in inconsistency between file types and file extensions. In addition, some attackers may disguise risky files by modifying file extensions to bypass the file filtering mechanism based on file extensions. To address the preceding problems and improve the file filtering accuracy, the device provides the file type feature identification function.

If file type feature identification is disabled, the device matches files only based on file extensions and file filtering rules.

If file type feature identification is enabled and the device matches files based on file extensions and file filtering rules: When no blocking rule is hit (for example, a file does not have an extension, the file extension is out of the matching range of the filtering rules, or the action for the matching rule of the file extension is **Alarm**), the file filtering module further identifies the real type of the file by detecting the feature information in the file content, and matches the identified real file type against the file filtering rules. The combination of file extension detection and file type feature identification reduces the risk of virus files entering internal networks and confidential information leakage.

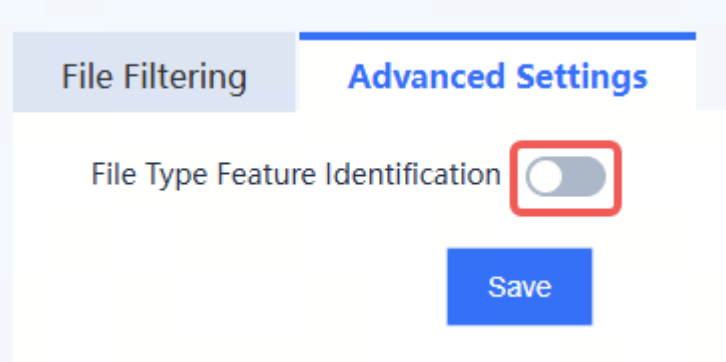
Note

- If a file matches a file filtering rule with the blocking action by extension, the device blocks the file transfer without identifying file type features.
- If a file matches multiple file filtering rules simultaneously, the action with the highest priority is performed. The priorities of actions in descending order are as follows: **Block** > **Alarm** > **Permit**.

Procedure

(1) Choose **Object** > **Content Template** > **File Filtering** > **Advanced Settings**.

(2) Toggle on **File Type Feature Identification**.



(3) Click **Save**.

5.10.7 AI-based Threat Detection

1. Overview

As the core remote management entries for Linux and Windows systems, SSH and Remote Desktop Protocol (RDP) are primary targets of ransomware and host control attacks. Attackers locate open services through port scanning, and then launch brute force attacks against SSH or RDP. Conventional solutions can hardly detect stealth attacks such as multi-host distributed attacks, medium- and low-frequency tentative connections, and bypassing traditional defense mechanisms based on single-IP frequency threshold.

To address these issues, the device provides the AI-based Threat Detection function. It uses the built-in lightweight AI behavior analysis engine to perform feature extraction and model aggregation on attack traffic such as SSH/RDP-encrypted attacks and port scanning. This effectively identifies stealth attacks such as medium- and low-frequency tentative connections and multi-host collaboration. Compared with traditional frequency detection, this function significantly improves the security protection capability of remote management ports.

2. Customizing a Detection Template

Application Scenario

You can create custom templates for detection and defense based on the defense scenario.

Prerequisites

You have installed and activated the AI-based Threat Detection license. For details about how to activate the license, see 7.2.4 Activating the License.

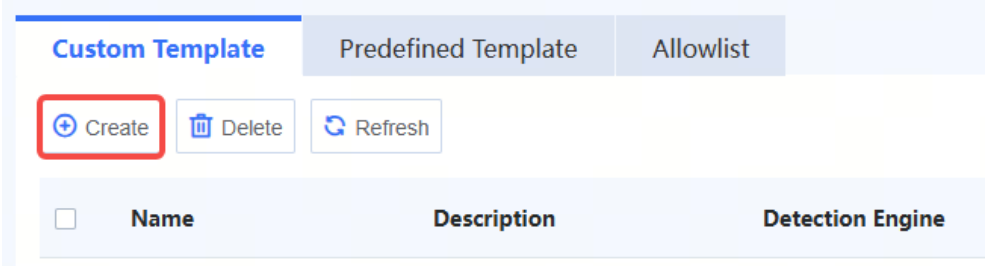
Note

If the AI-based Threat Detection license is not activated, the AI-based Threat Detection function is unavailable. After the license expires, the AI-based Threat Detection function is still available but its engine library cannot be upgraded.

Procedure

(1) Choose **Object** > **Content Template** > **AI-based Threat Detection** > **Custom Template**.

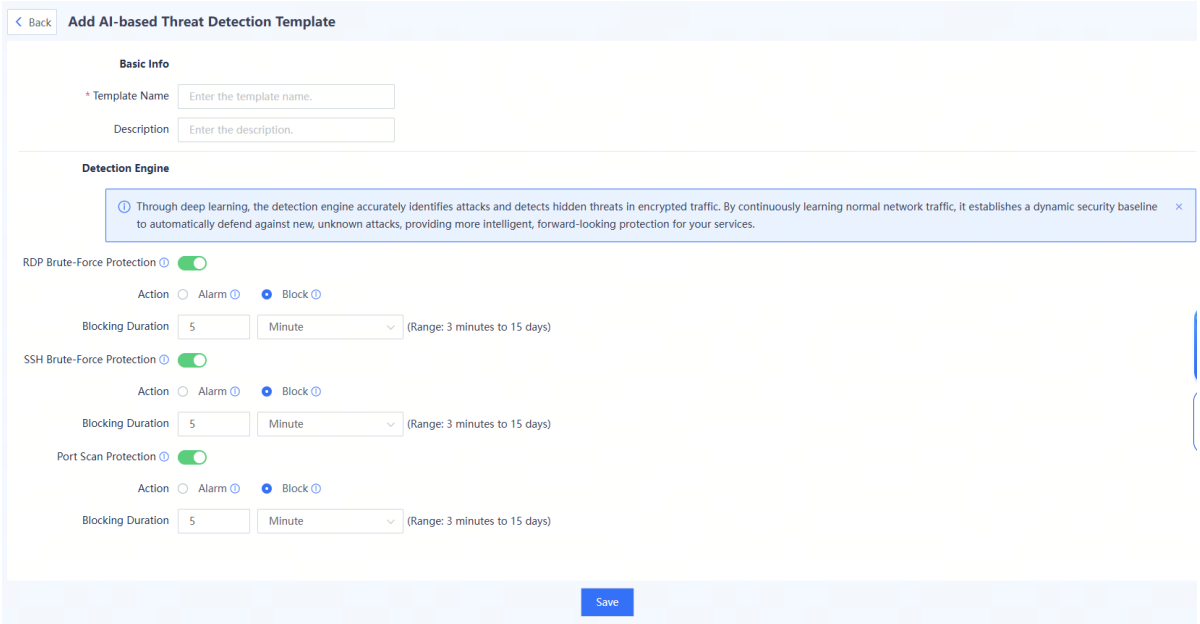
(2) Click **Create**.



(3) Enter a template name and select an attack type to be detected and the processing action for the attack type.

- **Alarm**: Permits traffic matching the template and generates a security log.
- **Block**: Adds the source IP address of traffic matching the template to a temporary blocklist, blocks traffic from this IP address within the validity period of the temporary blocklist, and generates a security log.

The default validity period of the temporary blocklist is 5 minutes, which is configurable. After you delete or disable a template, the temporary blocklist does not become invalid. To make the temporary blocklist ineffective, wait until the temporary blocklist expires or choose **Policy** > **Blocklist and Allowlist** > **Temporary IPv4 Blocklist** > **Temporary IPv6 Blocklist** to manually delete the temporary blocklist.



(4) Click **Save**.

Follow-up Procedure

- An AI-based Threat Detection template must be referenced in a security policy to trigger the detection mechanism. For details about security policies, see 4.1 Security Policy.

3. Viewing the Predefined Detection Template

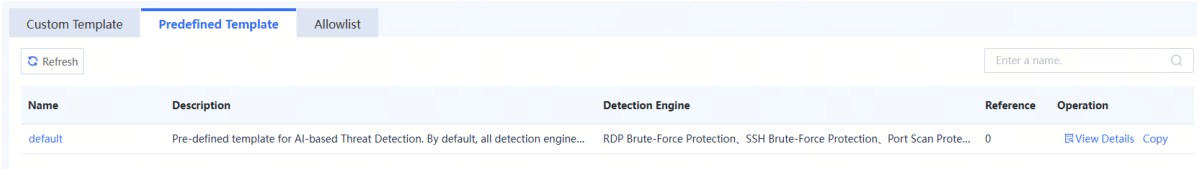
Application Scenario

The device provides predefined detection templates. You can directly reference predefined templates in security policies based on actual defense requirements to further detect and filter the traffic.

A predefined template cannot be added or modified. You can copy it as a custom template and then modify it.

Procedure

(1) Choose **Object** > **Content Template** > **AI-based Threat Detection** > **Predefined Template**.



(2) Click **View Details** to view parameters in the predefined template.

(3) Click **Copy** to copy the content of the predefined template and modify it based on service needs.

Follow-up Procedure

- An AI-based Threat Detection template must be referenced in a security policy to trigger the detection mechanism. For details about security policies, see 4.1 Security Policy.

4. Configuring a Detection Allowlist

Application Scenario

You can create an allowlist based on the defense scenario (such as false report). After that, the device directly permits traffic matching the allowlist and does not record a security log.

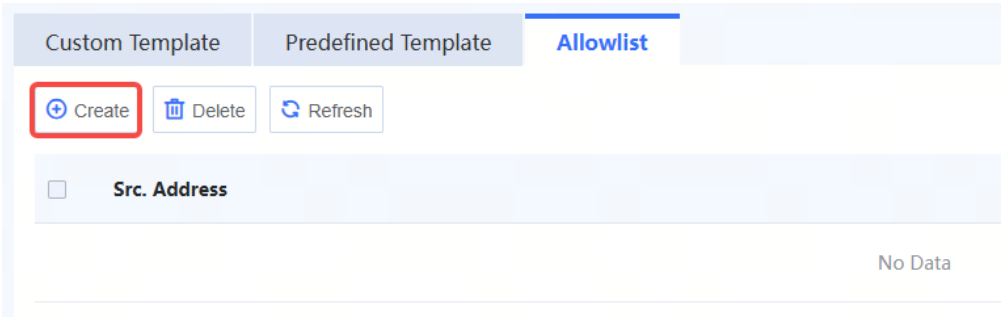
Precautions

After an allowlist is created, if an IP address in the allowlist is the same as that in the temporary blocklist sourced from AI-based Threat Detection, the system automatically removes that IP address from the temporary blocklist (**Policy** > **Blocklist and Allowlist** > **Temporary IPv4 Blocklist** or **Temporary IPv6 Blocklist**).

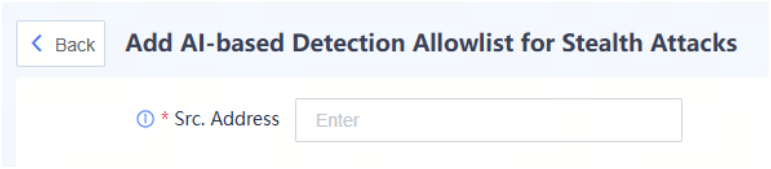
Procedure

(1) Choose **Object** > **Content Template** > **AI-based Threat Detection** > **Allowlist**.

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



(3) Enter the IP address to be added to the allowlist.



(4) Click **Save**.

5. Viewing AI-based Threat Detection Logs

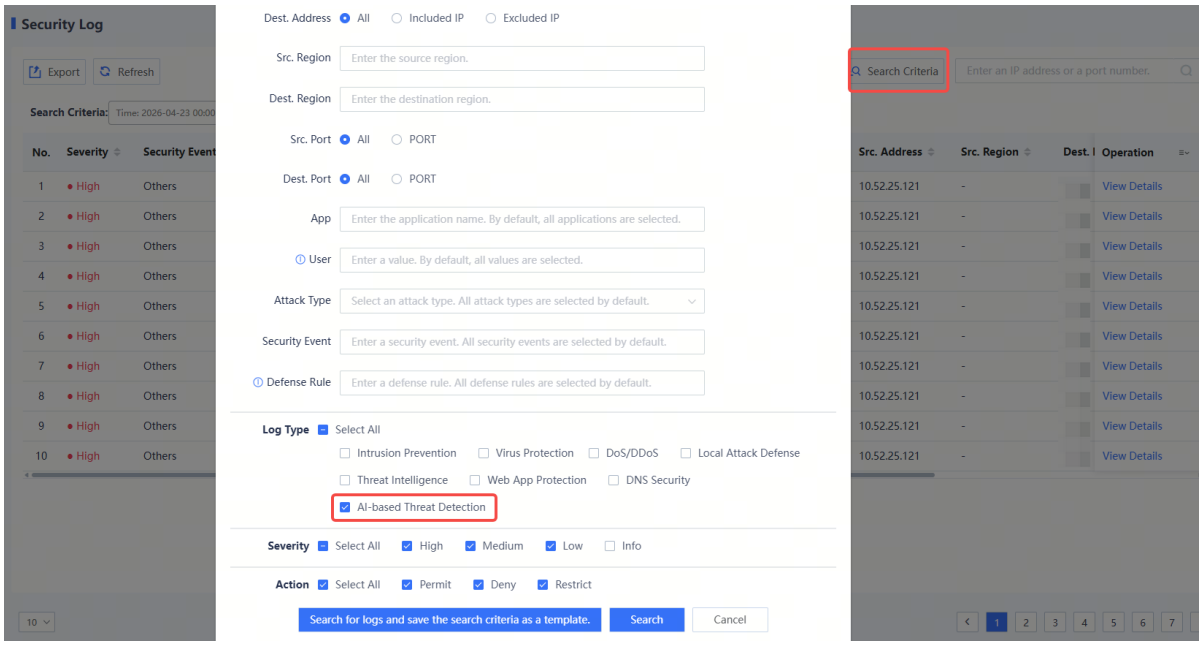
Application Scenario

If attack traffic matches an AI-based Threat Detection policy, the device generates a security log with the type marked as **AI-based Stealth Attack Detection**. You can view the detailed attack information and matching attack type in the logs to block or permit the traffic accordingly.

Procedure

(1) Choose **O&M** > **Logs** > **Security Log**.

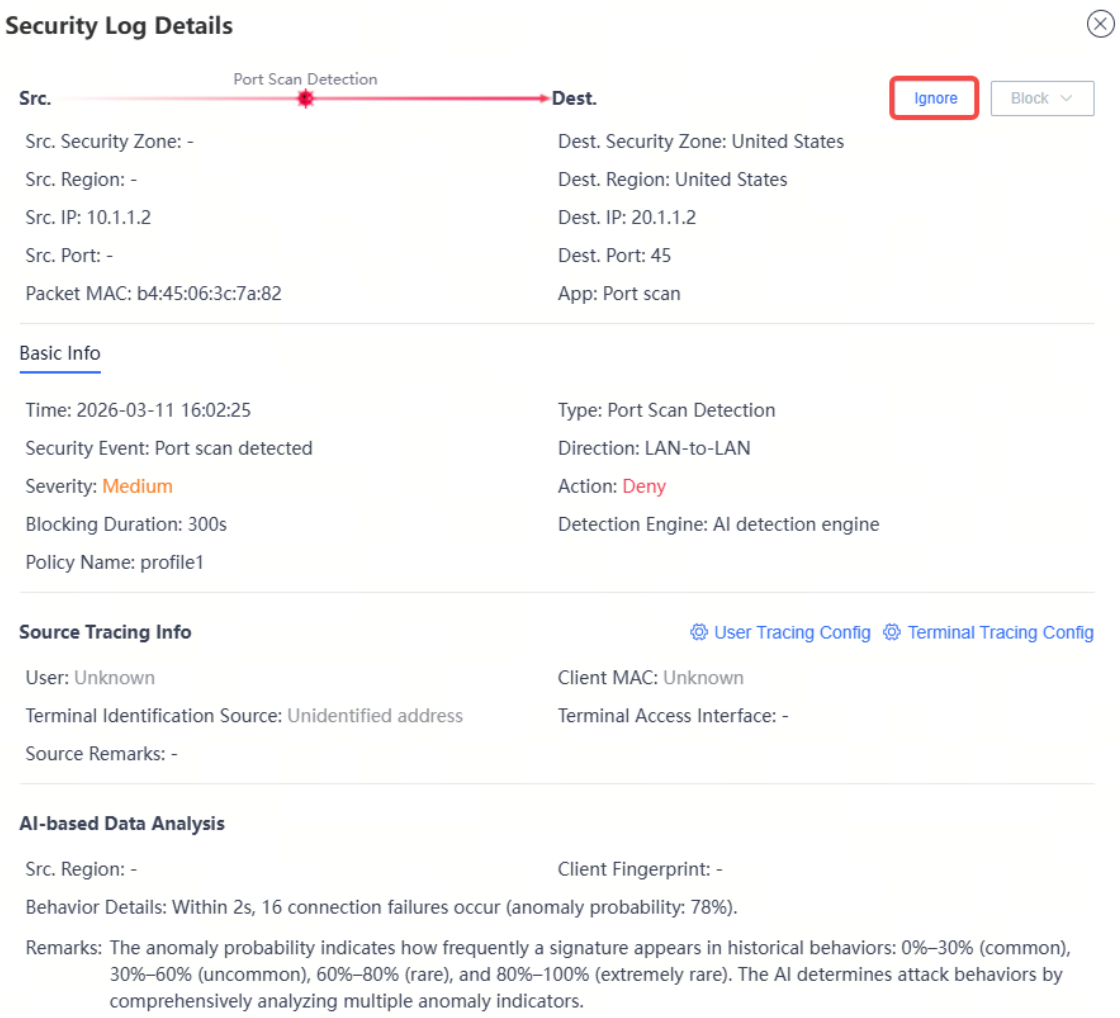
(2) Click **Search Criteria** and set **Log Type** to **AI-based Stealth Attack Detection**.

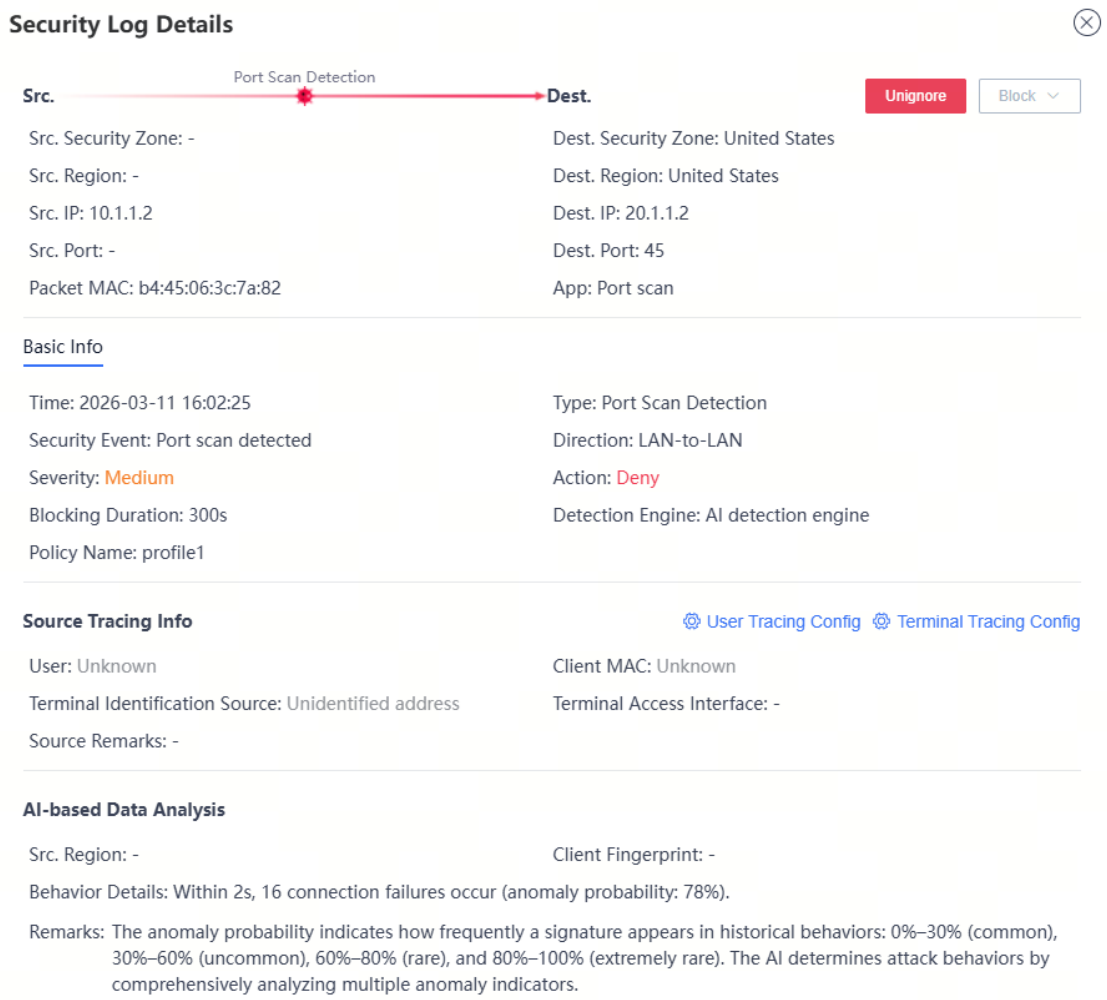


(3) Click **View Details** to view the detailed attack log.

If you confirm that the identified attack is false reported, click **Ignore**. The system automatically adds the source IP address matching the security log to the detection allowlist and removes that IP address from the temporary blocklist (**Policy** > **Blocklist and Allowlist** > **Temporary IPv4 Blocklist** or **Temporary IPv6 Blocklist**).

To remove the IP address from the detection allowlist, click **Unignore** or choose **Object** > **Content Template** > **AI-based Threat Detection** > **Allowlist** to delete the corresponding allowlist.


Security Log Details
Port Scan Detection
Src.
Dest.
Ignore
Block
Src. Security Zone: -
Dest. Security Zone: United States
Src. Region: -
Dest. Region: United States
Src. IP: 10.1.1.2
Dest. IP: 20.1.1.2
Src. Port: -
Dest. Port: 45
Packet MAC: b4:45:06:3c:7a:82
App: Port scan
Basic Info
Time: 2026-03-11 16:02:25
Type: Port Scan Detection
Security Event: Port scan detected
Direction: LAN-to-LAN
Severity: Medium
Action: Deny
Blocking Duration: 300s
Detection Engine: AI detection engine
Policy Name: profile1
Source Tracing Info
User Tracing Config
Terminal Tracing Config
User: Unknown
Client MAC: Unknown
Terminal Identification Source: Unidentified address
Terminal Access Interface: -
Source Remarks: -
AI-based Data Analysis
Src. Region: -
Client Fingerprint: -
Behavior Details: Within 2s, 16 connection failures occur (anomaly probability: 78%).
Remarks: The anomaly probability indicates how frequently a signature appears in historical behaviors: 0%–30% (common), 30%–60% (uncommon), 60%–80% (rare), and 80%–100% (extremely rare). The AI determines attack behaviors by comprehensively analyzing multiple anomaly indicators.



Note

For details about fields in the security log and more configuration, see 8.3.2 2. Querying Security Logs.

6. Upgrading the AI-based Threat Detection Engine Library

The AI-based Threat Detection engine library is continuously updated. You can upgrade the AI-based Threat Detection engine library to detect more types of stealth attacks. For details about signature library upgrade, see 7.5 Signature Library Upgrade.

5.10.8 Advanced Settings

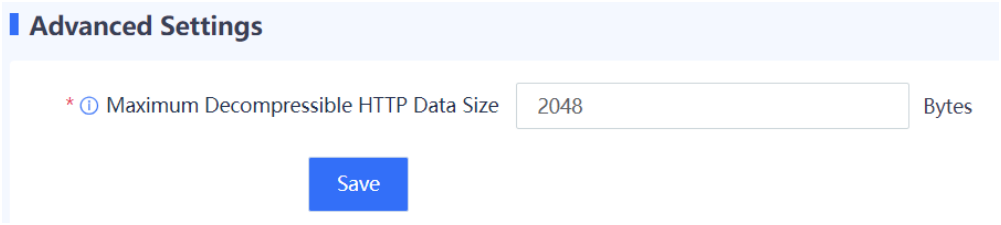
Application Scenario

The maximum decompressible HTTP data size refers to the maximum length of the HTTP body field that can be decompressed by application-layer resolution. The part that exceeds the maximum decompressible size is not decompressed. In scenarios where security detection services (such as intrusion prevention and keyword filtering) are required, if the configured maximum decompressible HTTP data size is too small, security detection services cannot be performed properly. However, a large value indicates that more system resources are required for decompressing the HTTP body field, which may affect the forwarding performance of the system. Therefore, you need to set this parameter to an appropriate value.

Procedure

(1) Choose **Object** > **Content Template** > **Advanced Settings**.

(2) Set the maximum decompressible HTTP data size.



(3) Click **Save**.

5.11 Security Rule Base Management

5.11.1 Intrusion Prevention Rule Base

Application Scenario

The intrusion prevention 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 intrusion prevention rule base. If matched, the device processes it according to user configuration.

The device has multiple predefined rules. You can also configure custom rules.

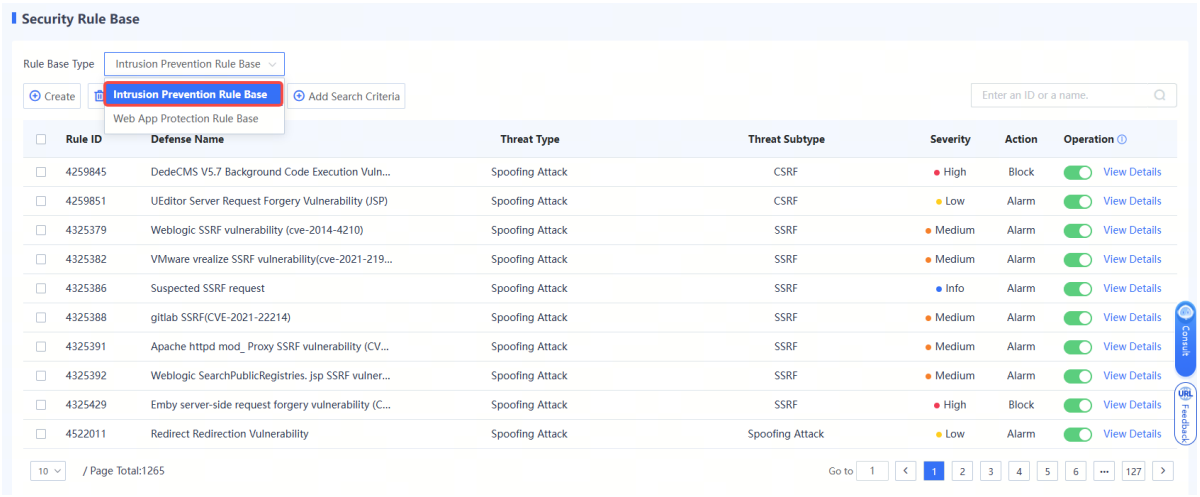
Note

- The custom rule configuration takes effect only when **Custom Rule** is selected in the IPS template referenced by the security policy.
- Only custom rules can be edited or deleted, and only predefined rules can be enabled or disabled.

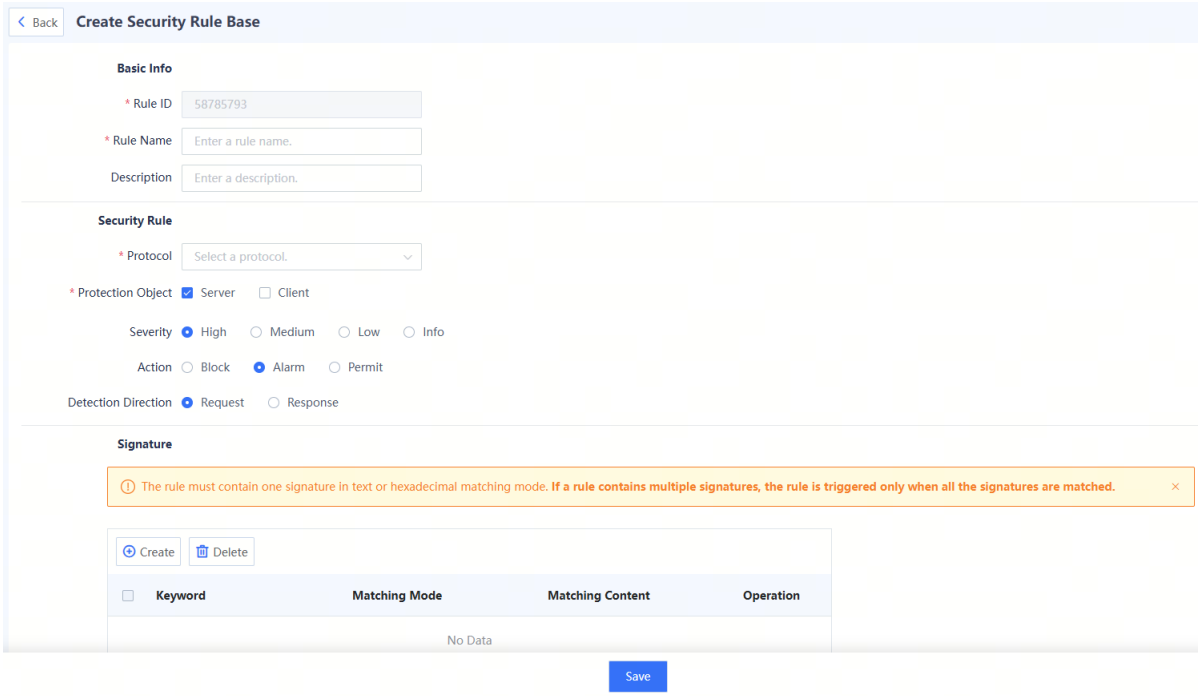
Procedure

(1) Choose **Object** > **Security Rule Base**.

(2) Select **Intrusion Prevention Rule Base** from the Rule Base Type drop-down list box.



(3) Click **Create** to add an intrusion prevention rule.



Item	Description	Remarks
Basic Info		
Rule ID	ID of the intrusion prevention rule.	The ID is automatically generated and cannot be modified.
Rule Name	Name of the intrusion prevention rule.	[Example] Filter1
Description	Description of the intrusion prevention rule.	-
Security Rule		
Protocol	Protocol of traffic to be detected. Traffic of the other protocols does not hit the rule.	Select a value from the drop-down list. [Example] DNS
Protection Object	Object to be protected.	[Example] Server
Severity	Severity of the attacks that hit the rule. **High**, **Medium**, **Low**, and **Notification** can be selected.	[Example] High

Item	Description	Remarks
Action	Action taken by the device on an attack that hits the rule. ● **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.	[Example] Block
Detection Direction	Direction of the traffic to be detected by the rule.	[Example] Request
Signature ● You can add signatures only after the protocol is configured. ● The rule must contain one signature in text or hexadecimal matching mode. ● If a rule contains multiple signatures, the rule is triggered only when all the signatures are matched. ● If you modify the protocol or detection direction, all signatures of this rule will be deleted. Exercise caution when performing this operation.		
Keyword	Protocol field to be detected.	Select a value from the drop-down list.
Matching Mode	Signature matching mode: ● **Text**: Text description is matched. ● **Regular Expression**: PCRE regular expression is matched. ● **Hexadecimal**: Hexadecimal content is matched.	Select a value from the drop-down list.
Matching Content	Signature matching content.	Enter signature matching content for the rule. If the matching mode is **Text**, matching content is case-insensitive by default. You can select **Case-Sensitive** to make the content case-sensitive.

(4) Click **Save**.

Follow-up Procedure

- The custom rule configuration takes effect only when **Custom Rule** is selected in the IPS template referenced by the security policy.
- You can select multiple custom rules and click **Delete** to delete them in a batch.
- After a predefined rule is enabled, the device detects the threats defined by the rule for the traffic passing the device.
- After a predefined rule is disabled, the device does not detect the threats defined by the rule for the traffic passing the device.
- Click **Add Search Criteria** to set search criteria to filter rules displayed on the page.

5.11.2 Web App Protection Rule Base

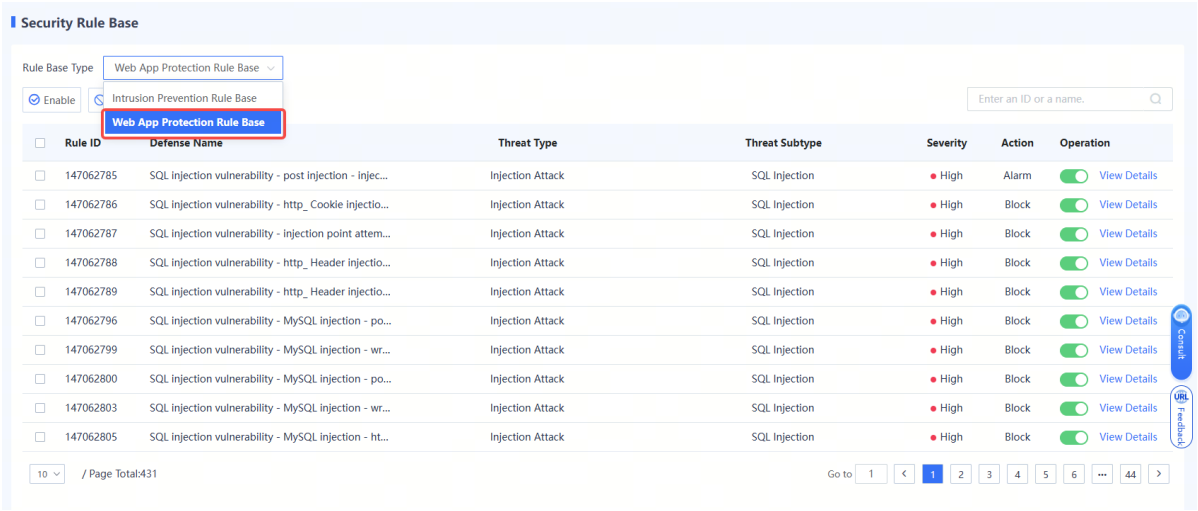
Application Scenario

The web app protection rule base (also called web app protection signature library) stores signature information of threats that can be detected by the device from traffic. When traffic passes through the device, the web app protection function compares the traffic with signature information in the web app protection rule base. If the traffic is matched as a threat, the device processes the traffic accordingly based on the user configuration.

Procedure

(1) Choose **Object** > **Security Rule Base**.

(2) Select **Web App Protection Rule Base** for **Rule Base Type**.



(3) Perform the action in the corresponding web app protection rule.

- Enable a rule and detect threats defined in the rule.
- Disable a rule and skip the rule during traffic detection.
- Click **Add Search Criteria** to customize the search criteria. Only rules matching the search criteria are displayed on the page.

6 Network Configuration

6.1 Interface

6.1.1 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.

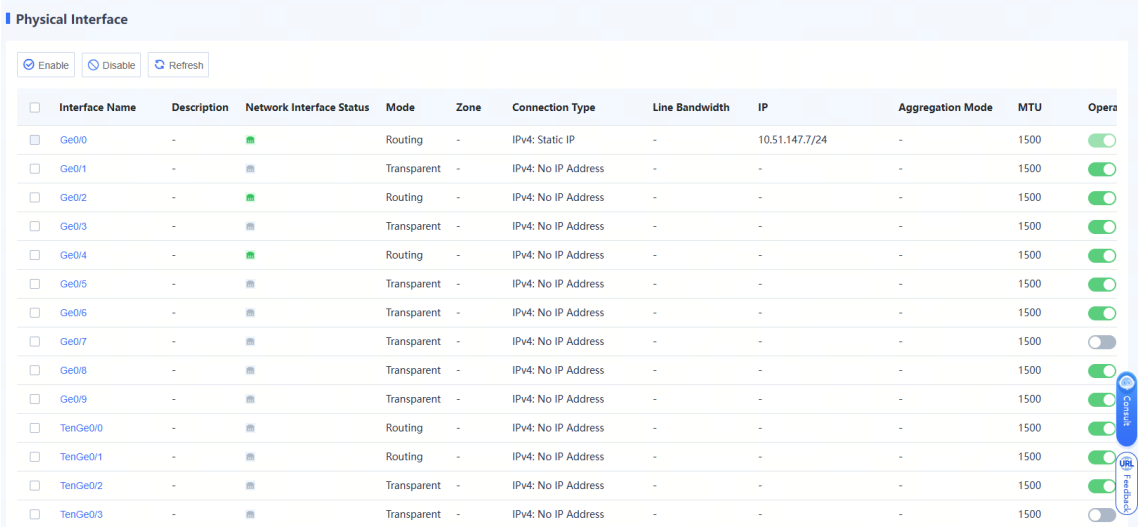
- If the ISP provides multiple PPPoE accounts and the ISP device supports multi-PPPoE, you can enable the multi-PPPoE function to allow multiple PPPoE accounts to perform dial-up over the same physical line. For details about the multi-PPPoE function, see 6.1.8 Multi-PPPoE.

Procedure

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

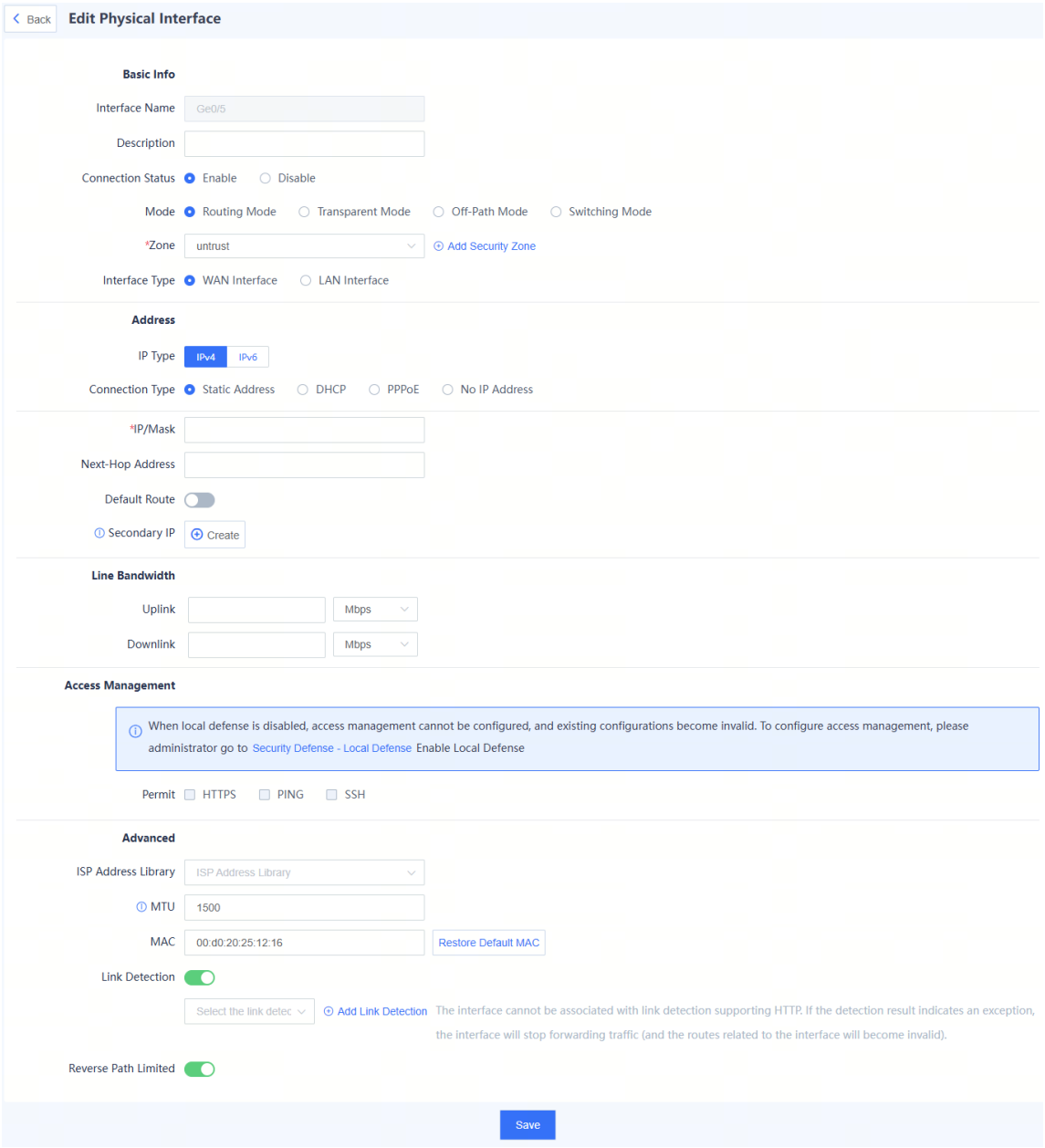
> **Caution**
>
> Disabling an interface or modifying the interface configuration may cause network interruption on all terminals connected to the interface. Exercise caution when performing this operation.

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.



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

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



(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 external network

Item	Description	Remarks
Connection Status	Enables or disables the interface.	[Example] Enable
Mode	Interface access mode. ● **Routing Mode**: The interface forwards traffic based on IP addresses. ● **Transparent Mode**: The interface forwards traffic based on MAC addresses. ● **Off-Path Mode**: The interface only receives mirrored traffic, but does not forward traffic. ● **Switching Mode**: The interface works at Layer 2 and forwards data based on MAC addresses. All interfaces in switching mode share the IP address of the switching interface. For details about switching interfaces, see 6.1.4 Configuring a Switching Interface.	The management interface cannot be set to the transparent mode, off-path mode, or switching mode. [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. ● The default bridge interface of the system is **br0**. To add a bridge interface, click **Add Bridge Interface**. For details about the configuration items, see 6.1.3 Configuring a Bridge Interface. [Example] br0
Switching Interface	Specifies the switching interface to which the interface in switching mode belongs.	● This parameter is valid when **Mode** is set to **Switching Mode**. ● The default value is **vswitch0**, which cannot be changed. For details about the switching interface, see 6.1.4 Configuring a Switching Interface.
Zone	Security zone to which the interface belongs.	[Example] trust
Interface Type	Logical attribute of the interface.	When the interface mode is set to **Switching Mode**, **Interface Type** can only be set to **LAN Interface**. [Example] LAN Interface
IP Type	IP address type of the interface. Valid values: **IPv4** and **IPv6**.	[Example] IPv4

Item	Description	Remarks
IPv4		
Connection Type	Network connection type of the interface. Valid values: **Static Address**, **DHCP**, and **PPPoE**. ● **Static Address**: Applicable when a planned IP address is allocated to the device. The IP address and mask must be manually configured. ● **DHCP**: Applicable when the DHCP server is deployed on an upstream device or ISP line. The interface can automatically obtain an IP address from the upper-level DHCP server. ● **PPPoE**: Applicable for dialup access to the ISP network. The username and password of the dialup user must be configured. If **No IP Address** is selected, the interface does not have an IP address. Ensure that other management channels are configured, for example, you can access the device through the IP address of another interface.	[Example] Static Address
Connection Type: 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	IP address of the next node for forwarding data.	This parameter is available when **Interface Type** is set to **WAN Interface** and **Connection Type** is set to **Static Address**. [Example] 192.168.1.2
Default Route	Whether to automatically generate and enable a default route.	This parameter is valid when **Interface Type** is set to **WAN Interface** and **Connection Type** is set to **Static Address**. To generate a default route, you must enter the next-hop address. [Example] Enable

Item	Description	Remarks
Secondary IP	Set a secondary IP address for the interface. An interface on the device can be configured with multiple IP addresses, of which one is the primary IP address and the others are secondary IP addresses. Secondary IP addresses can be used in a scenario where different service types need to be assigned to different IP subnets.	● This parameter is available when **Connection Type** is set to **Static Address**. ● Click **Create** to set the secondary IP address and mask. ● A secondary IP address cannot be the same as the primary IP address. [Example] 192.168.1.100/24
Connection Type: **PPPoE** (with multi-PPPoE disabled)		
Account	Account that is required to obtain an IP address through PPPoE.	When **Connection Type** is set to **PPPoE** and multi-PPPoE is disabled, you only need to set a single PPPoE account. [Example] Admin
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
Connection Type: **PPPoE** (with multi-PPPoE enabled) ● Click **Create** to add a PPPoE link. ● Select PPPoE links and click **Delete** to delete selected links. ● Enter the username of a PPPoE account in the search box in the upper right corner to query the PPPoE link configuration. Note: After you enable multi-PPPoE, one interface supports up to 48 PPPoE client sessions.		
PPPoE Username	Username for the PPPoE link.	-
PPPoE Password	Password for the PPPoE link.	-
Description	Description for the PPPoE link.	-
DHCP Service	Whether the DHCP server function is enabled on the interface to assign IPv4 addresses to connected devices.	This parameter is available when **Interface Type** is set to **LAN Interface** and **Connection Type** is set to **Static Address**. [Example] Enable

Item	Description	Remarks
IP Assignment Range	Range of IP addresses allocated by the DHCP server.	● Configure this parameter when the DHCP service is enabled. ● Enter an IP address range per line. ● Use a hyphen (-) between two IP addresses to specify a range. [Example] 192.168.1.1-192.168.1.10
Primary DNS Server	Primary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 192.168.10.1
Secondary DNS Server	Secondary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 192.168.30.1
Line Bandwidth	Bandwidth provided by ISP for the line, including the uplink bandwidth and dowlink bandwidth.	Enter the bandwidth value and select a unit. This parameter is available when **Interface Type** is set to **WAN Interface**. [Example] 100 Mbps
Access Management	Access management modes permitted by the PPPoE interface: ● **HTTPS**: Permit access to the interface through HTTPS. (If you need to log in to the web UI of the device using the interface address, select this option). ● **PING**: Permit access to the interface through ping. ● **SSH**: Permit access to the interface through SSH.	This configuration is valid when local defense is enabled on the device. [Example] Select **HTTPS**.
ISP Address Library	ISP of the line.	[Example] China Telecom
MTU	Maximum number of data bytes that can be sent by the PPPoE interface each time.	[Example] 1492
MAC	MAC address of the PPPoE interface.	[Example] 30:0d:9e:41:d9:0b

Item	Description	Remarks
Link Detection	Whether to enable link detection on the interface to test network connectivity of the link in real time. After this function is enabled, you need to select a link detection policy associated with the link. If the detection result is abnormal, the interface stops forwarding traffic and relevant routes of the interface become invalid.	You can associate the IPv4 address and IPv6 address of the interface with link detection objects separately. The IPv4 address can be associated with the link detection object with only one IPv4 detection node configured. The IPv6 address can be associated with the link detection object with only one IPv6 detection node configured. For details about link detection, see 6.14.1 Link Quality Detection.
Reverse Path Limited	After this function is enabled, the device uses the inbound interface of the corresponding request message as the outbound interface of the response message for forwarding and does not search the routing table. This ensures that the forward and reverse paths of the messages are consistent. In a scenario with multiple egresses, this function prevents the following issue: A request message enters over the ISP1 line, but the response message is returned over the ISP2 line, resulting in slow service access or even service interruption. This function takes effect only for new flows and does not take effect for traffic on the local device.	This function is enabled by default.
IPv6		
IPv6	When you set **IP Type** to **IPv6**, you must enable **IPv6**. Otherwise, the IPv6 address does not take effect.	N/A

Item	Description	Remarks
Connection Type	Mode for the physical interface to obtain an IPv6 address. When **Interface Type** is **WAN Interface**, the following modes are supported: static address, ND-RA, DHCP, and PPPoE. When **Interface Type** is **LAN Interface**, the following modes are supported: static address, ND-RA, DHCP, and prefix delegation.	● **Connection Type** can be set to **Prefix Delegation** for a LAN interface only when DHCPv6 prefix delegation is enabled on a WAN interface of the device (that is, the device can obtain an IPv6 address prefix pool from the DHCPv6 server). ● When **Connection Type** is set to **Prefix Delegation** for a LAN interface, RA is automatically enabled. In this case, the downstream terminals connected to the LAN interface can automatically obtain IPv6 addresses through SLAAC after being configured with this IPv6 address obtaining mode. [Example] Static Address
Prefix Pool ID	ID of the prefix pool bound to the interface in PD mode. The interface generates an IPv6 address based on the corresponding IPv6 address prefix pool.	● This parameter is available only when **Interface Type** is set to **LAN Interface** and **Connection Type** is set to **Prefix Delegation**. ● The prefix pool ID is manually specified when DHCPv6 prefix delegation is configured for the WAN interface. You can check the WAN interface configuration to obtain the prefix pool ID.
IP/Prefix Length	If the connection type of an interface is set to **Static Address**, this parameter needs to be set to specify the IPv6 address and prefix length of the interface. If the interface is a LAN interface and its connection type is **Prefix Delegation**, this parameter is used to configure the IPv6 address bound to DHCPv6 PD. The device generates the IPv6 address of the interface by combining the obtained prefix and the configured IPv6 address. If multiple interfaces are bound to the same prefix pool, their subnet IDs and interface IDs in the **IP/Prefix Length** value cannot be the same. Otherwise, different interfaces will generate the same IPv6 address, causing an address conflict. The prefix length must be 64 bits.	This parameter is available when **Connection Type** is set to **Static Address**. [Example] 2001::1/64

Item	Description	Remarks
Next-Hop Address	IP address of the next node for forwarding data.	This parameter is available when **Interface Type** is set to **WAN Interface** and **Connection Type** is set to **Static Address**. [Example] 2001::2
Account	PPPoE account when the interface uses PPPoE to obtain an IPv6 address.	This parameter is available when **Connection Type** is set to **PPPoE**.
Password	PPPoE password when the interface uses PPPoE to obtain an IPv6 address.	This parameter is available when **Connection Type** is set to **PPPoE**.
Default Route	Whether to enable the default route.	This parameter is available when **Interface Type** is set to **WAN Interface**. [Example] Enable
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	Configure a static neighbor entry. When one node attempts to communicate with another, it must obtain the link-layer address of the other. You can manually configure a static ND entry to resolve the IPv6 address of a neighbor node to a link-layer address.	Each ND entry consists of the IPv6 address and MAC address of a neighbor. Enter one or more lines to specify one or more ND entries. The input format is as follows: *ipv6-address mac-address* [Example] 1234::100 00:11:22:33:44:55
DHCP Service	Whether the DHCPv6 server function is enabled on the interface to assign IPv6 addresses to connected devices.	This parameter is available when IPv6 is enabled for the LAN interface and **Connection Type** of the LAN interface is set to **Static Address**. [Example] Enabled

Item	Description	Remarks
Primary DNS Server	Primary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 2001::1
Secondary DNS Server	Secondary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 2001::2
Advanced Address Settings Click to expand **Advanced IPv6 Settings**.		
Address Conflict Detection	Address conflict detection count. After address conflict detection is enabled, an interface sends Neighbor Solicitation (NS) packets to determine whether an IPv6 address is unique on the link, and performs address conflict detection again on the conflicting address based on the configured detection count and NS retransmission interval.	The value range is from 0 to 600. The value 0 indicates that conflict detection is disabled. [Example] 0
NS Retransmission 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	Prefix information that is advertised in the RA message. The following options can be configured: ● **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.
DHCPv6 Prefix Delegation Only WAN interfaces support this function.		
DHCPv6 Prefix Delegation	Configure the interface as a DHCPv6 client that applies for an IPv6 address prefix pool from the DHCPv6 server. The obtained IPv6 address prefix pool can be used to generate IPv6 addresses for LAN interfaces and intranet hosts.	[Example] Enabled
Prefix Pool ID	Specify a unique ID for the obtained IPv6 address prefix pool.	[Example] 1
Line Bandwidth	Interface bandwidth thresholds, including uplink and downlink bandwidth thresholds.	Enter the bandwidth value and select a unit. [Example] 100 kbps

Item	Description	Remarks
Access Management	Access management mode permitted for the specified interface. ● **HTTPS**: Permits interface access through HTTPS. (Select this option if you want to log in to the web UI of the device through the interface address.) ● **PING**: Permits interface access through Ping. **SSH**: Permits interface access through SSH.	The configuration takes effect when local defense is enabled on the device.
Advanced		
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 available when **Interface Type** is set to **WAN Interface** and **IP Type** is set to **IPv4**. [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.	[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.	This parameter is available when **Interface Type** is set to **WAN Interface** and **IP Type** is set to **IPv4**. For details about link detection, see 6.14.1 Link Quality Detection.
Reverse Path Limited	This function ensures that reverse traffic is sent back on the same path through the same interface and is enabled by default. After this function is enabled, it only takes effect on new traffic and does not take effect on local traffic.	[Example] Enable

(4) Click **Save**.

6.1.2 Configuring a Sub-interface

Application Scenario

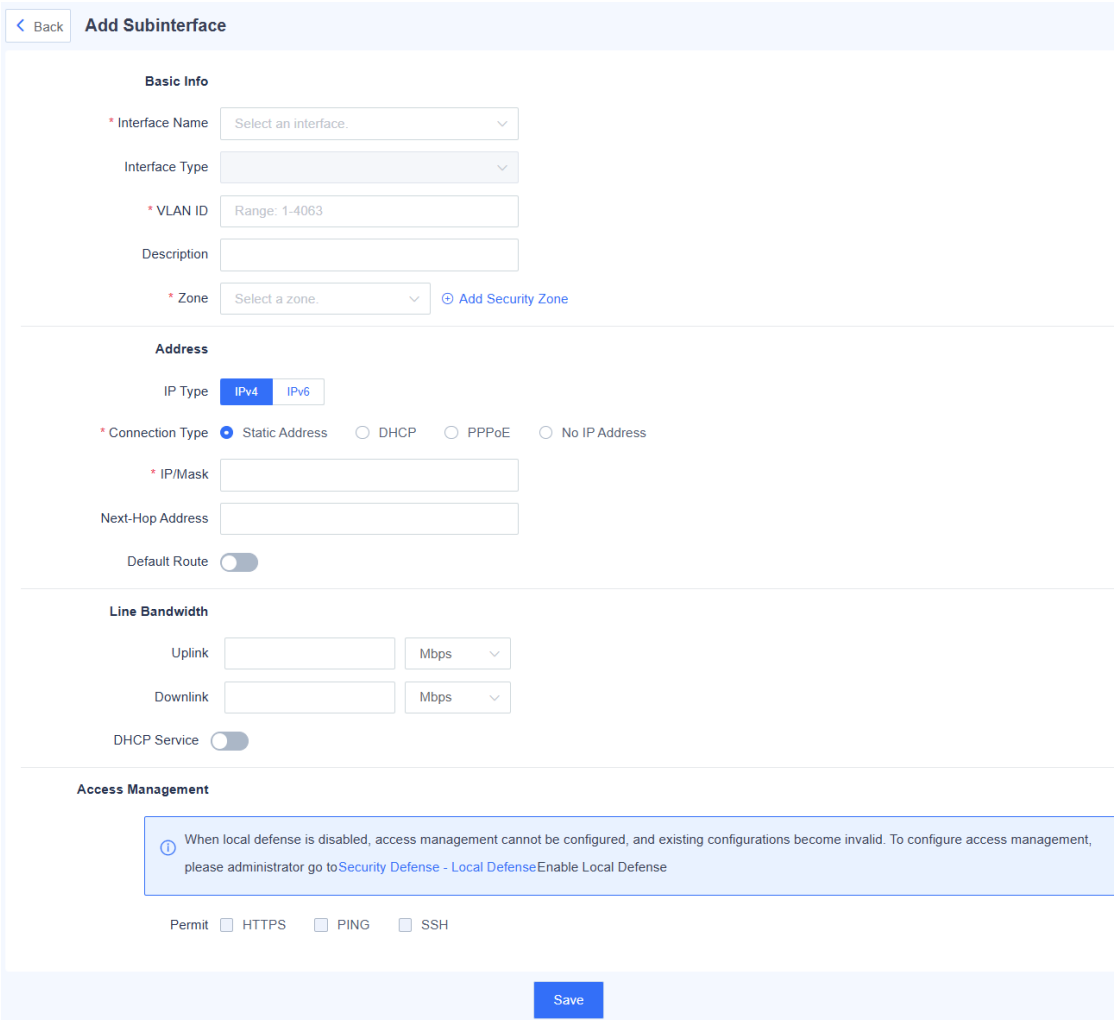
A sub-interface is a virtual interface created based on physical interface, switching interface, or aggregate interface, and is identified by VLAN. Upon receiving a packet, the physical interface, switching interface, or aggregate interface forwards the packet to the corresponding sub-interface for processing based on the VLAN field in the packet. To create multiple IP addresses for communication on a single physical interface, switching interface, or aggregate interface, you can create sub-interfaces on the local device and assign different VLAN IDs to them. On the peer device, create corresponding sub-interfaces to enable communication across subnets.

Procedure

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

(2) Click **Create**.

The **Add Subinterface** page is displayed.



(3) Set parameters for the sub-interface.

Item	Description	Remarks
Interface Name	Name of the interface on which a sub-interface needs to be created.	[Example] Ge0/1
Interface Type	Logical type of the sub-interface. By default, it is the same as that of the parent interface and cannot be modified.	The logical type of a sub-interface must be the same as that of the physical interface.
VLAN ID	VLAN ID that the sub-interface corresponds to.	[Example] 1
Description	Description of the sub-interface.	[Example] Interface connected to the external network.
Zone	Security zone to which the interface belongs.	[Example] trust
IP Type	IP address type of the sub-interface. Valid values are **IPv4** and **IPv6**.	[Example] IPv4
IPv4		
Connection Type	Mode used by the sub-interface to connect to the network. The following modes are supported: static address, DHCP, and PPPoE. If **No IP Address** is selected, the sub-interface does not have an IP address. Ensure that other management channels are configured, for example, you can access the device through the IP address of another interface.	The sub-interfaces of the switching interface cannot obtain IP addresses in PPPoE mode. [Example] Static Address
IP/Mask	Assigned IP address and mask for the sub-interface.	This parameter is valid when **Connection Type** is set to **Static Address**. [Example] 192.168.1.1/24
Next-Hop Address	IP address of the next node for forwarding data.	This parameter is available when **Interface Type** is set to **WAN Interface** and **Connection Type** is set to **Static Address**. [Example] 192.168.1.2

Item	Description	Remarks
Default Route	Whether to enable the default route.	This parameter is available when **Interface Type** is set to **WAN Interface** and **Connection Type** is set to **Static Address**. [Example] Enable
Secondary IP	Set a secondary IP address for the sub-interface.	● This parameter is available when **Connection Type** of the sub-interface is set to **Static Address**. ● Click **Create** to set the secondary IP address and mask. ● A secondary IP address cannot be the same as the primary IP address. [Example] 192.168.1.100/24
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
DHCP Service	Whether the DHCP server function is enabled on the sub-interface to assign IPv4 addresses to connected devices.	This parameter is available when the sub-interface is a LAN interface and **Connection Type** of the sub-interface is set to **Static Address**. [Example] Enable
IP Assignment Range	Range of IP addresses allocated by the DHCP server.	● Enter an IP address range per line. ● Use a hyphen (-) between two IP addresses to specify a range. ● Configure this parameter when the DHCP service is enabled. [Example] 192.168.1.1-192.168.1.10

Item	Description	Remarks
Primary DNS Server	Primary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 192.168.10.1
Secondary DNS Server	Secondary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 192.168.30.1
ISP Address Library	ISP network connected to the sub-interface. The sub-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 available when **Interface Type** is set to **WAN Interface** and **IP Type** is set to **IPv4**. [Example] China Telecom
MAC	MAC address of the interface.	This parameter is available when **Connection Type** is set to **PPPoE**. [Example] ae:9c:d1:f9:29:a5
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	Mode for the sub-interface to obtain an IPv6 address. When **Interface Type** is **WAN Interface**, the following modes are supported: static address, ND-RA, DHCP, and PPPoE. When **Interface Type** is **LAN Interface**, the following modes are supported: static address, ND-RA, DHCP, and prefix delegation.	● **Connection Type** can be set to **Prefix Delegation** for a LAN interface only when DHCPv6 prefix delegation is enabled on a WAN interface of the device (that is, the device can obtain an IPv6 address prefix pool from the DHCPv6 server). ● When **Connection Type** is set to **Prefix Delegation** for a LAN interface, RA is automatically enabled. In this case, the downstream terminals connected to the LAN interface can automatically obtain IPv6 addresses through SLAAC after being configured with this IPv6 address obtaining mode. [Example] Static Address

Item	Description	Remarks
Prefix Pool ID	ID of the prefix pool bound to the sub-interface in PD mode. The sub-interface generates an IPv6 address based on the corresponding IPv6 address prefix pool.	• This parameter is available only when **Interface Type** is set to **LAN Interface** and **Connection Type** is set to **Prefix Delegation**. • The prefix pool ID is manually specified when DHCPv6 prefix delegation is configured for the WAN interface. You can check the WAN interface configuration to obtain the prefix pool ID.
IP/Prefix Length	If the connection type of a sub-interface is set to **Static Address**, this parameter needs to be set to specify the IPv6 address and prefix length of the sub-interface. If the sub-interface is a LAN interface and its connection type is **Prefix Delegation**, this parameter is used to configure the IPv6 address bound to DHCPv6 PD. The device generates the IPv6 address of the sub-interface by combining the obtained prefix and the configured IPv6 address. If multiple interfaces are bound to the same prefix pool, their subnet IDs and interface IDs in the **IP/Prefix Length** value cannot be the same. Otherwise, different interfaces will generate the same IPv6 address, causing an address conflict. The prefix length must be 64 bits.	This parameter is valid when **Connection Type** is set to **Static Address**. [Example] 2001::1/64
Next-Hop Address	IP address of the next node for forwarding data.	This parameter is available when **Interface Type** is set to **WAN Interface** and **Connection Type** is set to **Static Address**. [Example] 2001::2
Account	PPPoE account when the sub-interface uses PPPoE to obtain an IPv6 address.	This parameter is available when **Connection Type** is set to **PPPoE**.
Password	PPPoE password when the sub-interface uses PPPoE to obtain an IPv6 address.	This parameter is available when **Connection Type** is set to **PPPoE**.
Default Route	Whether to enable the default route.	This parameter is available when **Interface Type** is set to **WAN Interface**. [Example] Enable

Item	Description	Remarks
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] Enabled
Static Neighbor Entry	Configure a static neighbor entry. When one node attempts to communicate with another, it must obtain the link-layer address of the other. You can manually configure a static ND entry to resolve the IPv6 address of a neighbor node to a link-layer address.	Each ND entry consists of the IPv6 address and MAC address of a neighbor. Enter one or more lines to specify one or more ND entries. The input format is as follows: *ipv6-address mac-address* [Example] 1234::100 00:11:22:33:44:55
DHCP Service	Whether the DHCPv6 server function is enabled on the interface to assign IPv6 addresses to connected devices.	This parameter is available when the sub-interface is a LAN interface, IPv6 is enabled for the sub-interface, and **Connection Type** of the sub-interface is set to **Static Address**. [Example] Enabled
Primary DNS Server	Primary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 2001::1
Secondary DNS Server	Secondary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 2001::2
Advanced Address Settings Click to expand **Advanced IPv6 Settings**.		

Item	Description	Remarks
Address Conflict Detection	Address conflict detection count. After address conflict detection is enabled, an interface sends NS packets to determine whether an IPv6 address is unique on the link, and performs address conflict detection again on the conflicting address based on the configured detection count and NS retransmission interval.	The value range is from 0 to 600. The value 0 indicates that conflict detection is disabled. [Example] 0
NS Retransmission 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	Prefix information that is advertised in the RA message. The following options can be configured: ● **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.
Access Management	Whether the interface supports HTTPS, ping, and SSH.	The configuration takes effect when local defense is enabled on the device.
MAC	MAC address of the sub-interface. By default, a sub-interface inherits the MAC address of its parent interface (physical interface). To prevent PPPoE dialup exceptions caused by restrictions of an ISP on dialup requests with the same MAC address, you are advised to modify the MAC address of the sub-interface.	● This parameter is available when **Connection Type** of the IPv4 address is set to **PPPoE**. ● Click **Auto MAC Address** to obtain a new MAC address for the sub-interface. [Example] ae:9c:d1:f9:29:a5
DHCPv6 Prefix Delegation Only WAN interfaces support this function.		
DHCPv6 Prefix Delegation	Configure the sub-interface as a DHCPv6 client that applies for an IPv6 address prefix pool from the DHCPv6 server. The obtained IPv6 address prefix pool can be used to generate IPv6 addresses for LAN interfaces and intranet hosts.	[Example] Enabled

Item	Description	Remarks
Prefix Pool ID	Specify a unique ID for an obtained IPv6 address prefix pool.	[Example] 1
Line Bandwidth	Bandwidth provided by ISP for the line, including the uplink bandwidth and dowlink bandwidth.	Enter the bandwidth value and select a unit. [Example] 100 Mbps
Before performing the following configurations, create a subinterface first. Then, click **Edit** in the **Operation** column of the subinterface and proceed with the configuration.		
MTU	Maximum number of data bytes for individual packets transmitted on the sub-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.	[Example] 1500
Link Detection	Link detection policy associated with the local sub-interface. This configuration can detect the network connectivity between the interface and the next hop in real time.	This parameter is available when **Interface Type** is set to **WAN Interface** and **IP Type** is set to **IPv4**. For details about link detection, see 6.14.1 Link Quality Detection.

(4) Click **Save**.

Follow-up Procedure

- On the **Subinterface** page, you can delete or modify sub-interfaces.

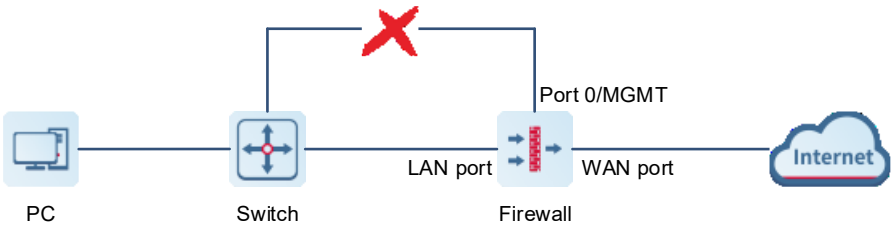
6.1.3 Configuring a Bridge Interface

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 can correctly configure an IP address and gateway to remotely manage the firewall through the IP address of the bridge interface. In actual networking, you do not need to separately connect port 0/MGMT to devices such as the switch. Remote O&M can be implemented through the bridge interface, which is easy to implement.

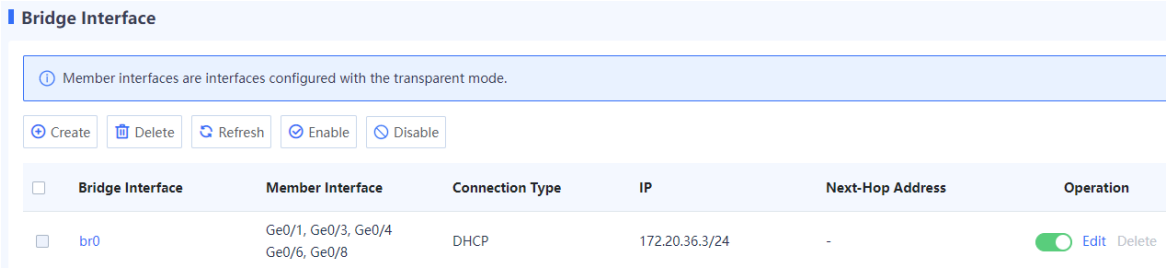
The firewall supports multiple groups of bridge interfaces, and traffic of the bridge groups is isolated from one another.



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.



Note

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

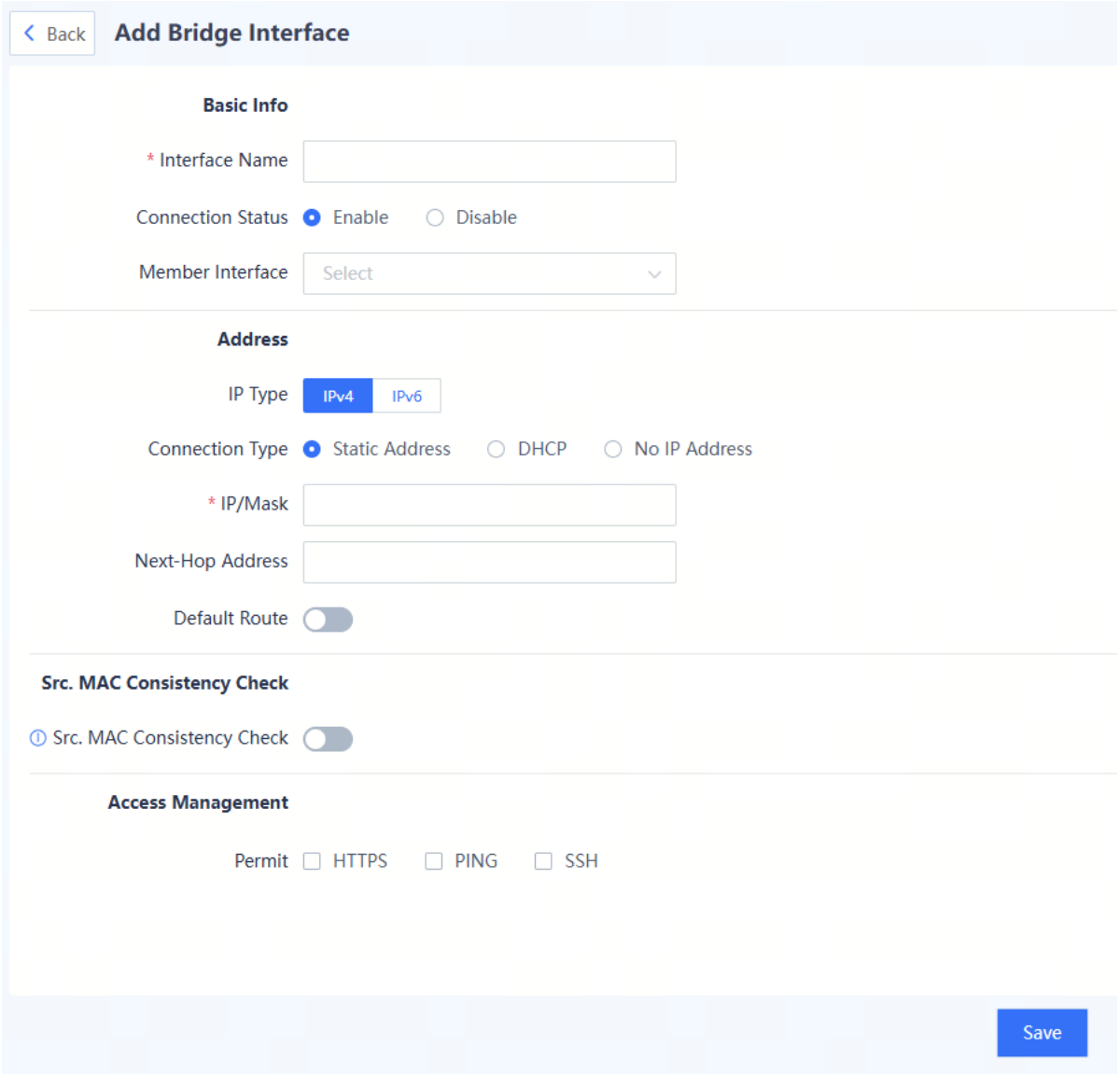
(2) Perform the corresponding operation on the bridge interface based on service requirements.

- 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**.



Item	Description	Remarks
Interface Name	Name of a bridge interface.	The name is specified when you create a bridge interface and cannot be modified in later steps. [Example] br1
Connection Status	Whether to enable the bridge interface.	[Example] Enable

Item	Description	Remarks
Member Interface	Member interface in the bridge interface. Members of the bridge interface are interfaces set to transparent mode. One bridge interface can contain multiple transparent interfaces, but each transparent interface can belong to only one bridge interface.	To add a member to the bridge interface, set **Bridge Interface** to the current bridge interface when you configure the corresponding member interface (such as a physical interface or aggregate interface). [Example] Ge0/2
Address		
IP Type	IP address type of the sub-interface. Valid values are **IPv4** and **IPv6**.	[Example] IPv4
IP Type: IPv4		
Connection Type	Connection type for the bridge interface, including: ● **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. ● **No IP Address**: Applicable when no IP address needs to be configured for the bridge interface. In this mode, you cannot access or manage the device through the bridge interface. Therefore, ensure that another management channel (for example, the IP address of another interface) has been configured for accessing the device.	[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

Item	Description	Remarks
Next-Hop Address	IP address of the next node for forwarding data.	You need to set this parameter when **Connection Type** is set to **Static Address**. [Example] 192.168.20.2
Default Route	Whether to enable the default route.	This parameter is available when **Connection Type** is set to **Static Address**. To generate a default route, you must enter the next-hop address. [Example] Enabled
IP Type: 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	Method used by the interface to obtain an IPv6 address. ● **Static Address**: Specifies an IPv6 address for the interface through manual configuration. ● **ND-RA**: Allows the interface to automatically obtain an IPv6 address through ND-RA. ● **DHCP**: Allows the interface to automatically obtain an IPv6 address through DHCPv6.	[Example] Static Address
IP/Prefix Length	IPv6 address and prefix length of the interface.	You need to configure this parameter when **Connection Type** is set to **Static Address**. [Example] 2001::1/64
Next-Hop Address	IP address of the next node to which the interface forwards data.	You can configure this parameter when **Connection Type** is set to **Static Address**. [Example] 2001::2
Default Route	Whether to automatically generate default routes.	[Example] Enable

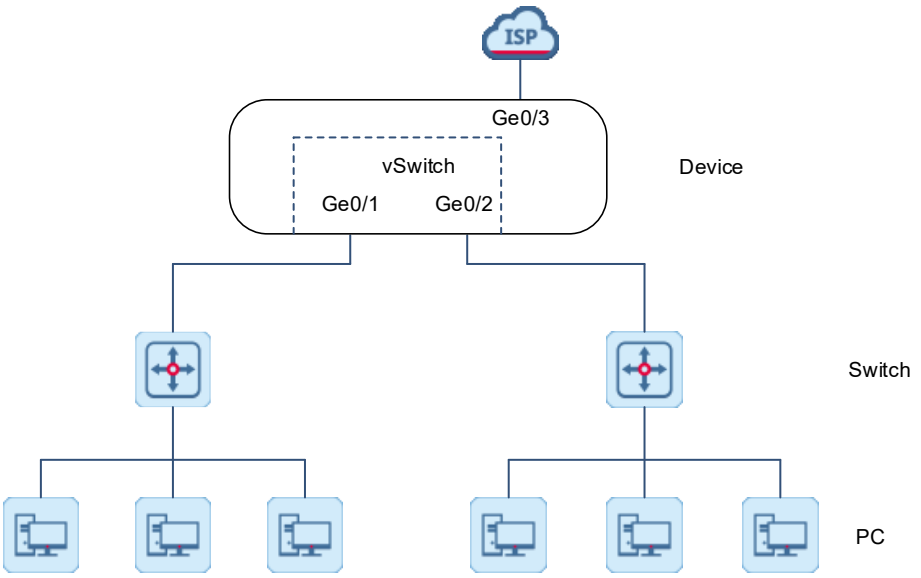
Item	Description	Remarks
Link-Local Address	Link-local address of the interface, which is automatically generated by the device.	-
Static Neighbor Entry	Static ND entry of the interface. When one node attempts to communicate with another, it must obtain the link-layer address of the other. You can manually configure a static ND entry to resolve the IPv6 address of a neighbor node to a link-layer address.	Each ND entry consists of the IPv6 address and MAC address of a neighbor. Enter one or more lines to specify one or more ND entries. The input format is as follows: *ipv6-address mac-address* [Example] 1234::100 00:11:22:33:44:55
Address Conflict Detection	Address conflict detection count. After address conflict detection is enabled, an interface sends NS packets to determine whether an IPv6 address is unique on the link, and performs address conflict detection again on the conflicting address based on the configured detection count and NS retransmission interval.	The value range is from 0 to 600. The value 0 indicates that conflict detection is disabled. [Example] 0
NS Retransmission Interval	Interval for sending two NS messages. If a device does not receive any response within a specified interval after sending an NS message, the device sends an NS message again.	The value range is from 1000 to 4294967295, in milliseconds. [Example] 1000
RS Sending Interval	Interval between two periodically sent RS messages.	The value range is from 4 to 3600, in seconds. [Example] 3600
Src. MAC Consistency Check	Whether to enable source MAC address consistency check. This function enables the interface to check whether the source MAC address of a packet is consistent with that in the session. If not, the session state of the packet is not checked, and the packet is transparently forwarded over the bridge network.	[Example] Enabled

Item	Description	Remarks
Access Management	Whether the bridge interface supports HTTPS, ping, and SSH. Select **HTTPS** if you want to log in to the device through the IP address of the bridge interface.	The configuration takes effect when local defense is enabled on the device. [Example] Select **HTTPS**.

6.1.4 Configuring a Switching Interface

Application Scenario

A vSwitch is a virtual logical interface composed of physical interfaces in switching mode. The IP address of the switching interface is used as the gateway address for downstream network devices and hosts. By correctly configuring the IP address and gateway on the switching interface, you can enable the internal hosts connected to the switching interface to communicate at Layer 3.



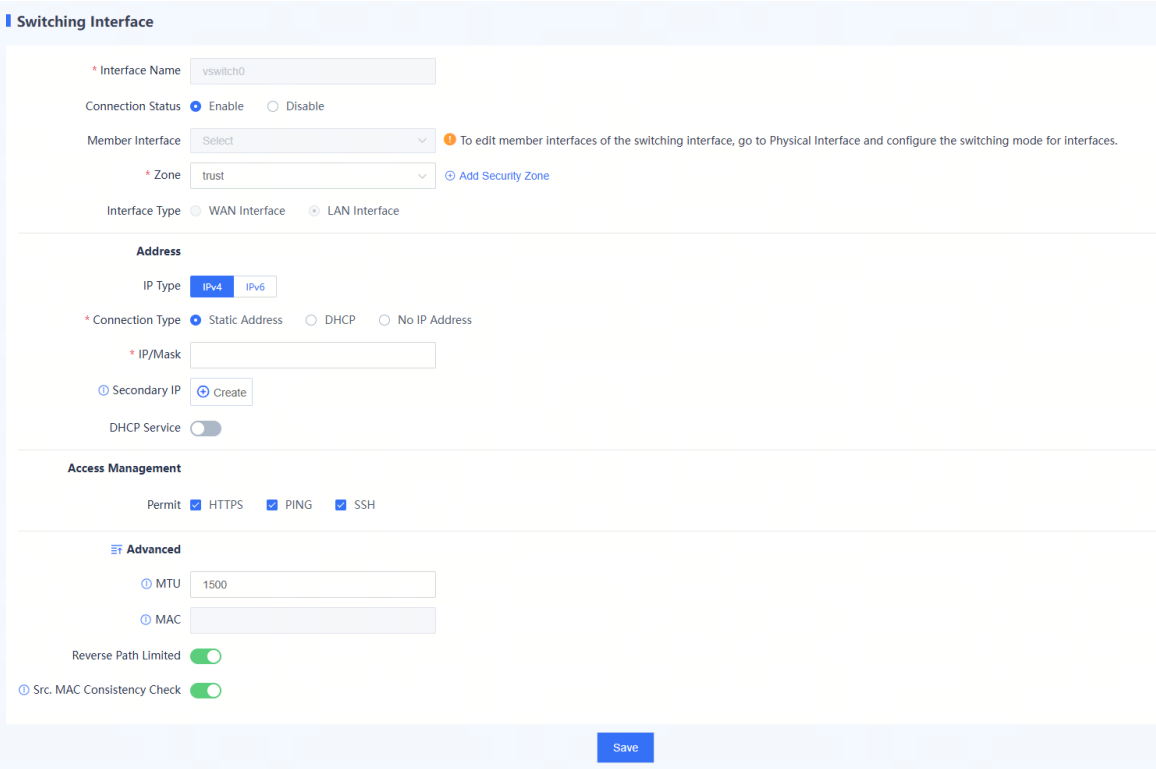
Note

The default switching interface of the system is **vswitch0**, which cannot be deleted. Switching interfaces cannot be added.

Procedure

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

(2) Configure the switching interface.



Item	Description	Remarks
Interface Name	Name of the switching interface, which is **vswitch0** by default and cannot be modified.	-
Connection Status	Whether the interface is enabled.	[Example] Enabled
Member Interface	The member interfaces of the switching interface include all interfaces in switching mode. To edit member interfaces, choose **Network** > **Interface** > **Physical Interface** and modify the interface modes of physical interfaces.	Interfaces in switching mode are automatically added to **vswitch0**.
Zone	Security zone to which the interface belongs.	[Example] trust
Interface Type	Logical attribute of the interface: ● **LAN Interface**: connects to an internal network. ● **WAN Interface**: connects to an external network, such as the internet.	The switching interface is a LAN interface by default.
Address		
IP Type	IP address type of the interface. Valid values: **IPv4** and **IPv6**.	-

Item	Description	Remarks
IPv4		
Connection Type	Mode for the switching interface to obtain an IPv4 address. Valid values: **Static Address** and **DHCP**. If **No IP Address** is selected, the interface does not have an IP address and cannot be used to access and manage the device. In this case, ensure that the local device can be accessed through the IP address of another interface. Otherwise, the device cannot be accessed or configured.	[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] 192.168.1.1/255.255.255.0
Secondary IP	Set a secondary IP address for the interface. An interface on the device can be configured with multiple IP addresses, of which one is the primary IP address and the others are secondary IP addresses. Secondary IP addresses can be used in a scenario where different service types need to be assigned to different IP subnets.	● Click **Create** to set the secondary IP address and mask. ● A secondary IP address cannot be the same as the primary IP address.
DHCP Service	Whether the DHCP server function is enabled on the switching interface to assign IPv4 addresses to connected devices.	This parameter is available when **Interface Type** is set to **LAN Interface** and **Connection Type** is set to **Static Address**. [Example] Enabled
IP Assignment Range	Range of IP addresses allocated by the DHCP server.	● Configure this parameter when the DHCP service is enabled. ● Enter an IP address range per line. ● Use a hyphen (-) between two IP addresses to specify a range. ● [Example] 192.168.1.1-192.168.1.10

Item	Description	Remarks
Primary DNS Server	Primary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 192.168.10.1
Secondary DNS Server	Secondary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 192.168.30.1
IPv6		
IPv6	When you set **IP Type** to **IPv6**, you must enable **IPv6**. Otherwise, the IPv6 address does not take effect.	-
Connection Type	Mode for the switching interface to obtain an IPv6 address. Valid values: **Static Address**, **ND-RA**, and **DHCP**.	[Example] Static Address
IP/Prefix Length	IPv6 address and network 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 by the device.	-
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
Static Neighbor Entry	Configure a static neighbor entry. When one node attempts to communicate with another, it must obtain the link-layer address of the other. You can manually configure a static ND entry to resolve the IPv6 address of a neighbor node to a link-layer address.	Each ND entry consists of the IPv6 address and MAC address of a neighbor. Enter one or more lines to specify one or more ND entries. The input format is as follows: *ipv6-address mac-address* [Example] 1234::100 00:11:22:33:44:55

Item	Description	Remarks
Advanced Address Settings Click  to expand **Advanced Address Settings**.		
Address Conflict Detection	Address conflict detection count. After address conflict detection is enabled, an interface sends NS packets to determine whether an IPv6 address is unique on the link, and performs address conflict detection again on the conflicting address based on the configured detection count and NS retransmission interval.	The value range is from 0 to 600. The value 0 indicates that conflict detection is disabled. [Example] 0
NS Retransmission Interval	Interval for sending two NS messages. If a device does not receive any response within a specified interval after sending an NS message, the device sends an NS message again.	The value range is from 1000 to 4294967295, in milliseconds. [Example] 1000
RA Sending Interval	Interval between two periodically sent RA messages.	The value range is from 1 to 1800, in seconds. [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.	The value range is from 0 to 9000, in seconds. [Example] 1800
RA Reachable Time	Period in which the device regards a neighbor reachable after detecting the neighbor reachability event.	The value range is from 1 to 3600000, in milliseconds. [Example] 30000

Item	Description	Remarks
RA Prefix Info	Configure the address prefix to be advertised in an RA message: ● **Address**: Address prefix. ● **Effective Time**: Time considered valid by a host after receiving the prefix in an RA message, in seconds. ● **Preferred Time**: Lifetime considered valid by a host when the host receives the prefix in an RA message, in seconds. ● **Enable Router Address Flag**: If this field is enabled, the prefix address field contains the prefix and address of the router sending the RA message. ● **Enable Direct Route Flag**: If this field is enabled, the address prefix can be used as on-link determination. That is, if the prefix of the destination address in an IPv6 packet sent by a host matches the configured prefix, the destination address is directly reachable on the same link (on-link). If this field is disabled, the prefix is not used for on-link determination. ● **Enable Auto Config Flag**: If this field is enabled, the prefix is used for SLAAC. Otherwise, it is used for stateful address autoconfiguration.	Click **Create** to add an RA prefix.
DHCP Service	Whether the DHCPv6 server function is enabled on the switching interface to assign IPv6 addresses to connected devices.	This parameter is available when **Interface Type** is set to **LAN Interface**, IPv6 is enabled for the interface, and **Connection Type** of the interface is set to **Static Address**. [Example] Enabled
Primary DNS Server	Primary DNS server used by the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 2001::1
Secondary DNS Server	Secondary DNS server used by the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 2001::2
Access Management		

Item	Description	Remarks
Access Management	Access management modes permitted by the interface: ● **HTTPS**: Permit access to the interface through HTTPS. (If you need to log in to the web UI of the device using the interface address, select this option). ● **PING**: Permit access to the interface through ping. ● **SSH**: Permit access to the interface through SSH. When **IP Type** is set to **IPv6**, you can enable the ping mode only.	This configuration is valid when local defense is enabled on the device. [Example] Select **HTTPS**.
Advanced		
MTU	Maximum number of data bytes in a single transmitted packet.	● It is an integer in the range of 1280 to 1600. ● The default value is 1500. [Example] 1500
MAC	MAC address of the interface, which is automatically set to the MAC address of a member interface.	This parameter cannot be manually configured. [Example] 30:0d:9e:41:d9:0b
Reverse Path Limited	This function ensures that reverse traffic is sent back on the same path through the same interface. In a scenario with multiple egresses, this function prevents the following issue: A request message enters over the ISP1 line, but the response message is returned over the ISP2 line, resulting in slow service access or even service interruption. This function takes effect only for new flows and does not take effect for traffic on the local device.	This function is enabled by default.
Src. MAC Consistency Check	This function enables the interface to check whether the source MAC address of a packet is consistent with that in the session. If not, the session state of the packet is not checked, and the packet is transparently forwarded over the bridge network.	[Example] Enabled

(3) Click **Save**.

6.1.5 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.

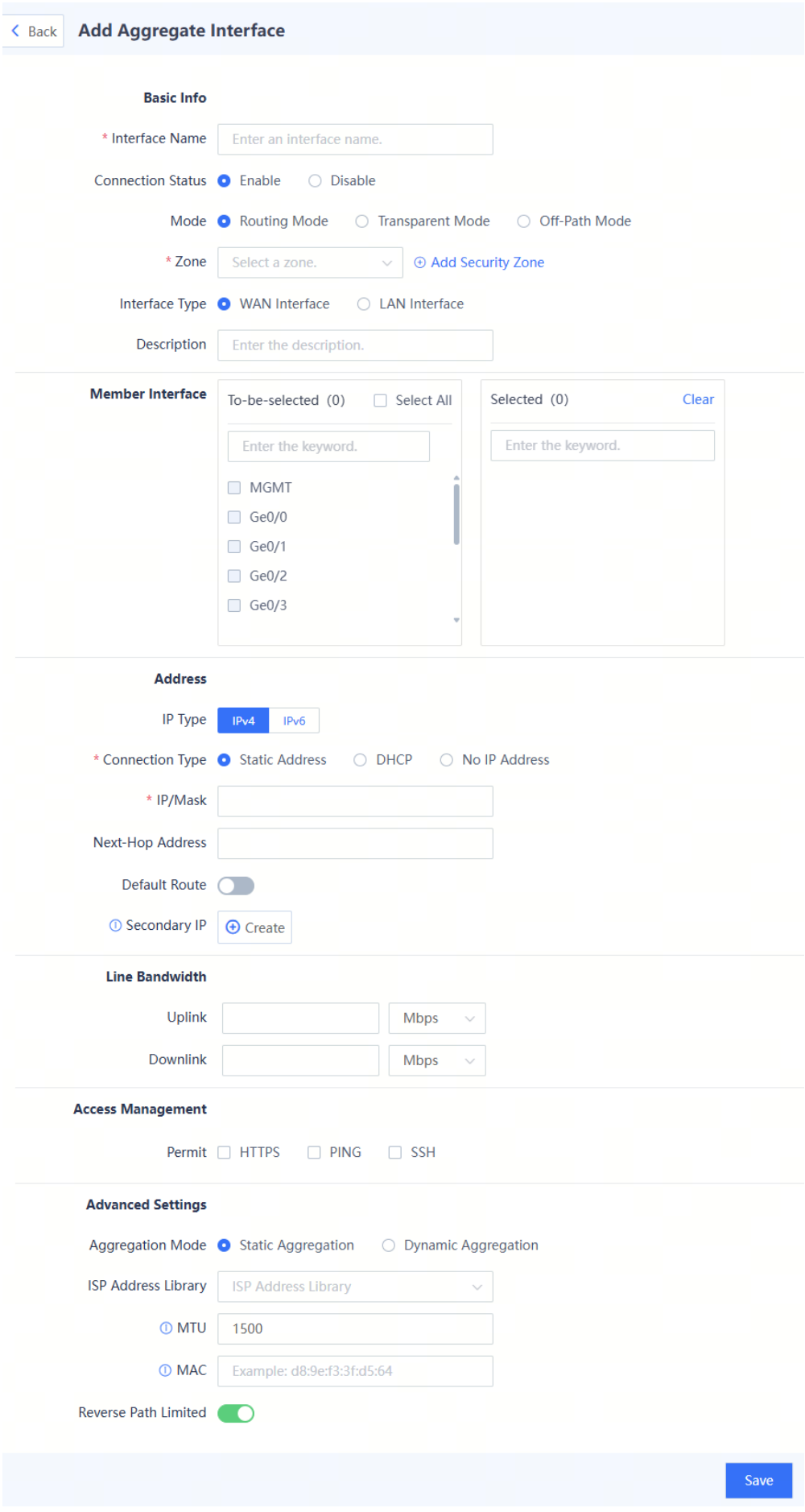
- If the bandwidth of the link between two devices can reach 1,000 Mbps (assuming that the interface rate of both devices is 1,000 Mbps), when the service traffic carried on the link exceeds 1,000 Mbps, the excess traffic is discarded. An aggregate interface can solve the problem of insufficient bandwidth: 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 x n.
- When two devices are connected by a single network cable, if the link is disconnected, the services carried on the link will be interrupted. However, when multiple connected interfaces are aggregated and bound, if one member link is disconnected, the device automatically distributes the traffic of the faulty link to other member links. As long as one link is working, the services carried on these interfaces will not be interrupted.

Procedure

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

(2) Click **Create**.

The **Add Aggregate Interface** page is displayed.


Back
Add Aggregate Interface
Basic Info
* Interface Name
Enter an interface name.
Connection Status
Enable
Disable
Mode
Routing Mode
Transparent Mode
Off-Path Mode
* Zone
Select a zone.
Add Security Zone
Interface Type
WAN Interface
LAN Interface
Description
Enter the description.
Member Interface
To-be-selected (0)
Select All
Enter the keyword.
MGMT
Ge0/0
Ge0/1
Ge0/2
Ge0/3
Selected (0)
Clear
Enter the keyword.
Address
IP Type
IPv4
IPv6
* Connection Type
Static Address
DHCP
No IP Address
* IP/Mask
Next-Hop Address
Default Route
Secondary IP
Create
Line Bandwidth
Uplink
Mbps
Downlink
Mbps
Access Management
Permit
HTTPS
PING
SSH
Advanced Settings
Aggregation Mode
Static Aggregation
Dynamic Aggregation
ISP Address Library
ISP Address Library
MTU
1500
MAC
Example: d8:9e:f3:3f:d5:64
Reverse Path Limited
Save

(3) Set parameters of aggregate interface.

Caution

- Only physical interfaces of the same type and bandwidth support aggregation; physical interfaces of different types and bandwidths do not support aggregation. For example, 1000M RJ45 interfaces and 1000M optical interfaces cannot be aggregated, and 1000M optical interfaces and 10G optical interfaces cannot be aggregated.
- 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.

Item	Description	Remarks
Interface Name	Name of the aggregate interface.	The interface name can contain only uppercase and lowercase letters and numbers. [Example] Ag1
Connection Status	Enables or disables the interface.	[Example] Enable
Mode	Interface access mode. ● **Routing** Mode: forwards traffic based on IP addresses. ● **Transparent Mode**: forwards traffic based on MAC addresses. ● **Off-Path Mode**: only receives mirrored traffic, but does not forward traffic.	[Example] 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.	[Example] Expand egress bandwidth.

Item	Description	Remarks
Member Interface	Physical interface that is added to the aggregate interface.	Up to 8 member interfaces can be included. [Example] Ge0/1
IP Type	IP address type of an interface, which can be IPv4 or IPv6.	[Example] IPv4
IPv4		
Connection Type	IP address obtaining method of the interface. Valid values: **Static Address** and **DHCP**. If **No IP Address** is selected, the aggregate interface does not have an IP address. In this case, ensure that another management channel is configured, for example, you can access the device using the IP address of another interface.	[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
Secondary IP	Set a secondary IP address for the aggregate interface.	• This parameter is available when **Connection Type** is set to **Static Address**. • Click **Create** to set the secondary IP address and mask. • A secondary IP address cannot be the same as the primary IP address. [Example] 192.168.1.100/24
Next-Hop Address	IP address of the next node for forwarding data.	This parameter is available when **Interface Type** is set to **WAN Interface** and **Connection Type** is set to **Static Address**. [Example] 192.168.1.2

Item	Description	Remarks
Default Route	Whether to generate the default route.	This parameter is available when **Interface Type** is set to **WAN Interface** and **Connection Type** is set to **Static Address**. [Example] Enabled
DHCP Service	Whether the DHCP server function is enabled on the aggregate interface to assign IPv4 addresses to connected devices.	This parameter is available when the aggregate interface is a LAN interface and **Connection Type** of the aggregate interface is set to **Static Address**. [Example] Enable
IP Assignment Range	Range of IP addresses allocated by the DHCP server.	● Configure this parameter when the DHCP service is enabled. ● Enter an IP address range per line. ● Use a hyphen (-) between two IP addresses to specify a range. [Example] 192.168.1.1-192.168.1.10
Primary DNS Server	Primary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 192.168.10.1
Secondary DNS Server	Secondary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 192.168.30.1
IPv6		
IPv6	When **IP Type** is set to **IPv6**, IPv6 must be enabled. Otherwise, IPv6 addresses do not take effect.	-

Item	Description	Remarks
Connection Type	Mode for the aggregate interface to obtain an IPv6 address. When **Interface Type** is **WAN Interface**, the following modes are supported: static address, ND-RA, and DHCP. When **Interface Type** is **LAN Interface**, the following modes are supported: static address, ND-RA, DHCP, and prefix delegation.	● **Connection Type** can be set to **Prefix Delegation** for a LAN interface only when DHCPv6 prefix delegation is enabled on a WAN interface of the device (that is, the device can obtain an IPv6 address prefix pool from the DHCPv6 server). ● When **Connection Type** is set to **Prefix Delegation** for a LAN interface, RA is automatically enabled. In this case, the downstream terminals connected to the LAN interface can automatically obtain IPv6 addresses through SLAAC after being configured with this IPv6 address obtaining mode. [Example] Static Address
Prefix Pool ID	ID of the prefix pool bound to the interface in PD mode. The interface generates an IPv6 address based on the corresponding IPv6 address prefix pool.	● This parameter is available only when **Interface Type** is set to **LAN Interface** and **Connection Type** is set to **Prefix Delegation**. ● The prefix pool ID is manually specified when DHCPv6 prefix delegation is configured for the WAN interface. You can check the WAN interface configuration to obtain the prefix pool ID.
IP/Prefix Length	If the connection type of an interface is set to **Static Address**, this parameter needs to be set to specify the IPv6 address and prefix length of the interface. If the interface is a LAN interface and its connection type is **Prefix Delegation**, this parameter is used to configure the IPv6 address bound to DHCPv6 PD. The device generates the IPv6 address of the interface by combining the obtained prefix and the configured IPv6 address. If multiple interfaces are bound to the same prefix pool, their subnet IDs and interface IDs in the **IP/Prefix Length** value cannot be the same. Otherwise, different interfaces will generate the same IPv6 address, causing an address conflict. The prefix length must be 64 bits.	This parameter is available when **Connection Type** is set to **Static Address**. [Example] 2001::1/64

Item	Description	Remarks
Next-Hop Address	IP address of the next node for forwarding data.	This parameter is available when **Interface Type** is set to **WAN Interface** and **Connection Type** is set to **Static Address**. [Example] 2001::2
Default Route	Whether to enable the default route.	This parameter is available when **Interface Type** is set to **WAN Interface**. [Example] Enabled
Link-Local Address	Link-local address of the interface, which is automatically generated by the device.	-
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	Configure a static neighbor entry. When one node attempts to communicate with another, it must obtain the link-layer address of the other. You can manually configure a static ND entry to resolve the IPv6 address of a neighbor node to a link-layer address.	Each ND entry consists of the IPv6 address and MAC address of a neighbor. Enter one or more lines to specify one or more ND entries. The input format is as follows: *ipv6-address mac-address* [Example] 1234::100 00:11:22:33:44:55
Advanced Address Settings Click to expand **Advanced Address Settings**.		
Address Conflict Detection	Address conflict detection count. After address conflict detection is enabled, an interface sends NS packets to determine whether an IPv6 address is unique on the link, and performs address conflict detection again on the conflicting address based on the configured detection count and NS retransmission interval.	The value range is from 0 to 600. The value 0 indicates that conflict detection is disabled. [Example] 0

Item	Description	Remarks
NS Retransmission Interval	Interval for sending two NS messages. If a device does not receive any response within a specified interval after sending an NS message, the device sends an NS message again.	The value range is from 1000 to 4294967295, in milliseconds. [Example] 1000
RA Sending Interval	Interval between two periodically sent RA messages.	The value range is from 1 to 1800, in seconds. [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.	The value range is from 0 to 9000, in seconds. [Example] 1800
RA Reachable Time	Period in which the device regards a neighbor reachable after detecting the neighbor reachability event.	The value is an integer, in milliseconds. [Example] 30000
RA Prefix Info	Configure the address prefix to be advertised in an RA message: ● **Address**: Address prefix. ● **Effective Time**: Time considered valid by a host after receiving the prefix in an RA message, in seconds. ● **Preferred Time**: Lifetime considered valid by a host when the host receives the prefix in an RA message, in seconds. ● **Enable Router Address Flag**: If this field is enabled, the prefix address field contains the prefix and address of the router sending the RA message. ● **Enable Direct Route Flag**: If this field is enabled, the address prefix can be used as on-link determination. That is, if the prefix of the destination address in an IPv6 packet sent by a host matches the configured prefix, the destination address is directly reachable on the same link (on-link). If this field is disabled, the prefix is not used for on-link determination. ● **Enable Auto Config Flag**: If this field is enabled, the prefix is used for SLAAC. Otherwise, it is used for stateful address autoconfiguration.	Click **Create** to add an RA prefix.

Item	Description	Remarks
Line Bandwidth	Interface bandwidth thresholds, including uplink and downlink bandwidth thresholds.	Enter the bandwidth value and select a unit. This parameter is available when **Interface Type** is set to **WAN Interface**. [Example] 100 kbps
DHCP Service	Whether the DHCPv6 server function is enabled on the interface to assign IPv6 addresses to connected devices.	This parameter is available when the aggregate interface is a LAN interface, IPv6 is enabled for the aggregate interface, and **Connection Type** of the aggregate interface is set to **Static Address**. [Example] Enabled
Primary DNS Server	Primary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 2001::1
Secondary DNS Server	Secondary DNS server for the DHCP service.	Configure this parameter when the DHCP service is enabled. [Example] 2001::2
DHCPv6 Prefix Delegation Only WAN interfaces support this function.		
DHCPv6 Prefix Delegation	Configure the interface as a DHCPv6 client that applies for an IPv6 address prefix pool from the DHCPv6 server. The obtained IPv6 address prefix pool can be used to generate IPv6 addresses for LAN interfaces and intranet hosts.	[Example] Enabled
Prefix Pool ID	Specify a unique ID for an obtained IPv6 address prefix pool.	[Example] 1
Line Bandwidth		

Item	Description	Remarks
Uplink/Downlink	Bandwidth of the line.	Enter the bandwidth value and select a unit. This parameter is available when **Interface Type** is set to **WAN Interface**. [Example] 100 kbps
Access Management		
Access Management	Whether the interface supports HTTPS, ping, and SSH. When **IP Type** is set to **IPv6**, only the ping function can be enabled.	The configuration takes effect when local defense is enabled on the device.
Advanced Settings		
Aggregation Mode	Aggregation mode of the interface: ● **Static Aggregation**: Multiple physical interfaces are manually bound together to form a logical aggregate interface. The member interfaces of a static aggregate interface are always in aggregation state regardless of the status of the peer device. ● **Dynamic Aggregation**: The local interface and the connected device perform dynamic negotiation based on the Link Aggregation Control Protocol (LACP). This mode allows devices to automatically negotiate and adjust the state of the aggregate interface by exchanging protocol packets. For example, when the peer interface is disconnected, the aggregate interface is unbound; when a service link fails, traffic is automatically switched to other member links for forwarding. This mode implements flexible link management.	[Example] Static Aggregation
System Priority	System priority of the local interface. A smaller value indicates a higher priority. During LACP negotiation, the end with a higher system priority becomes the active end. It first sets an aggregate interface and sends the updated LACP packet to the peer end. After receiving the packet, the peer end sets the corresponding interface to the aggregation state to ensure that the active states of interfaces at both ends are consistent.	This parameter is valid in dynamic aggregation mode. [Example] 65535

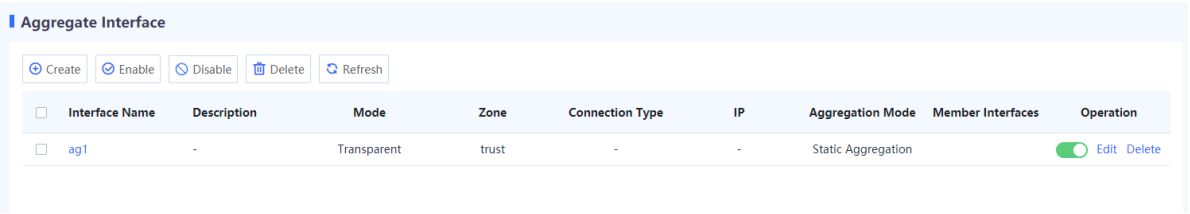
Item	Description	Remarks
Timeout Mode	Timeout mode of the interface in dynamic aggregation mode. After member interfaces are bound to a dynamic aggregate interface, the interface periodically exchanges LACP packets with the peer end. If the local interface does not receive LACP packets from the peer end within a period of time, it regards that the peer end is unreachable and removes the aggregation binding of local member interfaces. ● **Long Timeout**: The local interface sends an LACP packet every 30 seconds. If it does not receive a packet from the peer interface within 90 seconds, it considers the peer interface unreachable. ● **Short Timeout**: The local interface sends an LACP packet every 1 second. If it does not receive a packet from the peer interface within 3 seconds, it considers the peer interface unreachable.	This parameter is valid in dynamic aggregation mode. [Example] Long Timeout
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 parameter is available only when **Interface Type** is set to **WAN Interface** and **IP Type** is set to **IPv4**. [Example] China Telecom
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.	[Example] 1500
MAC	MAC address of the interface. If it is not specified, the MAC address of a member interface is used automatically.	[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.	This parameter is available only when **Interface Type** is set to **WAN Interface** and **IP Type** is set to **IPv4**. For details about link detection, see 6.14.1 Link Quality Detection.

Item	Description	Remarks
Reverse Path Limited	This function ensures that reverse traffic is sent back on the same path through the same interface and is enabled by default. After this function is enabled, it only takes effect on new traffic and does not take effect on local traffic.	[Example] Enable

(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**.



6.1.6 Configuring a Tunnel Interface

1. Configuring a VTI Interface

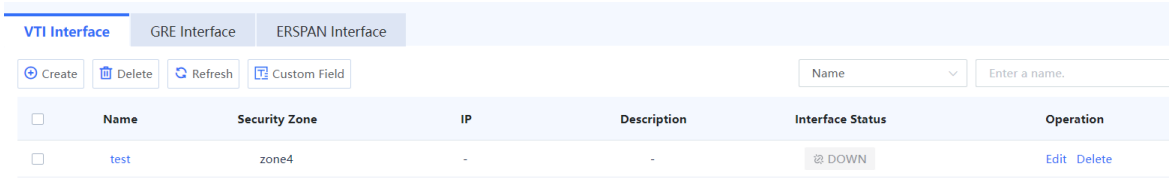
Application Scenario

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 virtual tunnel interface (VTI) 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.

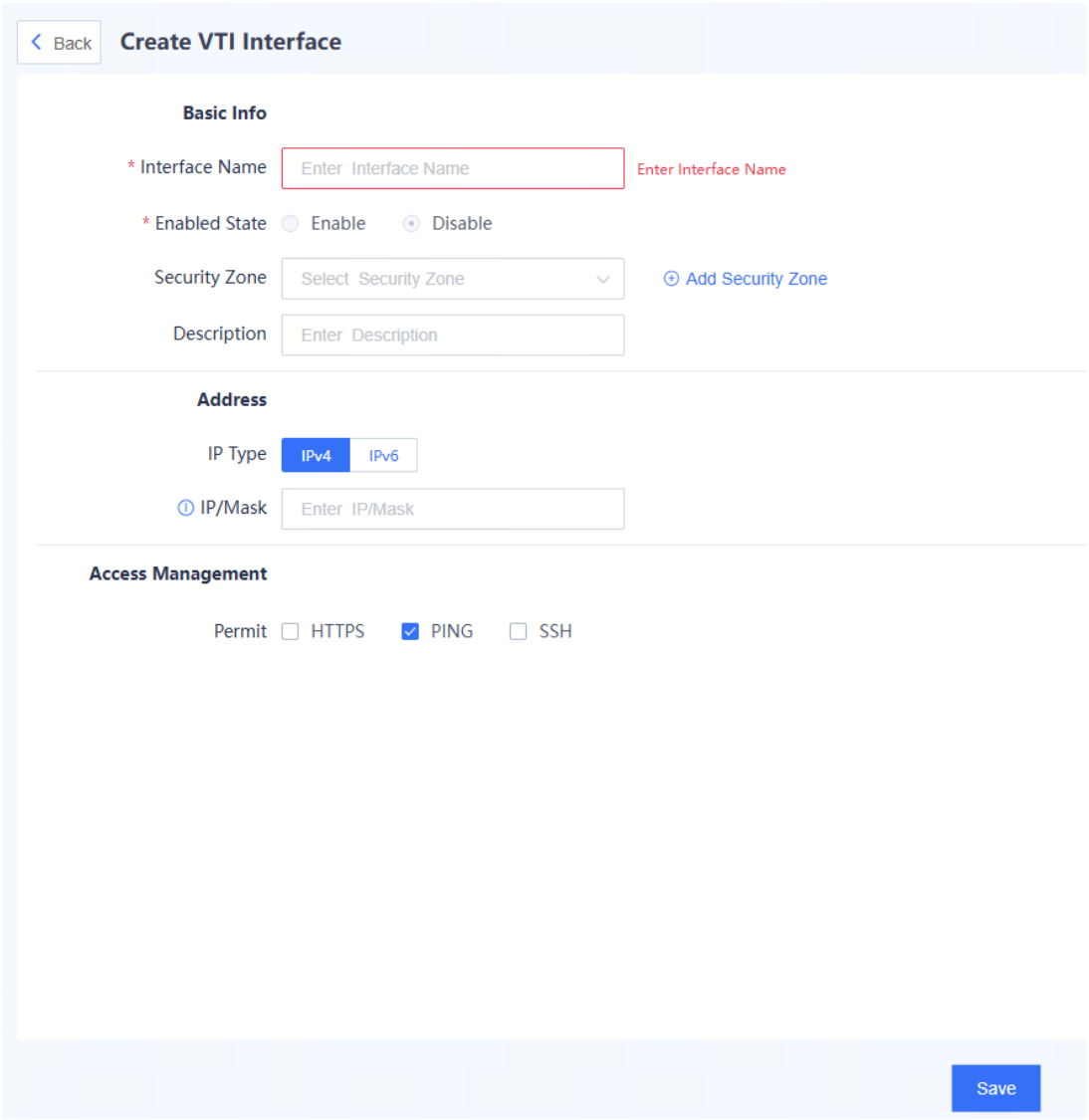
Procedure

(1) Choose **Network** > **Interface** > **Tunnel Interface** and click the **VTI interface** tab.



(2) Click **Create**.

The **Create VTI Interface** page is displayed.



(3) Set parameters for the tunnel interface.

Item	Description	Remarks
Interface Name	Name of the VTI interface.	The interface name must consist of uppercase and lowercase letters and digits and contain at least one letter. [Example] vti1

Item	Description	Remarks
Enabled State	Whether the VTI interface is enabled. Note that the actual status (Up/Down) of a VTI interface is irrelevant to its enabled status, but depends on whether an IPsec tunnel is successfully established.	● You can manually enable a VTI interface only when the VTI interface is referenced by an IPsec tunnel. ● The enabled status of the VTI interface is synchronized with the IPsec tunnel status, and no manual configuration is needed. When the IPsec tunnel is enabled, the VTI interface referenced by the IPsec tunnel is also automatically enabled. [Example] Disable
Security Zone	Security zone to which the interface belongs.	[Example] trust
Description	Interface description, showing the purpose of the interface.	[Example] IPsec tunnel
IP Type	IP address type of the interface. Valid values: **IPv4** and **IPv6**.	-
IP/Mask	IPv4 address and mask of a VTI interface.	[Example] 10.1.1.1/24
IP/Prefix Length	IPv6 address and prefix length of a VTI interface.	[Example] 2:14:58:a1:23:34:43:9/64
Access Management	Access management modes permitted by the interface: ● **HTTPS**: Permit access to the interface through HTTPS. ● **PING**: Permit access to the interface through ping. This option is selected by default. ● **SSH**: Permit access to the interface through SSH. When **IP Type** is set to **IPv6**, you can enable the ping mode only.	This configuration is valid when local defense is enabled on the device. [Example] Select **HTTPS**.

(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**.



2. Configuring an ERSPAN Interface

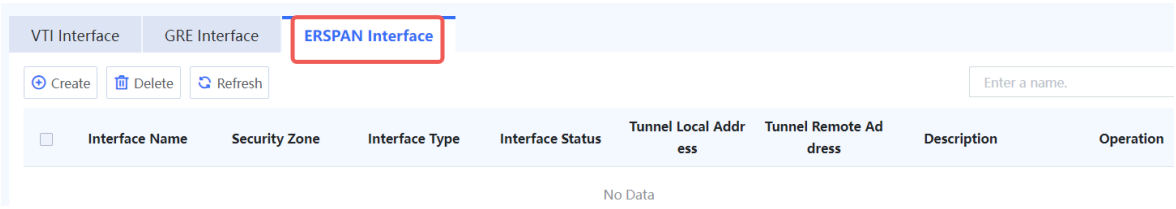
Application Scenario

Encapsulated Remote Switch Port Analyzer (ERSPAN) is a Layer 3 remote mirroring technology. It copies packets from a specified interface, VLAN, or CPU, encapsulates the packets into IP packets (that is, mirrored packets) using the Generic Routing Encapsulation (GRE) protocol, and then forwards the packets to the destination interface on a remote device. In this way, remote users can use data monitoring devices to analyze the packets. The firewall can be configured with an ERSPAN destination interface to receive mirrored packets from the peer device for risk analysis and identification.

ERSPAN is mainly used in network monitoring and troubleshooting scenarios to monitor network security and perform data security scan without affecting data forwarding of monitored devices.

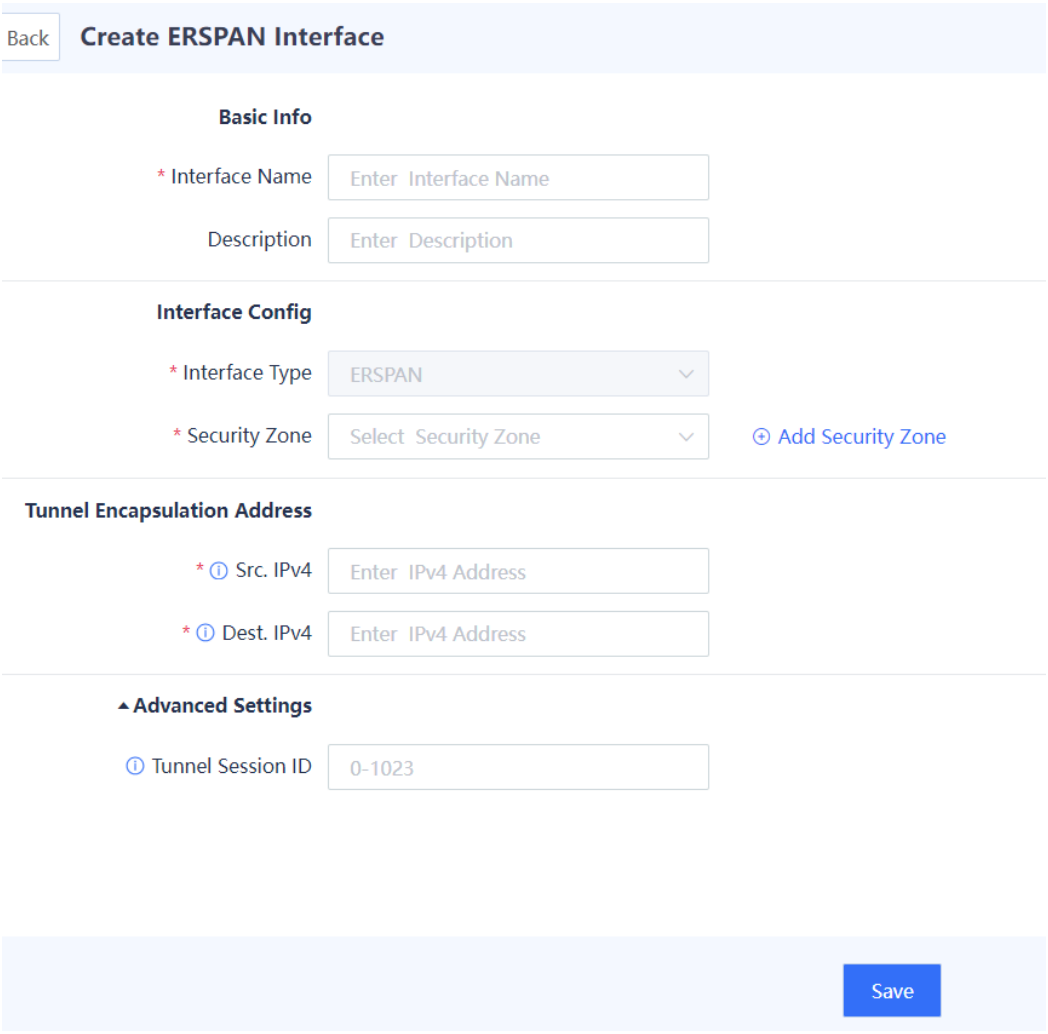
Procedure

(1) Choose **Network** > **Interface** > **Tunnel Interface** and click the ERSPAN Interface tab.



(2) Click **Create**.

The **Create ERSPAN Interface** page is displayed.



(3) Configure an ERSPAN interface.

Item	Description	Remarks
Basic Info		
Interface Name	Name of the ERSPAN interface. A maximum of 64 ERSPAN interfaces can be created.	The interface name must consist of uppercase and lowercase letters and digits and contain at least one letter. The length of the interface name cannot exceed 15 characters. [Example] ERSPAN1
Description	Interface description, showing the purpose of the interface.	[Example] Tunnel test
Interface Config		
Interface Type	The interface type is fixed to ERSPAN.	N/A

Item	Description	Remarks
Security Zone	Security zone to which the interface belongs.	[Example] trust
Tunnel Encapsulation Address		
Src. IPv4	Source address of a tunnel, that is, the local IPv4 address of a tunnel packet after being encapsulated using GRE. The source and destination IPv4 addresses do not need to be on the same network segment.	[Example] 10.1.1.10
Dest. IPv4	Destination address of a tunnel, that is, the remote IPv4 address of a tunnel packet after being encapsulated using GRE.	[Example] 10.1.2.20
Advanced Settings		
Tunnel Session ID	Unique identifier of a GRE tunnel. The keys at both ends of the tunnel must be set to the same value so that the receiving end can verify received packets. Multiple tunnels can be configured with the same source/destination IP address, but must be configured with different keys.	[Example] 2

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

Follow-up Procedure

- You can search for ERSPAN interfaces by name in the search box in the upper right corner.
- In the ERSPAN interface list, click **Edit** to modify the ERSPAN interface configuration or click **Delete** to delete an ERSPAN interface.
- Click **Refresh** to obtain the latest ERSPAN interface configuration.
- You can select multiple ERSPAN interfaces and click **Delete** to delete them in a batch.

6.1.7 Configuring a GRE Interface

1. Overview

The Generic Routing Encapsulation (GRE) protocol is used to encapsulate data packets of other protocols so that these packets can be transmitted on networks using a different protocol. The network-layer protocols of packets before and after encapsulation can be the same or different. The path through which encapsulated data packets are transmitted on the network is a GRE tunnel.

If IP networks at both ends of an IPsec tunnel need to communicate with each other, both ends must obtain the private network addresses of the peer networks. If dynamic routing protocols are deployed at both ends,

multicast packets of the routing protocols need to be transmitted through the IPsec tunnel. However, IPsec does not support the encapsulation of multicast packets. GRE can be used to encapsulate multicast packets into unicast packets and send the unicast packets to the peer network through the IPsec tunnel. In this case, the tunnel established between the two IP networks is a GRE over IPsec tunnel.

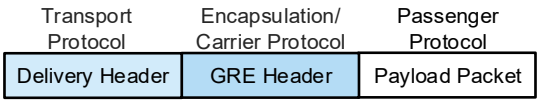
GRE tunnels transmit data in plaintext. If the data transmitted between the two ends of a tunnel needs to be encrypted, GRE over IPsec can be used.

2. Working Principle

The tunneling function includes the following three components:

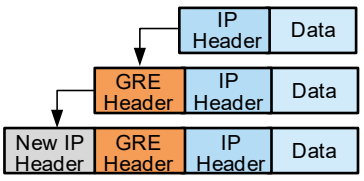
- Load protocol: Packet protocol before encapsulation, that is, the innermost tunnel protocol. IPv4 and IPv6 protocols are generally used as load protocols. For a GRE tunnel, the load protocol can be IPv4, IPv6, or MPLS.
- Carrier protocol: Encapsulation protocol, which is used for secondary encapsulation and identifying a load protocol. A GRE tunnel uses the GRE protocol as the carrier protocol.
- Transport protocol: Protocol for forwarding encapsulated packets, that is, the outermost tunnel protocol. IPv4 and IPv6, the most widely used protocols, are typically used as transport protocols.

Figure 6-1 GRE Packet Format



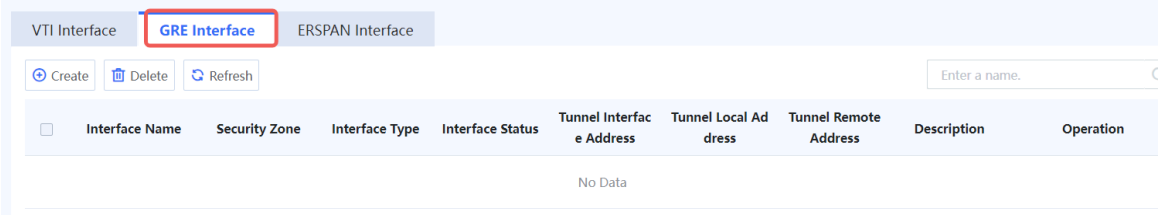
GRE encapsulates packets layer by layer based on the protocol stack. As shown in Figure 6-2, the encapsulation process consists of two steps: Add a GRE header to the original packet, and add a new IP header before the GRE header. Then the packet can be transmitted on a network using a different protocol. GRE uses a tunnel interface to perform encapsulation. During the encapsulation, the encapsulation protocol of the tunnel interface is GRE.

Figure 6-2 GRE Packet Encapsulation



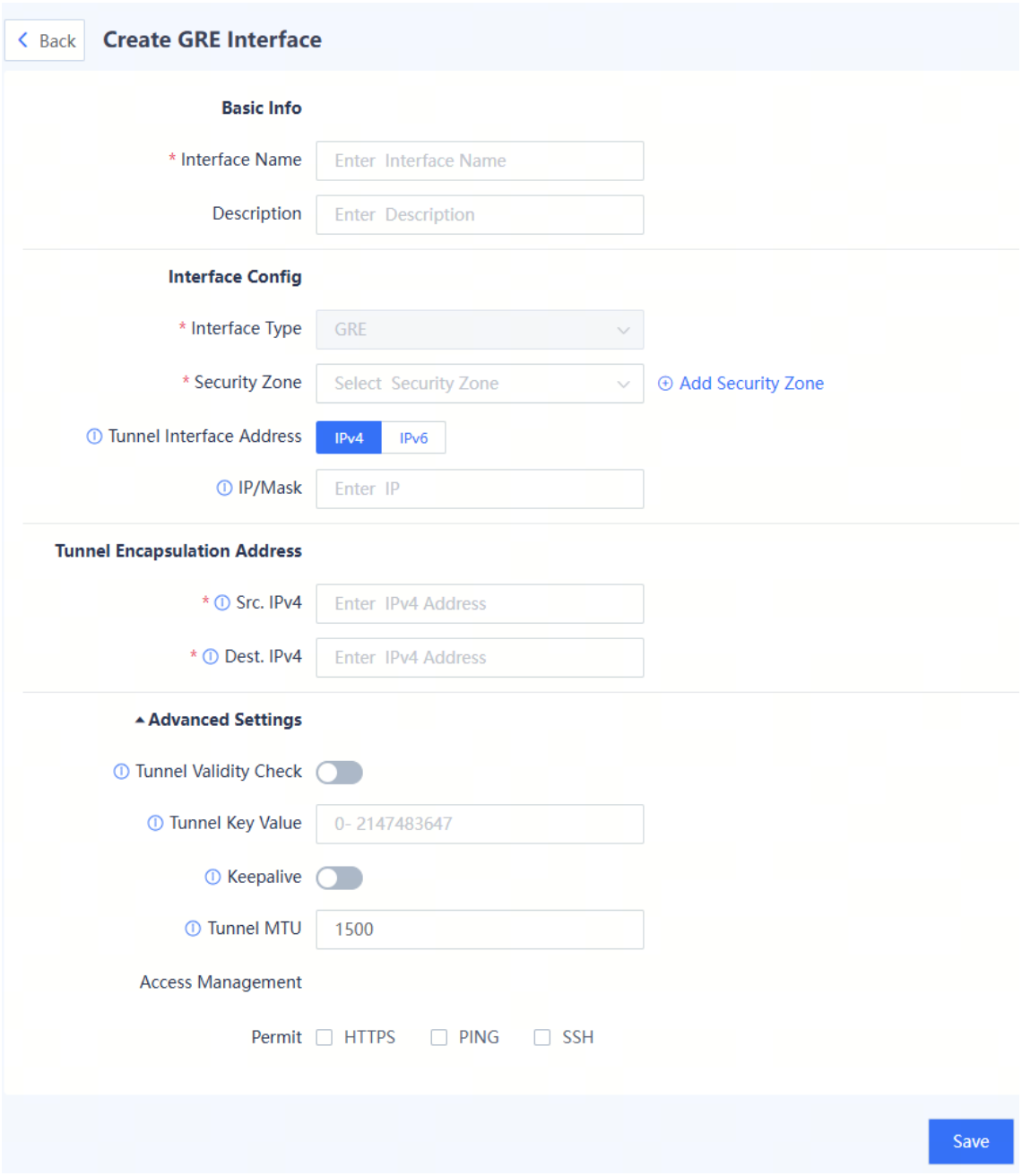
3. Procedure

(1) Choose **Network** > **Interface** > **Tunnel Interface** and click the **GRE Interface** tab.



(2) Click **Create**.

The **Create GRE Interface** page is displayed.



(3) Configure a GRE interface.

Item	Description	Remarks
Basic Info		

Item	Description	Remarks
Interface Name	Name of the GRE interface.	The interface name must consist of uppercase and lowercase letters and digits and contain at least one letter. [Example] gre1
Description	Description of the GRE interface, showing the purpose of the interface.	[Example] Tunnel test
Interface Config		
Interface Type	The interface type is fixed to GRE.	N/A
Security Zone	Security zone to which the interface belongs.	[Example] trust
Tunnel Interface Address	Address of the GRE interface. An IPv4 or IPv6 address can be set. If a GRE tunnel is used to implement IPv4 communication, set an IPv4 address. If a GRE tunnel is used to implement IPv6 communication, set an IPv6 address. Note: When configuring a static route for the tunnel, ensure that the destination IP address is not on the same network segment as the current IP address.	[Example] IPv4
IPv6 Protocol	To use IPv6, verify that the IPv6 function is enabled.	[Example] Enable
IP/Mask	IP address and mask of the GRE interface.	[Example] 10.1.1.1/24 or 2:14:58:a1:23:34:43:9/64
Tunnel Encapsulation Address		
Src. IPv4	Source address of a tunnel, that is, the local IPv4 address of a tunnel packet after being encapsulated using GRE.	[Example] 10.1.1.10
Dest. IPv4	Destination address of a tunnel, that is, the remote IPv4 address of a tunnel packet after being encapsulated using GRE.	[Example] 10.1.1.20
Advanced Settings		

Item	Description	Remarks
Tunnel Validity Check	If this function is enabled, the packet header and information are checked. If the check fails, the packet is discarded.	[Example] Enable
Tunnel Key Value	Unique identifier of a GRE tunnel. The keys at both ends of the tunnel must be set to the same value so that the receiving end can verify received packets. Multiple tunnels can be configured with the same source/destination IP address, but must be configured with different keys.	[Example] 2
Keepalive	If this function is enabled, tunnel availability is periodically checked based on the round-trip of keepalive messages on the tunnel link.	[Example] Enable
Keepalive Interval	Interval for retransmitting keepalive messages, in seconds. The default value is 10.	[Example] 10
Retransmission Times	Number of times that keepalive messages are retransmitted. If no response packet is received after the retransmission times, the local interface is shut down, and goes up again only after receiving a response packet from the peer end. The default number of retransmission times is 3.	[Example] 10
Tunnel MTU	Maximum Transmission Unit (MTU) of a tunnel, in bytes. The default value is 1500.	In GRE over IPsec scenarios, the MTU of the GRE tunnel must be the same as that of the IPsec VPN tunnel. [Example] 1500
Access Management	When local defense is disabled, access management cannot be configured, and existing configurations become invalid.	N/A

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

Follow-up Procedure

- You can search for a GRE interface by name in the search box in the upper right corner.
- In the GRE interface list, click **Edit** to modify the GRE interface configuration or click **Delete** to delete a GRE interface.

- Click **Refresh** to obtain the latest GRE interface configuration.
- You can select multiple GRE interfaces and click **Delete** to delete them in a batch.

6.1.8 Multi-PPPoE

Application Scenario

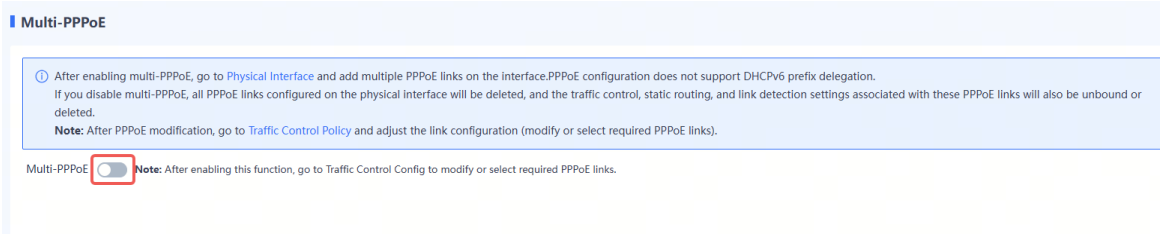
After the multi-PPPoE function of is enabled, multiple PPPoE links can be added to a single physical interface (that is, multiple PPPoE accounts can be used) to aggregate line bandwidths and improve the network transmission rate. With this function, the device can combine the bandwidths of multiple PPPoE connections based on multiple PPPoE sessions without the need for additional physical lines, meeting the demand for higher-speed Internet access.

Prerequisites

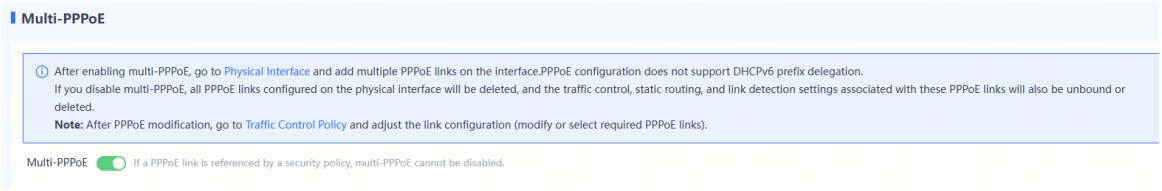
Before configuring multi-PPPoE, check whether the ISP permits the use of multiple PPPoE accounts for multi-PPPoE.

Procedure

(1) Choose **Network** > **Interface** > **Multi-PPPoE**.

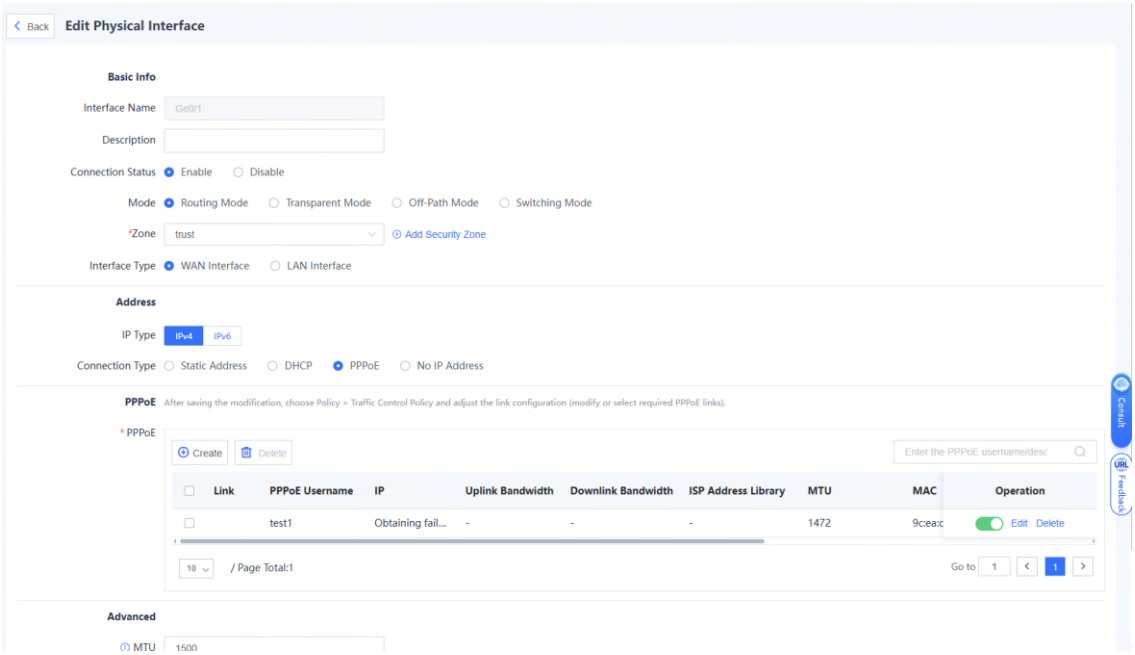


(2) Toggle on **Multi-PPPoE** to enable this function.

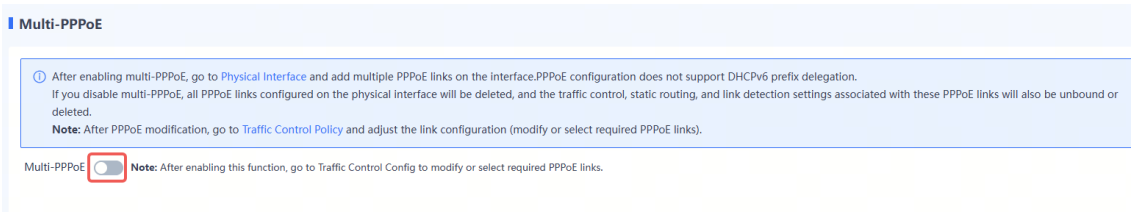


Follow-up Procedure

- After you enable multi-PPPoE, choose **Network** > **Interface** > **Physical Interface**, find the physical interface to be configured, set its **Connection Type** to **PPPoE**, click **Create** in the PPPoE list, and add multiple PPPoE links on the Interface. The following figure shows a configuration example.



- Toggle off **Multi-PPPoE** to disable this function.



Caution

- After you disable multi-PPPoE, all PPPoE links configured for physical interfaces will be deleted, and the traffic control, static routing, and link detection configurations associated with the PPPoE links will be automatically removed or deleted.
- If any PPPoE link is referenced by a security policy or NAT, multi-PPPoE cannot be disabled.

- If the PPPoE link configuration changes after you enable or disable multi-PPPoE, choose **Policy** > **Traffic Control Policy** to adjust the traffic control configuration of the corresponding links, or modify or reselect the PPPoE links that require traffic control.

6.1.9 Configuring a Cellular Interface

1. Overview

A cellular interface is provided by the device for connection to a cellular mobile communication network such as the 3G or 4G network. After you insert a carrier SIM card into the device and configure a cellular interface, the device can access the carrier network in wireless mode, without being restricted by geographical location or physical media. This flexibly implements wireless broadband access and interconnection for enterprise branches or small- and medium-sized enterprises.

Typical usage scenarios of cellular networks include, but are not limited to:

- Wired WAN link backup: A wireless WAN link can serve as the backup for the wired WAN link. When the primary link fails, the secondary link ensures normal service operation.
- Flexible and efficient network deployment: In scenarios such as remote areas or mobile office environments, wired links suffer from limited coverage, high deployment costs, and poor mobility. Wireless WAN access is recommended for rapid network deployment, providing network services required by services and ensuring service coverage.
- Secure VPN access: Enterprise branches can establish VPN tunnels with the enterprise headquarters through wireless links, enabling branch users to access the headquarters quickly, securely, and efficiently.

2. Configuring a Cellular Interface

Prerequisites

- Product models supporting a cellular interface:
  - RG-CF10S-LTE supports a cellular interface by default.
  - RG-CF30XS do not support a cellular interface, but can have a 4G module installed to support a cellular interface as the extended interface.

> **Note**
>
> The device of the standard configuration does not contain a 4G module. You can purchase a 4G module by yourself based on actual needs.

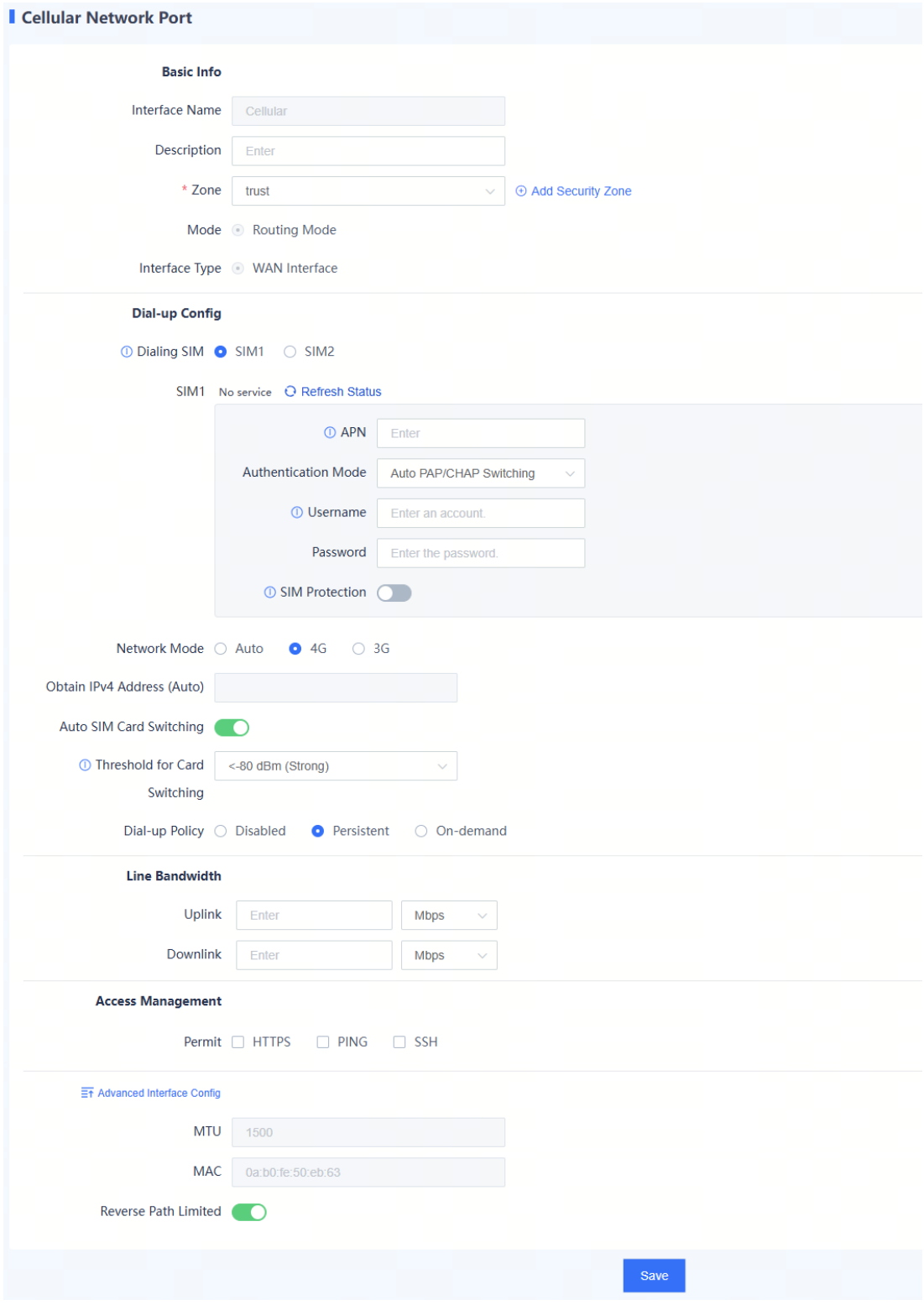
- Before configuring a cellular interface, complete the following tasks:
  - Ensure that the 3G or 4G network is available in the zone where the device is deployed.
  - Purchase the network service from the carrier and obtain a SIM card and network connection parameters.
  - Insert the SIM card into the device and ensure that the SIM card is in place. If the device supports a cellular interface through 4G module extension, install the 4G module and then insert the SIM card into the 4G module.

> **Caution**
>
> - The 4G module does not support hot swapping. You need to install or uninstall the 4G module when the device is powered off.
> - The SIM card does not support hot swapping. In scenarios with dual SIM cards, hot swapping of the SIM cards will lead to an exception of the auto SIM card switching function. You need to reconfigure working parameters for the two SIM cards on the **Cellular Network Port** page.

Procedure

(1) Choose **Network** > **Interface** > **Cellular Network Port**.

(2) Configure connection parameters for the cellular interface.



Item	Description	Remarks
Basic Info		

Item	Description	Remarks
Interface Name	Name of the cellular interface. The default value is **Cellular**.	The value is automatically generated by the system and cannot be modified.
Description	Description of the cellular interface, which is used to mark the interface.	[Example] SIM card 4G dial-up
Zone	Zone to which the interface belongs.	[Example] WAN
Mode	Working mode of the interface. The default value is **Routing Mode**, which cannot be modified.	-
Interface Type	Logical attribute of the interface. The default value is **WAN Interface**, which cannot be modified.	-
Dial-up Config		
Dialing SIM	SIM card selected for dial-up. Caution: ● Currently, the device supports dual SIM single standby. When one SIM card is in the dial-up state, switching dial-up to the other SIM card will lead to dial-up interruption. ● If no SIM card is inserted or the SIM card is abnormal, you cannot configure dial-up parameters for the SIM card.	[Example] SIM1
APN	Access Point Name (APN) used by the device to establish a connection to the carrier network. You need to obtain the APN from the carrier. If you replace the SIM card or carrier in the later stage, you need to reconfigure the APN information.	Set this parameter based on information provided by the carrier. [Example] cmnet
Authentication Mode	Authentication mode for access to the carrier network. The device supports **PAP Authentication**, **CHAP Authentication**, **Auto PAP/CHAP Switching**.	The authentication mode, username, and password are provided by the carrier. [Example] PAP Authentication
Username	Username used to access the carrier network.	The authentication mode, username, and password are provided by the carrier.
Password	Password used to access the carrier network.	The authentication mode, username, and password are provided by the carrier.

Item	Description	Remarks
SIM Protection	The SIM protection function is used to protect SIM card security and prevent unauthorized use of the SIM card. After this function is enabled, the SIM card is bound with the local device. If the SIM card is moved to a new device, you need to enter the correct PIN code for identity authentication. If the number of consecutive PIN code errors reaches the upper limit, the SIM card will be locked. You need to contact the carrier to obtain a Personal Unblocking Key (PUK) code to unlock the SIM card.	● You need to enter the PIN code for authentication, regardless of whether the SIM protection function is enabled. ● If the SIM card is replaced or the PIN code is changed for the SIM card on another device, you need to enter the PIN code for authentication and binding after inserting the SIM card. ● Contact the carrier to obtain the initial PIN code of the SIM card. The initial PIN code has low security. It is recommended to change the PIN code in time after enabling the SIM protection function. [Example] Enable
PIN	Change the PIN code of the SIM card, which must be a string of 4 to 8 digits. Contact the carrier to obtain the initial PIN code.	After enabling the SIM protection function, click **Edit** to change the PIN code of the SIM card.
Advanced Dial-up Config		
Network Mode	Network connection mode of the interface. The options are as follows: ● **Auto**: The device automatically determines to connect to the 4G or 3G network. If the 4G network is available, the device connects to the 4G network preferentially. ● **4G**: The device connects to the 4G network only. ● **3G**: The device connects to the 3G network only.	[Example] Auto
Obtain IPv4 Address (Auto)	The interface automatically obtains an IPv4 address through dial-up.	The value is automatically displayed in the system and cannot be modified.
Auto SIM Card Switching	After this function is enabled, the device automatically switches between SIM cards based on the RSSI when multiple SIM cards are available.	[Example] Enable
Signal Threshold for Card Switching	If the RSSI of the current SIM card is lower than the specified signal threshold for card switching, the device automatically switches to another enabled SIM card for dial-up. If no other SIM card is available or the RSSI of other SIM cards is also lower than the specified signal threshold for card switching, switching is not performed.	This parameter is available only when the auto SIM card switching function is enabled. [Example] < -100 dBm (Weak)
Dial-up Policy		

Item	Description	Remarks
Dial-up Policy	Dial-up policy. ● **Disabled**: The device does not dial up. ● **Persistent**: After the device is started, the cellular interface automatically initiates dial-up to establish a connection to the carrier network and retains the online state after successful dial-up. If dial-up fails, the cellular interface tries dial-up again at the specified interval. ● **On-demand**: The cellular interface is automatically triggered to dial up in a specific scenario. If you select this option, dial-up is automatically triggered when the wired WAN interface is abnormal or detection of the specified link fails.	[Example] Persistent
Dial-up on WAN Failure	The device monitors the status of the specified wired WAN interface. If a fault is detected, the cellular interface is automatically triggered to dial up. After the monitored interface restores normal, the cellular interface stops dial-up.	● You can configure this parameter only when **On-demand** is selected for **Dial-up Policy**. ● After you enable this function, you must specify at least one monitored interface. If multiple monitored interfaces are specified, the cellular interface is triggered to dial up only when all the monitored interfaces are faulty. [Example] Enable
Dial-up on Link Detection Failure	The device monitors the link status through associated link detection objects. If the link detection result is abnormal, the cellular interface is automatically triggered to dial up. After the link detection result restores normal, the cellular interface stops dial-up.	● You can configure this parameter only when **On-demand** is selected for **Dial-up Policy**. ● After you enable this function, you must specify a link detection object. Click **Add Link Detection** to create a link detection object. [Example] Enable
Line Bandwidth	Bandwidth provided by the carrier for lines, including the uplink bandwidth and downlink bandwidth.	Enter a bandwidth value and select a unit. [Example] 100 Mbps

Item	Description	Remarks
Access Management	Access management mode of the cellular interface. The options are as follows: ● **HTTPS**: Permits interface access through HTTPS. (Select this option if you want to log in to the web UI of the device through the cellular interface address.) ● **PING**: Permits interface access through Ping. ● **SSH**: Permits interface access through SSH.	The configuration takes effect when local protection is enabled on the device. [Example] Select **HTTPS**.
Advanced Interface Config		
MTU	Maximum number of data bytes in a packet sent by the cellular interface.	[Example] 1500
MAC	MAC address of the cellular interface.	[Example] 00:0d:9e:41:d9:0b
Reverse Path Limited	Ensures that reverse response packets are sent to the interface that sends the original request packets. In the multi-egress scenario, this function prevents response packets from being transmitted over ISP2 when the corresponding request packets are sent over ISP1. This function prevents slow service access and even service interruption. This function applies to new traffic only but not the local traffic.	[Example] Enable

(3) Click **Save**.

6.2 Security Zone

6.2.1 Overview

Security zone is a security concept introduced for devices. A security zone is a set of networks connected by interfaces.

Note that with the development of firewalls, security zones can also be considered as a set of interfaces, and the corresponding packet forwarding rules are as follows:

- In NGFW_NTOS1.0R12 and later versions, **any** indicates all interfaces. In versions earlier than NGFW_NTOS1.0R12, **any** indicates all security zones and the following restrictions exist:
  - Packets between interfaces that do not belong to any security zones are discarded.
  - Packets between an interface in a security zone and an interface not in any security zone are discarded.
- Packets between interfaces in the same security zone or between interfaces in different security zones are checked according to security policies and local defense policies.
- Packets with the local device address as the source address are not checked according to security policies

or local defense policies.

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.

6.2.2 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

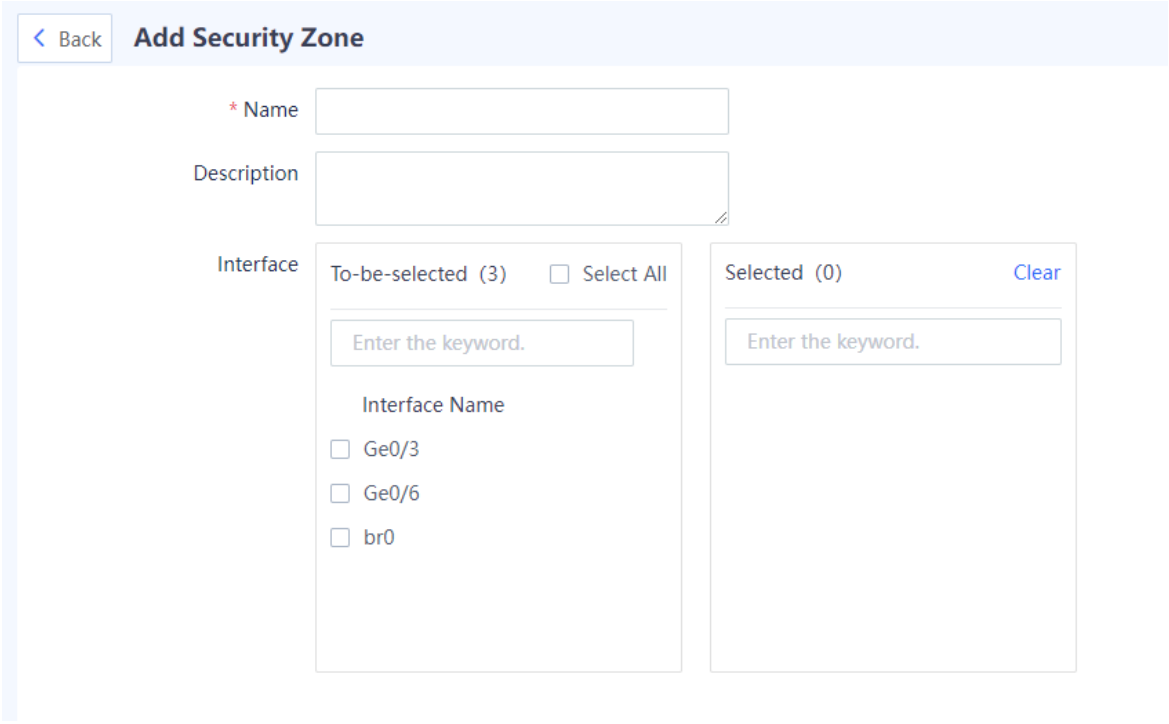
(1) Access the **Add Security Zone** page.

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.	[Example] Zone1
Description	Description of the security zone, which is used to distinguish different security zones.	[Example] New zone
Interface	Interfaces to be added to the security zone.	● 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**.

6.3 Route Management

6.3.1 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.

CF 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 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.
- OSPFv2: For details, see 6.4 OSPF.

In a scenario where multiple routing modes are available, the priorities in a descending order are as follows: intelligent routing, static routing, OSPFv2, 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.

6.3.2 Creating a Static Route

Application Scenario

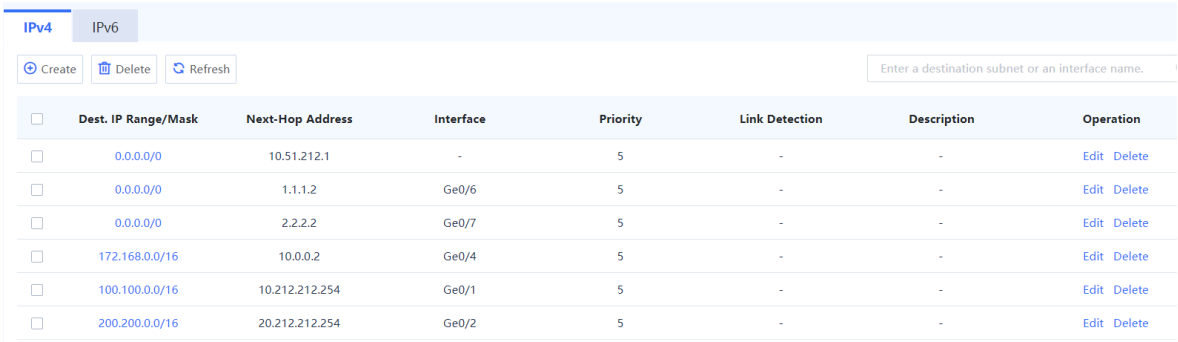
You can configure the IP address, next-hop address, and interface to create a static route for network interconnection and packet forwarding.

Procedure

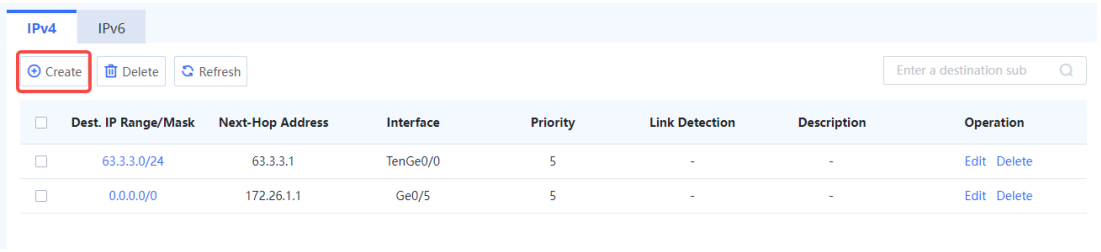
(1) Access the **Create Static Routing** page.

a Choose **Network** > **Routing/Load Balancing** > **Static Routing**.

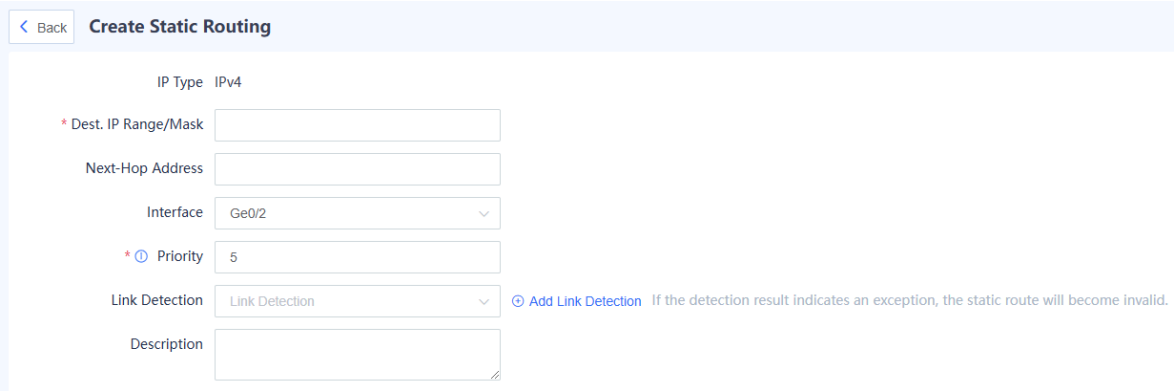
b Click the **IPv4** or **IPv6** tab to create an IPv4 or IPv6 static route as needed.



c Click **Create**.



(2) Set parameters of the static route.



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
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.	● The value ranges from 1 to 255. ● A smaller value indicates a higher priority. [Example] 15

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 static route becomes invalid.	This parameter can be configured only after a WAN interface is selected. For details about link detection, see 6.14.1 Link Quality Detection.
Description	Description of the static route.	-

(3) Click **Save**.

6.3.3 Creating an Intelligent Routing Policy

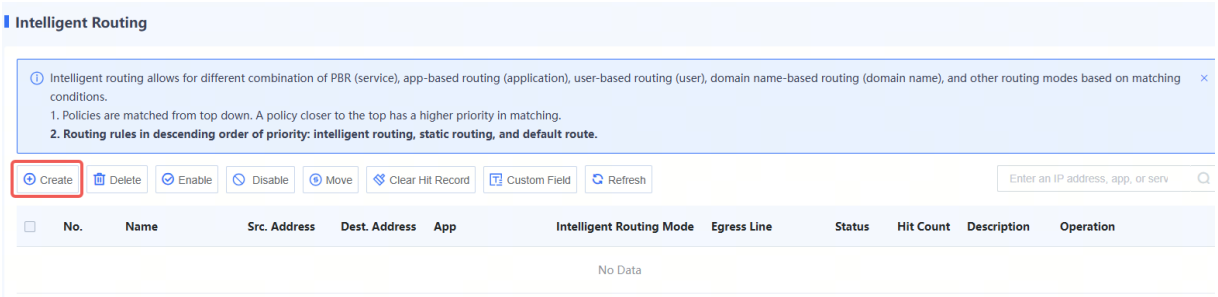
Application Scenario

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

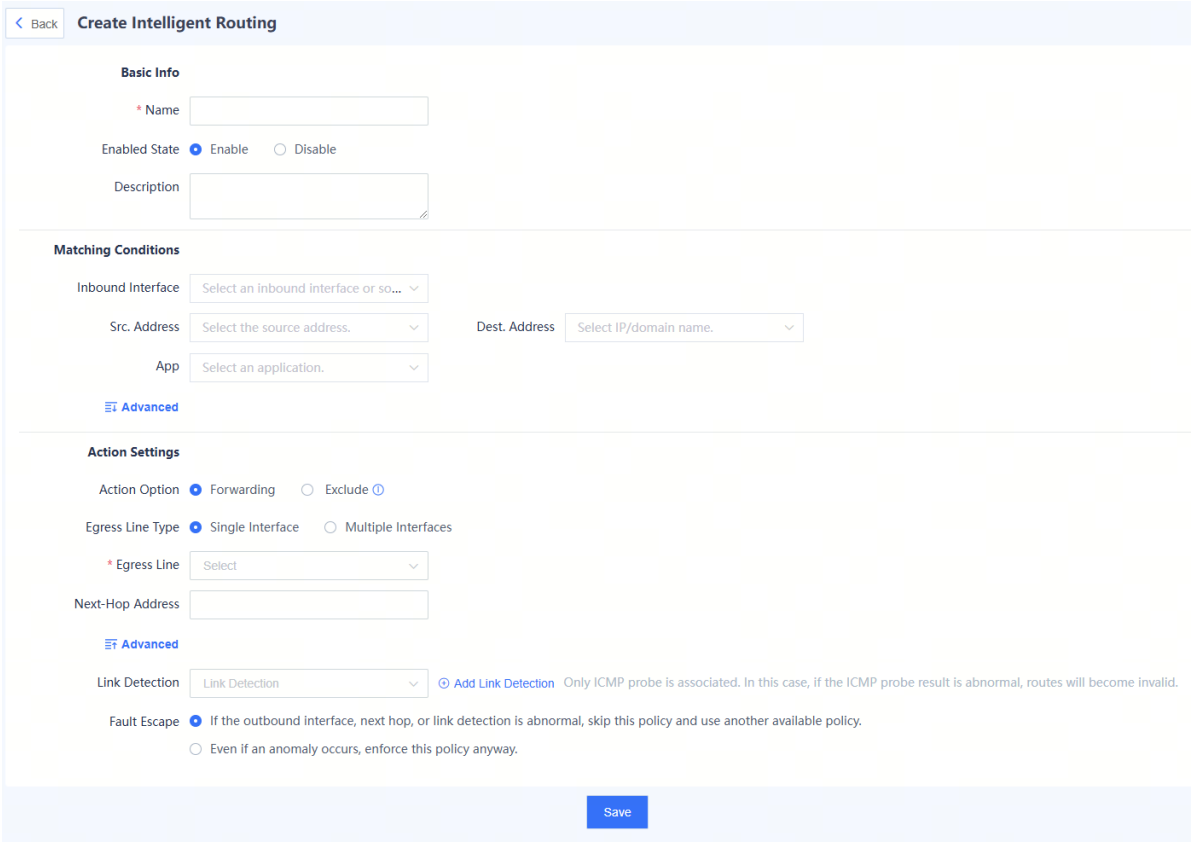
Procedure

(1) Choose **Network** > **Routing/Load Balancing** > **Intelligent Routing**. The Intelligent Routing page is displayed.

(2) Click **Create** to access the **Create Intelligent Routing** page.



(3) Set parameters for the intelligent routing policy.



Item	Description	Remarks
Basic Info		
Name	Name of the intelligent routing policy.	[Example] Policy_1
Enabled State	Whether to enable the intelligent routing policy.	[Example] Enable
Description	Route description.	-
Matching Conditions The relationship between matching conditions is AND. Packets must meet all matching conditions before they can be forwarded according to this routing rule. The relationship between the values configured in a single matching condition is OR. As long as a packet matches any value, the packet is considered to match the condition.		
Inbound Interface	Forwards the packets from this inbound interface based on the policy.	Click the drop-down list, and select an inbound interface in the **To-be-selected** area. The selected interface is automatically added to the **Selected** area. [Example] trust

Item	Description	Remarks
Src. Address	Forwards the packets from the source address based on the policy.	• Click the drop-down list, and select an address object in the **To-be-selected** area. The selected address object is automatically added to the **Selected** area. • Click **Add Address** to add an address object to set the source address range to be matched. • Click **Add Address Group** to add an address group to set the source address range to be matched. [Example] any
Dest. Address	Forwards the packets destined for the address (IP address or domain name) based on the policy.	• Click the drop-down list, and select an address object in the **To-be-selected** area. The selected address object is automatically added to the **Selected** area. • Click **Add Address** to add an IP address or domain name to set the destination address range to be matched. • Click **Add Address Group** to add an address group to set the destination address range to be matched. [Example] any
App	Forwards the packets of this application type based on the policy.	• Click the drop-down list, and select an application in the **To-be-selected** area. The selected application is automatically added to the **Selected** area. • Click **Add Custom App** to add a custom application. • Click **Add App Group** to add an application group for matching. [Example] any
Service	Forwards the packets of this service type based on the policy.	• Click the drop-down list, and select a service in the **To-be-selected** area. The selected service is automatically added to the **Selected** area. • Click **Add Service** to add a service. • Click **Add Service Group** to add a service group for matching. [Example] any

Item	Description	Remarks
User	Forwards the packets of this user or user group based on the policy.	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. ● Click **Add User** to add a user. ● Click **Create User Group** to add a user group for matching. [Example] any
Effective Time	Time range in which the intelligent routing policy is effective.	[Example] any
Action Settings		
Action Option	Processing action for packets that meet the conditions: ● **Forwarding**: Forwards packets based on intelligent routing. The egress route and next-hop address need to be configured. ● **Exclude**: Excludes some packets with an intelligent routing policy of a lower priority. Excluded packets are forwarded by other routes, for example, static route and default route.	[Example] Forwarding
Egress Line Type	● **Single Interface**: A single outbound interface needs to be configured for packets that meet the conditions. ● **Multiple Interfaces**: Multiple outbound interfaces need to be configured for packets that meet the conditions.	[Example] Single Interface
Intelligent Routing Mode	If the egress line type is **Multiple Interfaces**, you also need to set the intelligent routing mode to enable load balancing based on the link bandwidth, link weight, link priority, or other factors.	[Example] Based on Weight
Egress Line List If the egress line type is **Multiple Interfaces**, you also need to configure an egress line list. Line parameters vary depending on the intelligent routing mode.		
Line	Name of an outbound interface.	Click **Create** to add interfaces. Click **Confirm**. The interfaces are automatically added to the list.

Item	Description	Remarks
Next-Hop Address	IP address of the next node for forwarding data.	If a next-hop address has been configured for the selected interface, the next-hop address is automatically filled in after you click **Confirm**. You can also manually modify the address. If no next-hop address is configured for the selected interface, you need to manually configure the address after clicking **Confirm**. [Example] 192.168.1.1 or 1234::100
Weight	Link weight of the outbound interface. For example, set the weights of outbound interfaces 1 and 2 to 5 and 1, respectively. In this case, traffic is distributed to outbound interfaces 1 and 2 at a ratio of 5:1.	[Example] 1
Priority	Link priority of the outbound interface. A larger value indicates a higher priority. Traffic is preferentially distributed to the interface with a higher priority.	[Example] 1
Max. Session Number	Maximum number of sessions on the outbound interface. If the number of sessions established on the interface exceeds the maximum number, traffic is forwarded based on the routing priority in the routing table.	[Example] 2000
Operation	● Click **Copy** to copy the attributes (uplink/downlink bandwidth, uplink/downlink load threshold, priority, and weight) except for the interface name to other interfaces in the egress line list. ● Click **Delete** to delete an egress line.	-
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.	This parameter can be configured only after a WAN interface is selected. For details about link detection, see 6.14.1 Link Quality Detection.

Item	Description	Remarks
Fault Escape	The device automatically checks the interface status, next-hop status, and link detection result before executing an intelligent routing policy. If any of the items is abnormal, the device processes the issue based on the specified fault escape method: automatically skip this policy, use another available policy, or forcibly execute this policy.	[Example] If the outbound interface, next hop, or link detection is abnormal, skip this policy and use another available policy.

(4) Click **Save**.

6.3.4 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.

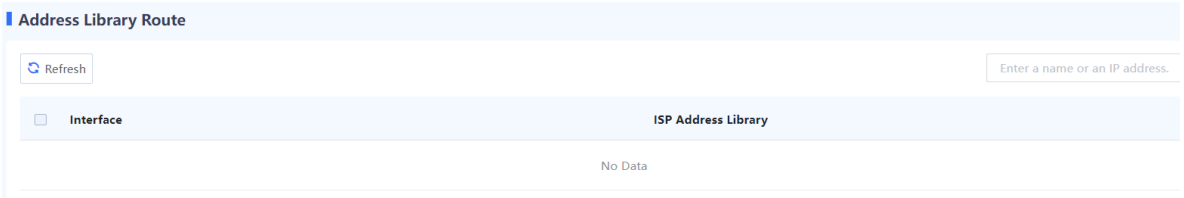
Prerequisites

- You have completed the configuration of the ISP address library. For details, see 5.7 ISP Address Library.
- You have configured an ISP address library to be associated with WAN interfaces. For details, see 6.1 Interface.

Procedure

(1) Choose **Network** > **Routing/Load Balancing** > **Address Library Route**.

(2) View the address library routing entries on the firewall.



6.3.5 Configuring a Routing Policy

Application Scenario

On a traditional network, routing devices search routing tables based on the destination addresses of packets and forward the packets based on the information in the routing tables. However, as network applications become increasingly complex, users require routing devices to provide more refined and diversified traffic control functions in addition to traditional routing.

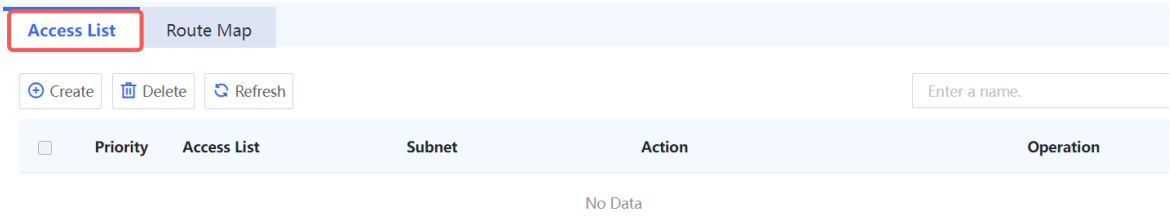
A routing policy set is used to change packet forwarding paths or routing information (including routing attributes, next hop, forwarding interface, and priority), which is implemented using an access list and route map. To implement route filtering, an access list must be used in a route map. Routing policies provide services for different routing protocols, and complete the policy-based control of routing information based on a specified policy set.

Procedure

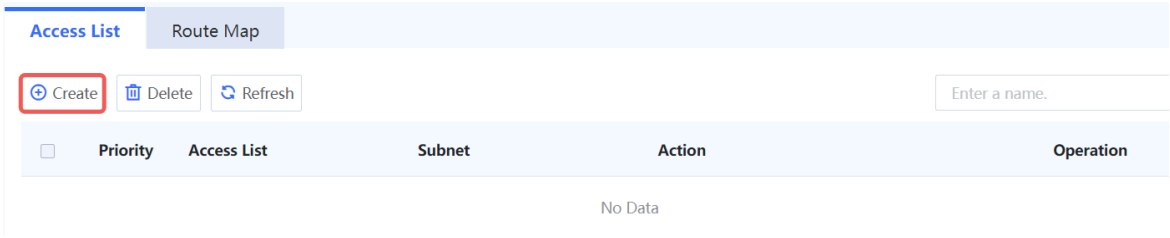
(1) Configure an access list.

a Choose **Network** > **Routing/Load Balancing** > **Routing Policy**.

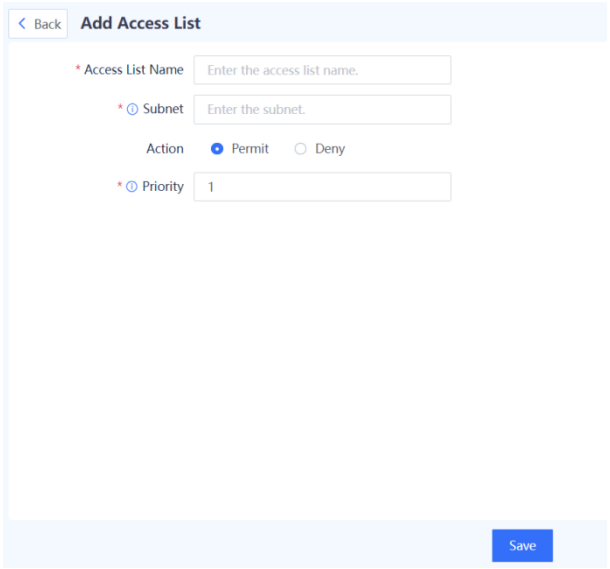
b Click the **Access List** tab.



c Click **Create**.



d Configure an access list.



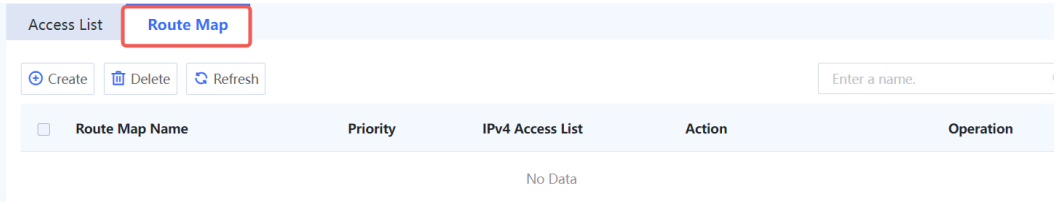
Item	Description	Remarks
Access List Name	Access list name. A maximum of 50 access lists with different names can be configured, and a maximum of 10 access lists with the same name can be configured. That is, a total of 500 access lists can be configured.	[Example] list_1
Subnet	IPv4 subnet and mask for matching.	Enter a valid IPv4 subnet and mask. [Example] 172.168.1.0/24
Action	Action to be taken: ● **Permit**: Packets on the specified subnet are matched. ● **Deny**: Packets on the specified subnet are not matched.	[Example] Permit
Priority	A lower value indicates a higher priority. Access lists with the same name cannot have the same priority.	[Example] 1

e Click **Save**.

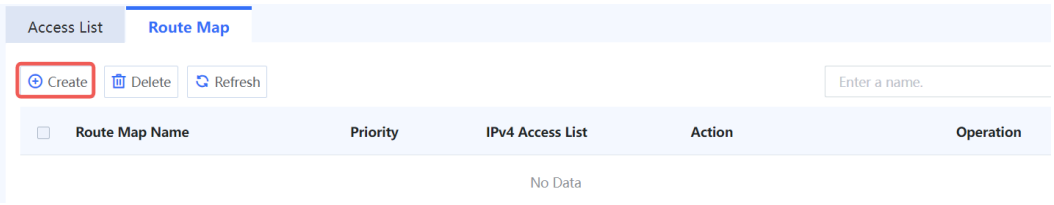
(2) Configure a route map.

a Choose **Network** > **Routing/Load Balancing** > **Routing Policy**.

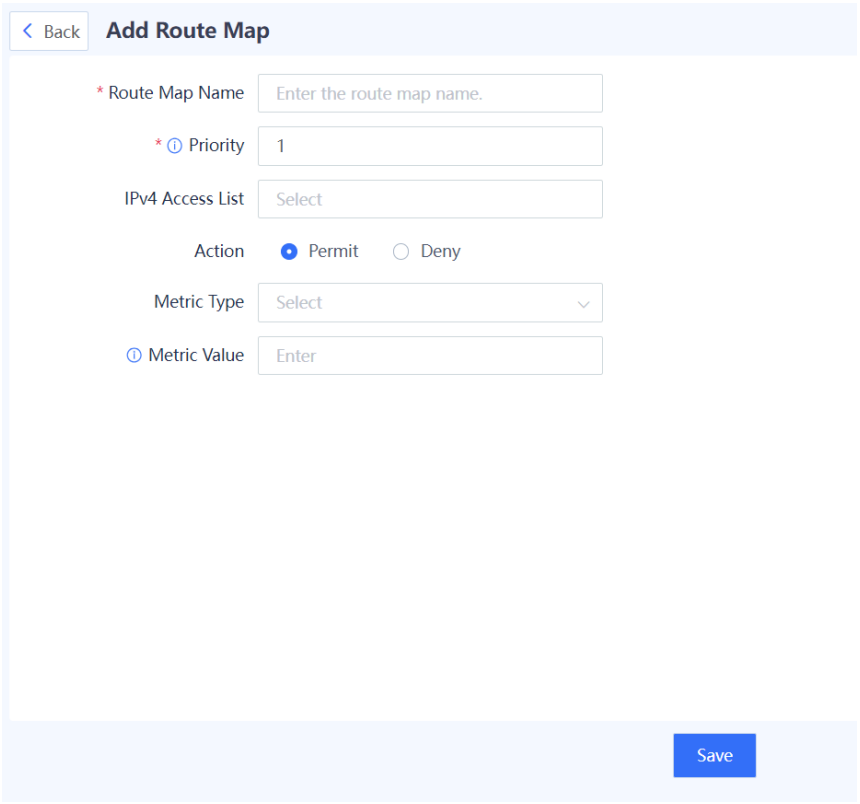
b Click the **Route Map** tab.



c Click **Create**.



d Configure a route map.



Item	Description	Remarks
Route Map Name	Route map name. A maximum of 50 route maps with different names can be configured, and a maximum of 10 route maps with the same name can be configured. That is, a total of 500 route maps can be configured.	[Example] list_1
Priority	A lower value indicates a higher priority. Route maps with the same name cannot have the same priority.	[Example] 1
IPv4 Access List	Referenced IPv4 access list. A referenced access list cannot be deleted directly. It can be deleted only after the route map is deleted. If no access list is configured: When the action is set to **Permit**, all routes are advertised. When the action is set to **Deny**, no route is advertised.	Select from the drop-down list.
Action	Action to be taken: ● **Permit**: Routes that match the rule can be advertised. ● **Deny**: Routes that match the rule cannot be advertised.	[Example] Permit
Metric Type	Metric type. The value can be type 1 or type 2 external route.	[Example] type-1

Metric Value	Metric value.	[Example] 1

e Click **Save**.

Follow-up Procedure

- On the **Access List** and **Route Map** tab pages, you can delete or edit access lists or route maps.
- For details about invoking route maps, see 6.4.6 3. (Optional) Configuring Advanced OSPF Settings.

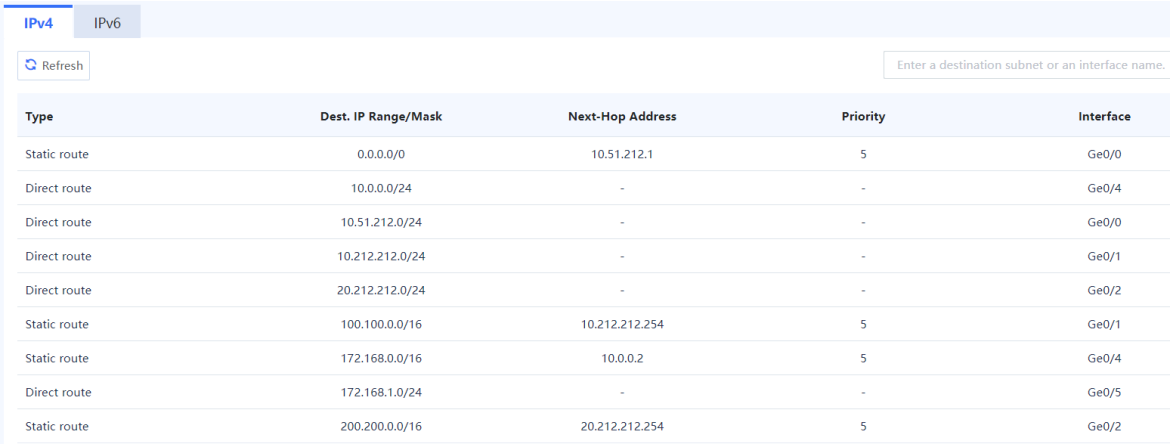
6.3.6 Viewing Route Tables

Procedure

(1) Choose **Network** > **Routing/Load Balancing** > **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	10.51.212.1	5	Ge0/0
Direct route	10.0.0.0/24	-	-	Ge0/4
Direct route	10.51.212.0/24	-	-	Ge0/0
Direct route	10.212.212.0/24	-	-	Ge0/1
Direct route	20.212.212.0/24	-	-	Ge0/2
Static route	100.100.0.0/16	10.212.212.254	5	Ge0/1
Static route	172.168.0.0/16	10.0.0.2	5	Ge0/4
Direct route	172.168.1.0/24	-	-	Ge0/5
Static route	200.200.0.0/16	20.212.212.254	5	Ge0/2

6.4 OSPF

6.4.1 Overview

The Open Shortest Path First (OSPF) protocol is an Interior Gateway Protocol (IGP) that is used within the autonomous system (AS) to allow devices to obtain routes to a remote network.

In the early stage of dynamic routing, Routing Information Protocol (RIP) was mainly used on networks. RIP is a distance vector routing protocol, facing some problems such as slow convergence, routing loop, poor scalability, and is used for simple networks only. OSPF version 2 (OSPFv2) is a link-state routing protocol, which addresses the preceding problems. Therefore, OSPFv2 is widely used on large and medium-sized networks.

Note

OSPFv2 is applicable to IPv4, and OSPF Version 3 (OSPFv3) is applicable to IPv6. The protocol running mechanism and most configurations are the same.

6.4.2 Concepts

1. Configuring the Router ID

The router ID uniquely identifies a router in an OSPF area. Router IDs of any two routers cannot be the same.

2. Area

On a large network where each device runs OSPF, an increase in the number of devices leads to the data volume rise of the link-state database (LSDB). This results in high storage space consumption and increases the complexity of the Shortest Path First (SPF) algorithm, incurring heavy device load. In addition, any change in the topology triggers all devices on the network to recalculate routes.

As shown in Figure 6-3, the OSPF protocol solves the problem of frequent LSDB updates by dividing the AS into different areas. In this way, OSPF improves network utilization and relieves the computing pressure on large networks. An area is a logical group of devices, and each group is identified by an area ID. The border between areas is a device. A device may belong to one area or multiple areas. One network segment (link) can belong to only one area. That is, each OSPF-enabled interface must belong to a specified area.

OSPF areas fall into the following types:

- Common area

Common areas include a backbone area and normal areas. Area 0 is the backbone area, and other areas are normal areas. Normal areas must be directly connected to the backbone area.

- Stub area

Configuring a stub area can reduce the number of Link State Advertisements (LSAs) in the area. The Area Border Router (ABR) in the stub area does not transfer Type 5 LSAs (external routes), but advertises the default route to the stub area.

- Totally stub area

A totally stub area is upgraded from a stub area. A router in the totally stub area does not transfer Type 3 LSAs (inter-domain routes) and Type 5 LSAs (external routes), but advertises the default route to the stub area.

- NSSA

A Not-So-Stubby Area (NSSA) is similar to a stub area, but can contain an Autonomous System Boundary Router (ASBR). The route redistributed by an ASBR is transferred in the NSSA in the form of Type 7 LSA, and the Type 7 LSA is translated into Type 5 LSA on the ABR and then transferred to other areas. The ABR also advertises the default route to the NSSA.

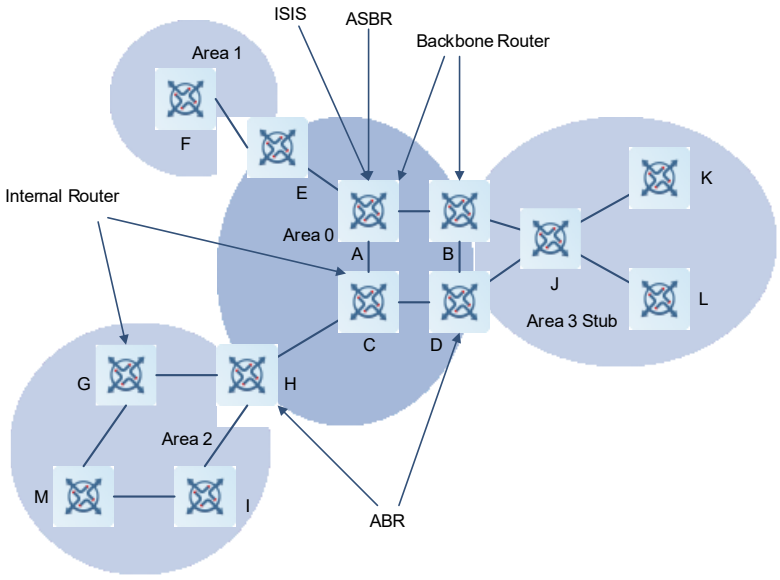
- Totally NSSA

The relationship between a totally NSSA and NSSA is similar to that between a totally stub area and stub area. Different from an NSSA, a totally NSSA forbids transfer of Type 3 LSAs (inter-domain routes).

Note

- A backbone area cannot be configured as a stub area, totally stub area, NSSA, or totally NSSA.
- A stub area or totally stub area cannot contain any ASBR.

Figure 6-3 Different Types of OSPF Areas and Routers



3. OSPF Device Role

The following device roles are defined in OSPF, and assigned with different responsibilities:

- Internal router

All interfaces of an internal router belong to the same area, For example, routers A, C, F, G, I, M, J, K, and L in Figure 6-3.

- ABR

An ABR connects a normal area to the backbone area. An ABR belongs to two or more areas, and one of the areas must be the backbone area, For example, routers B, D, E, and H in Figure 6-3.

- Backbone router

A backbone router has at least one interface that belongs to the backbone area. All ABRs and all internal routers in Area 0 are backbone routers. For example, routers A, B, C, D, E, and H in Figure 6-3.

- ASBR

An ASBR exchanges routing information with other ASs. An ASBR is not necessarily located on the border of an area. It can be an internal router or ABR. For example, router A in Figure 6-3.

4. LSA

OSPF encapsulates and advertises routing information description by using LSAs. Table 6-1 lists common LSA types.

Table 6-1 OSPF LSA Types

LSA Type	Description
Router-LSA (Type 1)	This LSA is generated by each router. It describes the link state and cost of the router, and is advertised in the area to which the router belongs.

Network-LSA (Type 2)	This LSA is generated by a designated router (DR). It describes the link states on the local network segment, and is advertised in the area to which the DR belongs.
Network-summary-LSA (Type 3)	This LSA is generated by an ABR. It describes a route to a specific network segment in an area, and is advertised to all areas except totally stub areas and NSSAs.
ASBR-summary-LSA (Type 4)	This LSA is generated by an ABR. It describes a route to an ASBR, and is advertised to all areas except the area to which the ASBR belongs.
AS-external-LSA (Type 5)	This LSA is generated by an ASBR. It describes a route to a destination outside the AS, and is advertised to all areas except stub areas and NSSAs.
NSSA LSA (Type 7)	This LSA is generated by an ASBR. It describes a route to a destination outside the AS, and is advertised only in the NSSA.
Opaque LSA (Type 9/Type 10/Type 11)	An Opaque LSA provides a universal mechanism for OSPF extension, wherein: ● Type 9 LSAs are advertised only on the network segment where the interface originating Type 9 LSAs resides. Grace LSAs used for Graceful Restart (GR) are a type of Type 9 LSAs. ● Type 10 LSAs are advertised in an OSPF area. LSAs used for Traffic Engineering (TE) are a type of Type 10 LSAs. ● Type 11 LSAs are advertised in an AS. Currently, no applications of Type 11 LSAs are available.

Note

An ABR uses Type 3 LSAs to advertise a default route to the stub/totally stub area or NSSA/totally NSSA.

An ABR converts Type 7 LSAs in the NSSA/totally NSSA to Type 5 LSAs, and advertises Type 5 LSAs to the backbone area.

5. OSPF Packet

OSPF encapsulates its data in IP packets. OSPF packets fall into five types, as listed in Table 6-2.

Table 6-2 OSPF Packet Types

Packet Type	Description
Hello	Hello packets are sent periodically to discover and maintain OSPF neighbor relationships.
DD	Database Description (DD) packets carry brief information about the local LSDB and are used to synchronize LSDBs between OSPF neighbors.

LSR	Link State Request (LSR) packets are used to request the required LSAs from neighbors. LSR packets are sent only after DD packets are exchanged successfully between OSPF neighbors.
LSU	Link State Update (LSU) packets are used to send the required LSAs to neighbors.
LSAck	Link State Acknowledgement (LSAck) packets are used to acknowledge the receipt of an LSA.

6. OSPF Network Type

OSPF classifies networks into two types according to the link layer protocol, as listed in Table 6-3.

Table 6-3 OSPF Network Types

Network Type	Neighbor Relationship and DR Election
Broadcast	● Neighbors are automatically discovered, and the DR and backup designated router (BDR) are elected. ● The DR or BDR exchanges LSAs with all the other routers to establish adjacencies. ● Except the DR and BDR, all the other routers do not exchange LSAs with each other, and no adjacency is established.
P2P	● Neighbors are automatically discovered, and the DR or BDR is not elected. ● Routers at both ends exchange LSAs to establish an adjacency.

7. DR and BDR

On a broadcast network, many unnecessary LSAs are created when adjacencies are established between routers. To address this problem, OSPF defines the DR and BDR.

After the DR and BDR are elected, all routers establish adjacencies with only the DR and BDR, and send routing information to only the DR or BDR. Then the DR broadcasts network link states. The routers other than the DR and BDR are called DR others. The DR others do not establish adjacencies or exchange any routing information with each other, thereby reducing the number of adjacencies between routers on the broadcast network, as shown in Figure 6-4 and Figure 6-5.

Figure 6-4 Number of Adjacencies Before DR Election

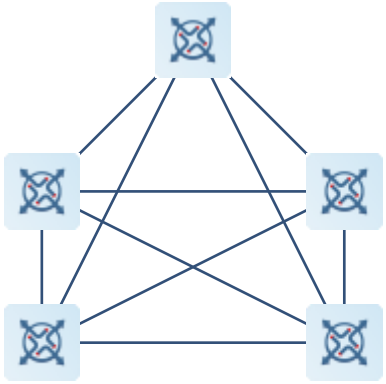
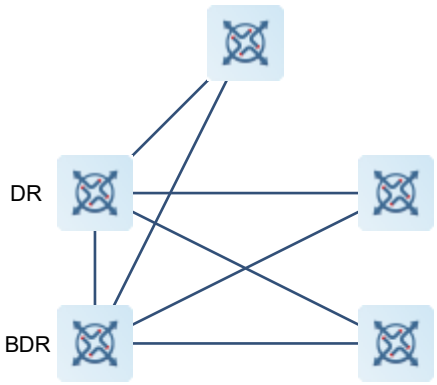


Figure 6-5 Number of Adjacencies After DR Election



8. OSPF Administrative Distance

The administrative distance (AD) is used to evaluate the reliability of a route. A smaller AD value indicates that the route is more trustworthy. If there are multiple routes to the same destination, the router preferentially selects a route with a smaller AD value. The route with a larger AD value becomes a floating route, that is, a backup route of the optimal route. The AD value is a concept at the local end. Modifying the AD value affects route selection only on the local router.

6.4.3 Working Principle of OSPF

1. OSPF Neighbor States

On the OSPF network, neighbor devices need to establish adjacencies before exchanging link information. Devices can establish neighbor relationships and adjacencies with each other.

- Neighbor relationship: If Hello packets can be exchanged between two routers, and parameters carried in the Hello packets can be successfully negotiated, the two routers establish a neighbor relationship.
- Adjacency: If two neighbor routers successfully exchange LSAs and synchronize LSDBs, the two routers establish an adjacency.

OSPF has eight neighbor states, as listed in Table 6-4.

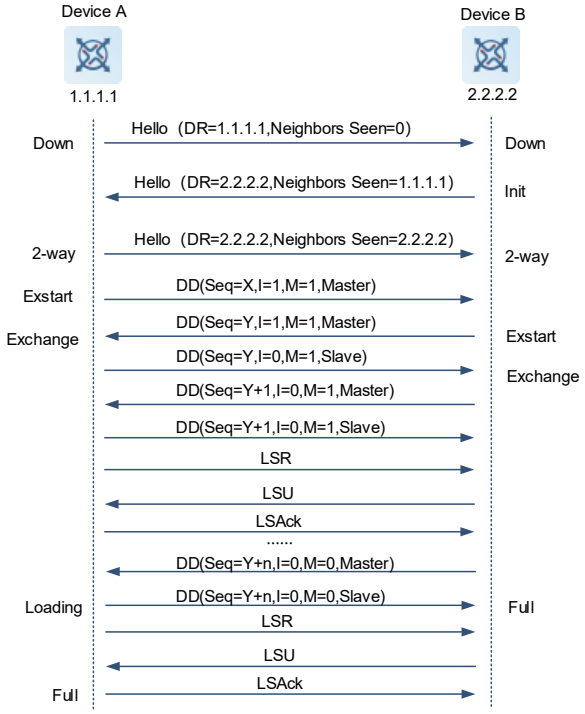
Table 6-4 OSPF Neighbor State Machine and Description

Neighbor State Machine	Description
Down	Initial OSPF neighbor state, which indicates that a router fails to receive Hello packets from its neighbor before the dead interval expires.
Init	The local router receives a Hello packet sent from its neighbor, but the peer router does not receive a Hello packet sent from the local router.

Two-Way	Mutual neighbors: ● Both ends receive the Hello packet sent from the peer end, and establish a neighbor relationship. ● After this phase ends, DR and BDR are elected for broadcast access.
Exstart	Negotiation on the master/slave relationship: ● The initial sequence number is selected for establishing an adjacency. ● The master/slave relationship ensures sequential transmission of DD packets.
exchange	DD packets are exchanged to check whether the neighbor can provide new or updated link state information.
Loading	Based on the information provided by database descriptor (DBD) packets, routers exchange LSR and LSU packets to synchronize LSDBs.
Full	The LSDBs of the two routers have been synchronized, and the local router establishes an adjacency with its neighbor.

Figure 6-6 shows the OSPF adjacency establishment process on a broadcast network. In Full state, the two routers establish an adjacency with each other.

Figure 6-6 OSPF Adjacency Establishment Process on a Broadcast Network



2. OSPF Working Process

OSPF is a link-state routing protocol. Its working process consists of three phases:

(1) Neighbor discovery → Bidirectional communication

Adjacent routers establish an OSPF neighbor relationship and maintain bidirectional communication.

Routers send Hello packets through all OSPF-enabled interfaces. If Hello packets can be exchanged between two routers, and parameters carried in the Hello packets can be successfully negotiated, the two routers establish a neighbor relationship. When routers that are mutual neighbors find their own router IDs in Hello packets sent from neighbors, bidirectional communication is set up.

A Hello packet includes, but is not limited to, the following information:

- ID of the originating router
- Area ID, subnet mask, authentication information, Hello packet interval, and dead interval of the originating router interface
- IP addresses of the DR and BDR
- Priority of the originating router interface (used for DR/BDR election)
- Router ID of the neighbor of the originating router

(2) Database synchronization → Full adjacency

A router uses LSAs to advertise all its link states. Neighbors exchange LSAs to synchronize LSDBs and achieve full adjacency.

After bidirectional communication is set up between neighbor routers, the routers use DD, LSR, LSU, and LSAck packets to exchange LSAs and establish adjacencies. The brief process is as follows:

A router generates an LSA to describe all link states on the router.

- Neighbor routers exchange LSAs. When a router receives an LSA from its neighbor, it copies the LSA and saves the copy in the local LSDB, and then advertises the LSA to other neighbors.
- When the router and its neighbors obtain the same LSDB, full adjacency is achieved.

Note

If no changes in link costs or network changes (addition/deletion) occur, OSPF does not generate LSDB updates and advertisements. If any change takes place, the changed link states are advertised to quickly synchronize LSDBs.

(3) Shortest Path Tree (SPT) calculation → Routing table generation

The router calculates the shortest path to each destination network based on the LSDB and forms an OSPF routing table.

After the complete LSDB is obtained from the router, the Dijkstra algorithm is run to generate an SPT from the local router to each destination network. The SPT records the destination networks, next-hop addresses, and costs. OSPF generates a routing table based on the SPT.

If any change in link costs or network change (addition/deletion) occurs, the LSDB is updated. The router runs the Dijkstra algorithm again, generates a new SPT, and updates the routing table.

Note

The Dijkstra algorithm is used to find the shortest path from a vertex to other vertices in a weighted directed graph.

6.4.4 OSPF Route Advertisement

1. Route Redistribution

Route redistribution refers to the process of introducing default routes, static routes, and direct routes on the device to an OSPF process so that these routes can be advertised to neighbors using Type 5 and Type 7 LSAs.

Route redistribution is often used for inter-AS interconnection. You can configure route redistribution on an ASBR to advertise route information outside an AS to the inside of the AS, or route information inside an AS to the outside of the AS.

2. OSPF Route Types

Each OSPF route is preceded by an identifier that indicates the type of the route. Route advertisement on the device supports the following two OSPF route types:

- E1: Type 1 external route

This type of route describes how to reach a destination network outside an AS. The cost of this type of route is the addition of the route cost from the local router to the ASBR and the route cost from the ASBR to the destination network. This type of route does not exist on routers in the stub area or NSSA.

- E2: Type 2 external route

This type of route also describes how to reach a destination network outside an AS. However, the cost of this type of route is the route cost from the ASBR to the destination network only. This type of route does not exist on routers in the stub area or NSSA.

Note

The reliability of E2 routes is lower. OSPF considers that the route cost from the ASBR to a destination outside an AS is far larger than the route cost from the local router to the ASBR within the AS. Therefore, when the route cost is calculated, only the route cost from the ASBR to a destination outside an AS is considered.

6.4.5 OSPF Route Summarization

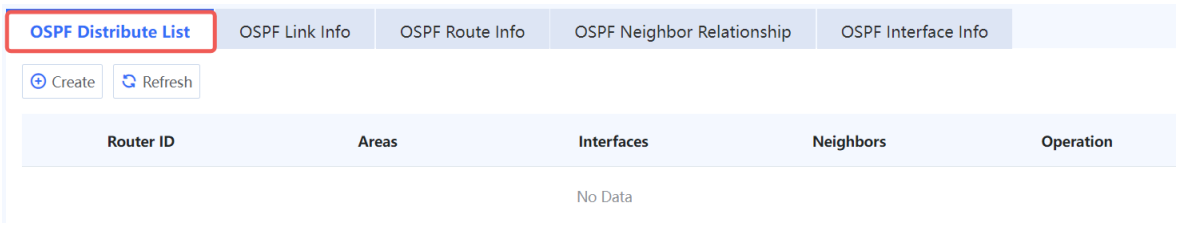
Route summarization is a process of summarizing routing information with the same prefix into one route, and only advertising the summarized route to neighbors. Route summarization helps reduce the protocol interaction load and routing table size, enhancing route stability.

6.4.6 OSPF Configurations

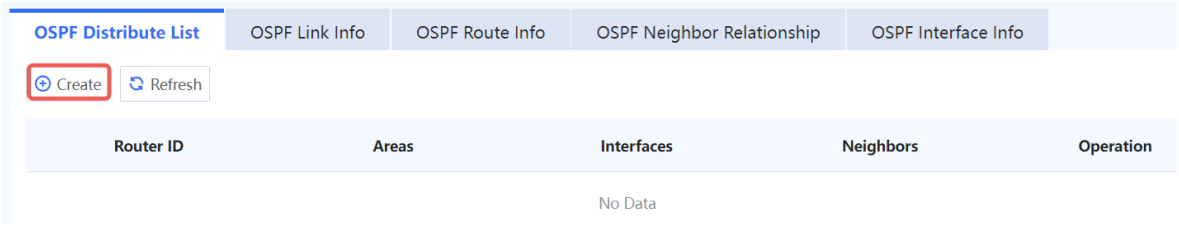
1. Configuring a Router ID

(1) Choose **Network** > **Routing/Load Balancing** > **OSPF**.

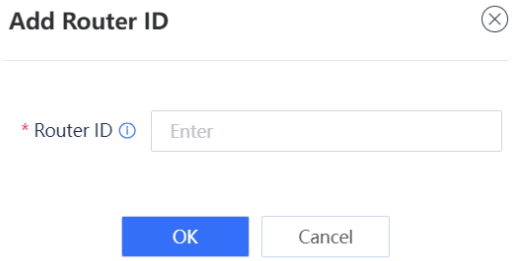
(2) Click the **OSPF Distribute List** tab.



(3) Click **Create**.



(4) In the **Add Router ID** dialog box that is displayed, configure a router ID.



Item	Description	Remarks
Configuring the Router ID	Unique ID of the router. Enter a valid IP address except 0.0.0.0.	Enter a valid IP address. [Example] 192.168.1.1

(5) Click **OK**.

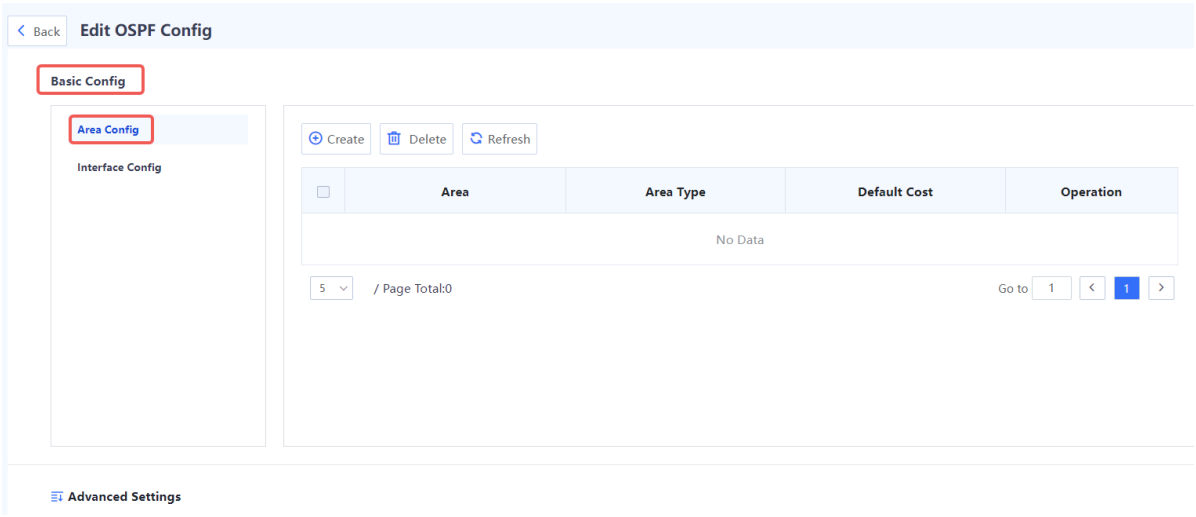
2. Setting Basic OSPF Configurations

(1) Configure an area.

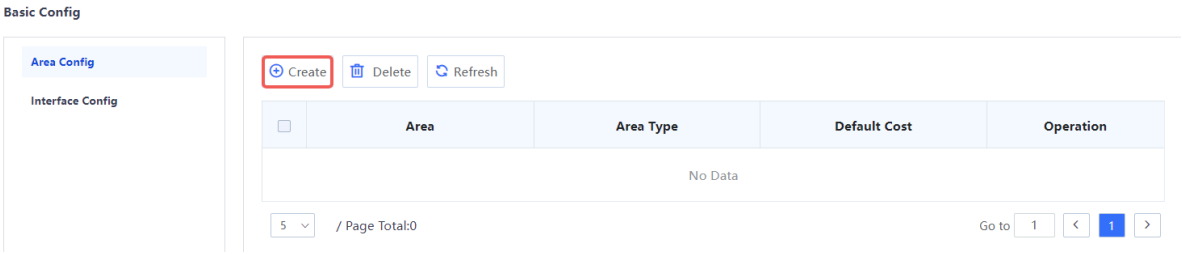
a Click **Edit** in the **Operation** column of a router.



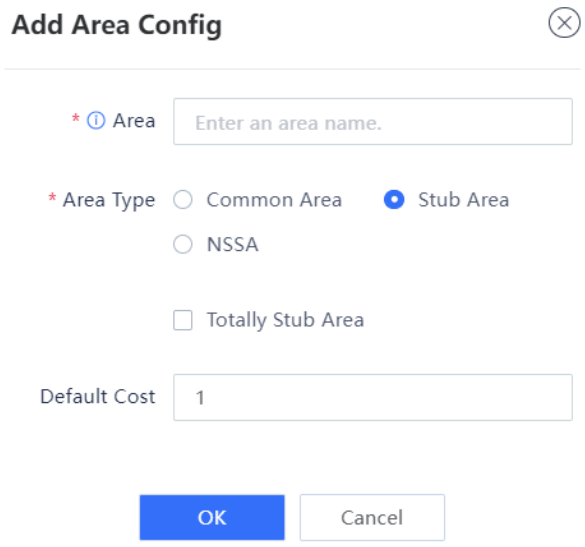
b Choose **Basic Config** > **Area Config**.



c Click **Create**.



d In the dialog box that is displayed, configure an area.

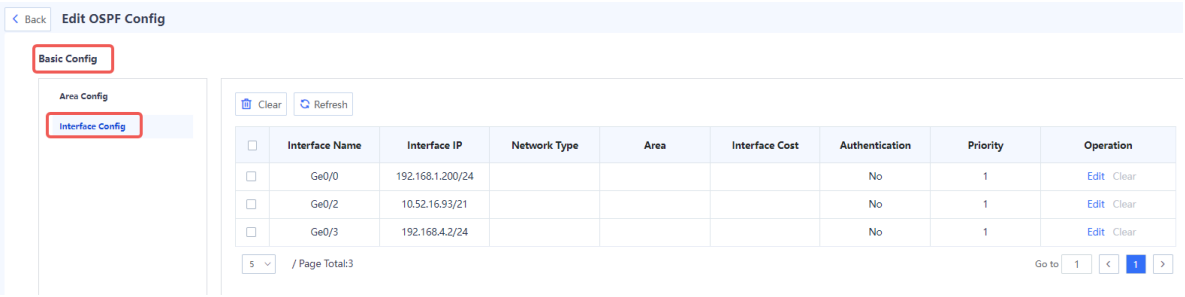


Item	Description	Remarks
Area	Area ID. To create a backbone area, set the value to 0.0.0.0. Only one backbone area can be established.	Enter a valid IPv4 address. [Example] 1.1.1.1
Area Type	The following three types are supported: ● **Common Area**: Set **Area** to 0.0.0.0 to create a backbone area. Set **Area** to another valid IP address to create a normal area. The default cost value is not displayed for both backbone and normal areas. ● **Stub Area**: Click **Stub Area** only to create a stub area, or click **Stub Area** and select **Totally Stub Area** to create a totally stub area. The default cost value is displayed for both stub and totally stub areas. ● **NSSA**: Click **NSSA** only to create an NSSA, or click **NSSA** and select **Totally NSSA** to create a totally NSSA. The default cost value is displayed for both NSSA and totally NSSA.	[Example] Stub Area
Default Cost	Cost of the default route advertised to the stub area or NSSA through OSPF. This parameter is mandatory when **Area Type** is **Stub Area** or **NSSA**.	[Example] 2

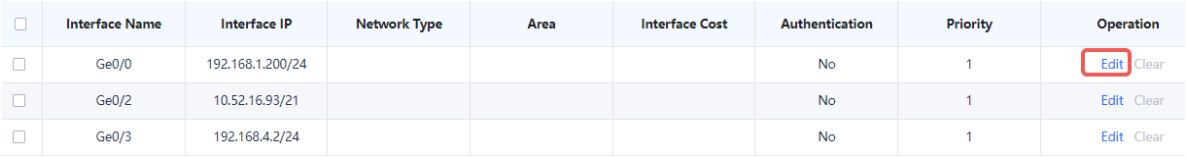
e Click **OK**.

(2) Configure an interface.

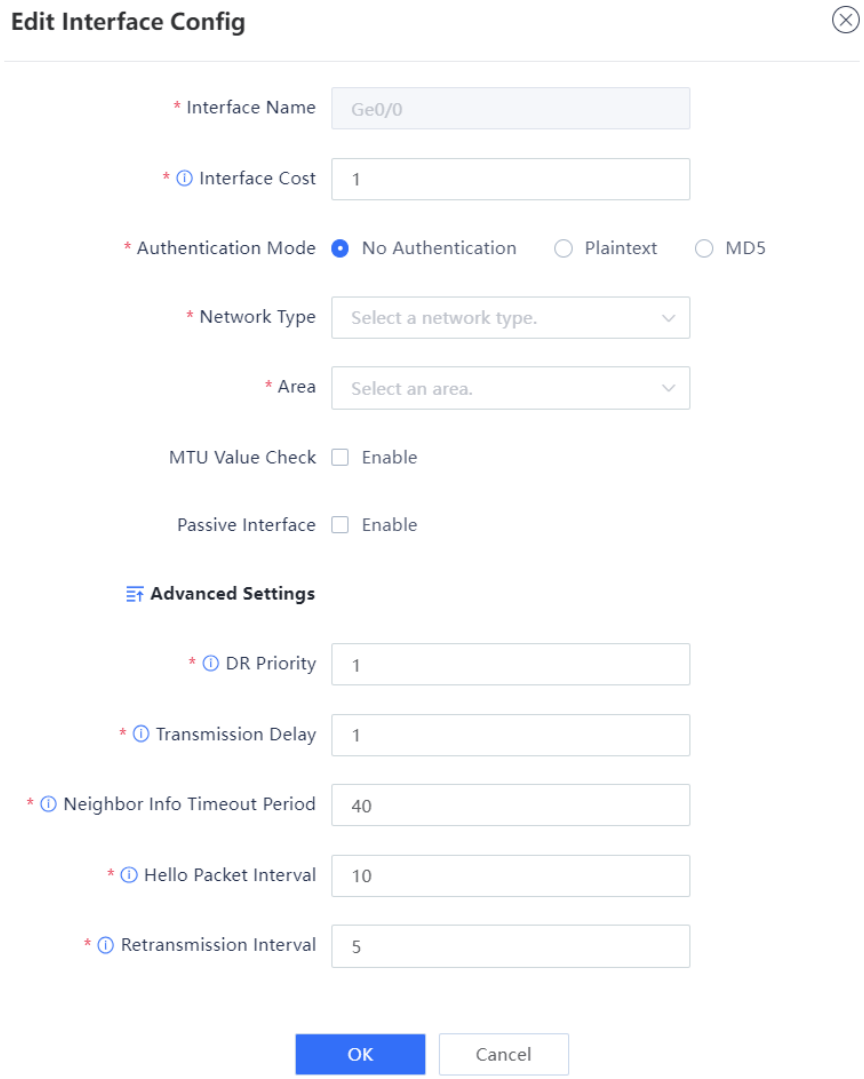
a Choose **Basic Config** > **Interface Config**.



b Click **Edit** in the **Operation** column of the interface.



c Configure interface settings.



Item	Description	Remarks
Interface Name	Name of an OSPF interface.	The system automatically displays the interface name. [Example] Ge0/0
Interface Cost	Cost required to run the OSPF protocol on the interface. The interface cost value is determined by dividing the bandwidth reference value by the interface bandwidth. If the result is smaller than 0, the integer value 1 should be used.	[Example] 1

Item	Description	Remarks
Authentication Mode	Packet authentication mode of the OSPF interface: ● **No Authentication**: no authentication ● **Plaintext**: plaintext authentication ● **MD5**: MD5 authentication If **Plaintext** or **MD5** is selected, you need to set a key.	[Example] 2
Network Type	Network type of the OSPF interface. ● **Broadcast**: The network type is broadcast. ● **Point-to-Point**: The network type is P2P.	Select from the drop-down list.
Area	Associated area of the interface. If an associated area is deleted, a message is displayed indicating that the area is referenced by an interface.	Select from the drop-down list.
MTU Value Check	When receiving a DD packet, OSPF checks whether the MTU value of the interface on the neighbor is the same as that of the local interface. If the interface MTU value in the received DD packet is larger than that of the local interface, the adjacency cannot be established. To resolve this problem, you can disable MTU value check. By default, this option is not selected.	[Example] Enable
Passive Interface	To prevent other routers on the network from learning the routing information of the local router, you can configure a specified network interface on the local router as a passive interface. The passive interface cannot send or receive OSPF packets. By default, this option is not selected.	[Example] Disable
(Optional) Advanced Settings		
DR Priority	The router with the highest priority becomes the DR, and the router with the second highest priority becomes the BDR. A router with the DR priority of 0 does not participate in the DR/BDR election. The default value is 1 second.	[Example] 1
Transmission Delay	LSA packet transmission delay of the interface. The default value is 1 second.	[Example] 1

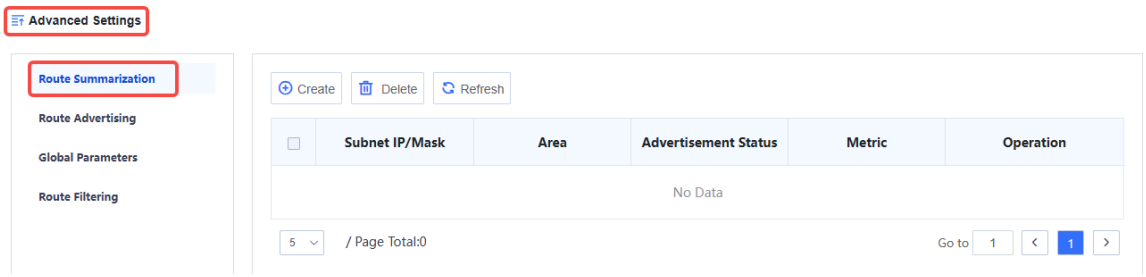
Item	Description	Remarks
Neighbor Info Timeout Period	The neighbor information timeout period must be longer than the Hello packet interval. The default value is 40 seconds. If the values on both ends are different, they cannot establish a neighbor relationship.	[Example] 40
Hello Packet Interval	A shorter Hello packet interval indicates that OSPF can detect topology changes more quickly, but the network traffic increases. The Hello packet interval must be shorter than the neighbor information timeout period. The default value is 10 seconds. If the values on both ends are different, they cannot establish a neighbor relationship.	[Example] 10
Retransmission Interval	After a router sends an LSA to its neighbor, it waits for the acknowledgment packet from the neighbor. If no acknowledgment packet is received within the specified interval, the LSA is retransmitted. The default value is 5 seconds.	[Example] 5

d Click **OK**.

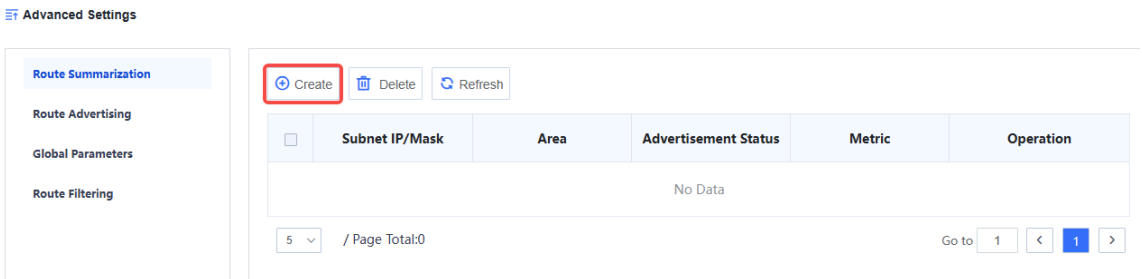
3. (Optional) Configuring Advanced OSPF Settings

(1) Configure route summarization.

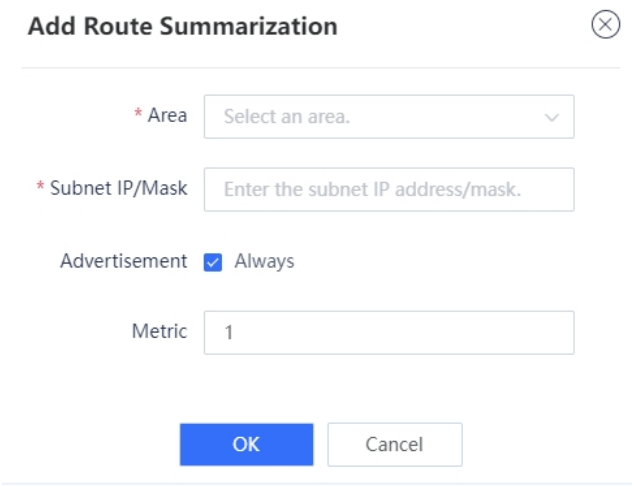
a Choose **Advanced Settings** > **Route Summarization**.



b Click **Create**.



c Configure route summarization.

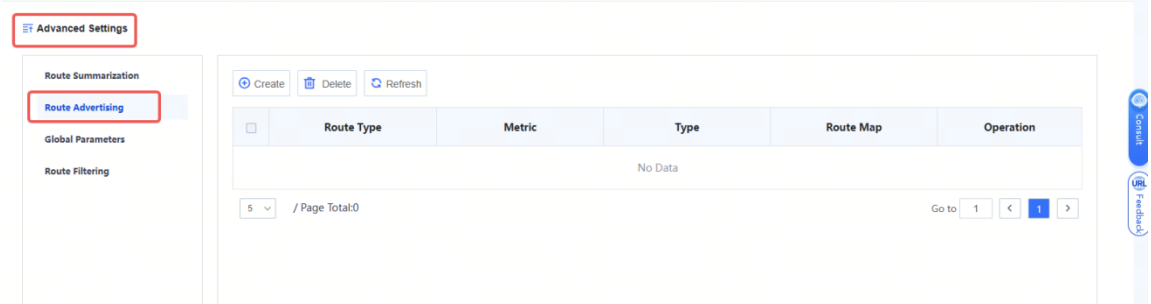


Item	Description	Remarks
Area	Route summarization area.	Select from the drop-down list.
Subnet IP/Mask	IPv4 subnet and mask for route summarization. The subnet address cannot be larger than or equal to 224.0.0.0. After a subnet address is configured, it is automatically summarized. For example, if 1.1.1.1/24 is configured, it automatically changes to 1.1.1.0/24.	[Example] 192.168.1.0/24
Advertisement	Whether to advertise the summary route to adjacent areas that are not totally stub area or totally NSSA.	[Example] Enabled
Metric	Summary route metric.	[Example] 1

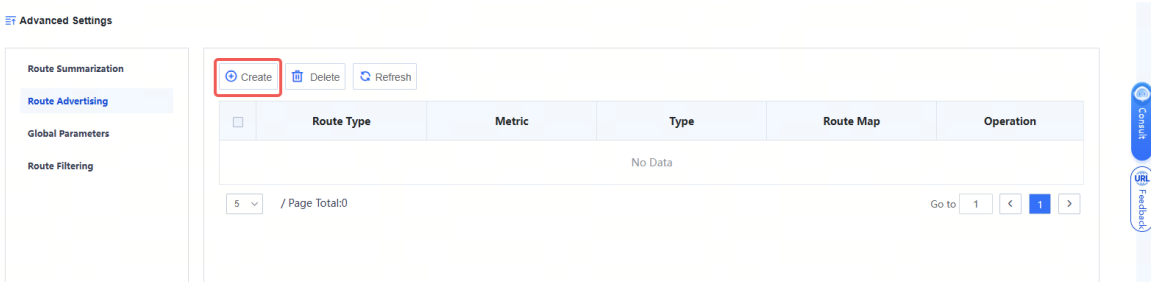
d Click **OK**.

(2) Configure route advertisement.

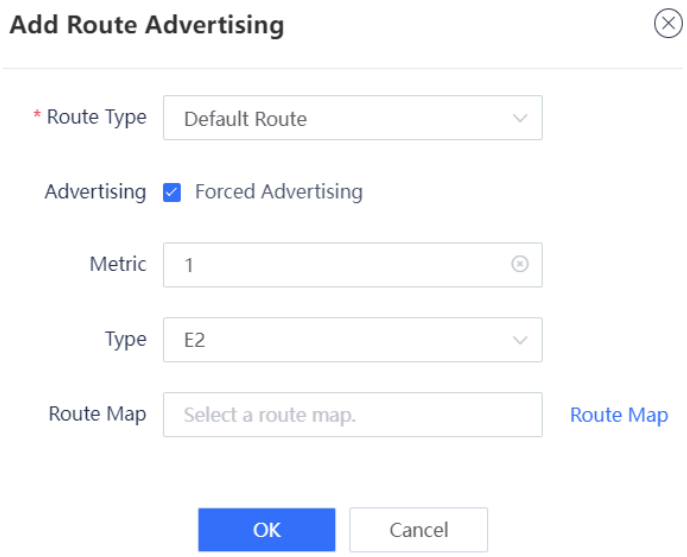
a Choose **Advanced Settings** > **Route Advertising**.



b Click **Create**.



c Configure route advertisement settings.



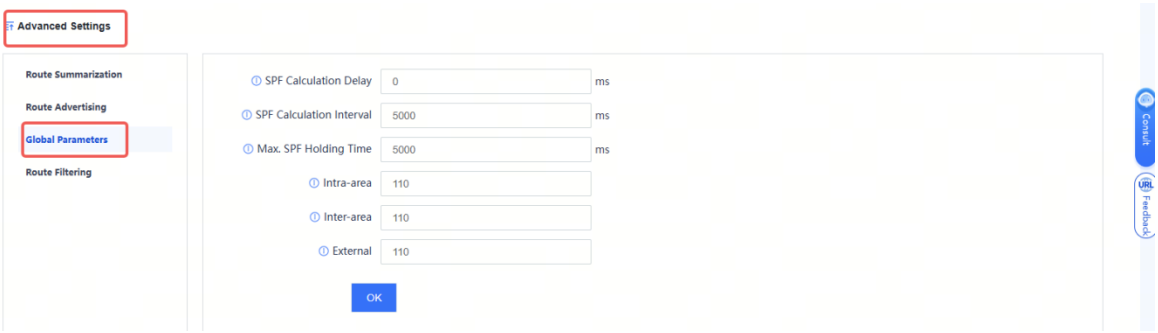
Item	Description	Remarks
Route Type	Select **Default Route**, **Static Route**, or **Direct Route**. Each type of routes can be introduced only once.	[Example] Default Route
Advertising	Whether to advertise routes to neighbors.	[Example] Disabled
Metric	Link metric.	[Example] 1
Type	The following two types are supported: ● **E1**: Type 1 external route ● **E2**: Type 2 external route	[Example] E2
Route Map	Set a route map by specifying an access list to filter routing information. For details on how to configure a route map, see 6.3.5 Configuring a Routing Policy.	Select from the drop-down list.

d Click **OK**.

(3) Configure global parameters.

a Choose **Advanced Settings** > **Global Parameters**.

b Configure global parameters.

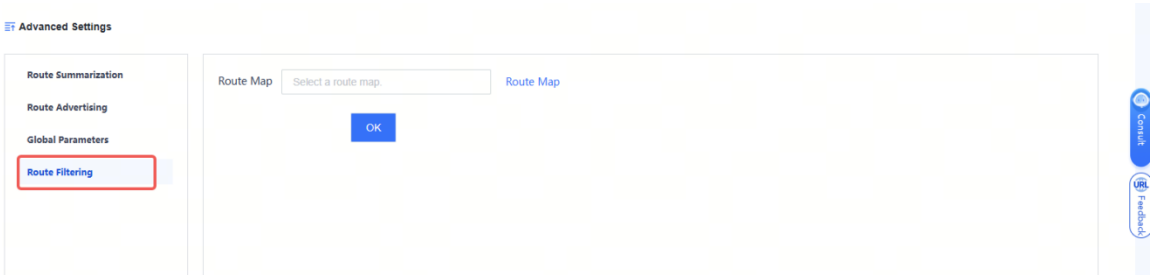


Item	Description	Remarks
SPF Calculation Delay	The minimum time between a topology change and the start of SPF calculation. The default value is 0.	[Example] 0
SPF Calculation Interval	Interval between the completion of the first SPF calculation and the start of the second SPF calculation. The next interval is always longer than the previous interval. The default value is 5000.	[Example] 5000
Max. SPF Holding Time	Maximum waiting time between two SPF calculations. The default value is 5000.	[Example] 5000
Intra-area	Administrative distance of routes inside an OSPF area. A smaller value indicates a higher priority. The default value is 110.	[Example] 110
Inter-area	Administrative distance of routes between OSPF areas. A smaller value indicates a higher priority. The default value is 110.	[Example] 110
External	Administrative distance of routes outside an OSPF area. A smaller value indicates a higher priority. The default value is 110.	[Example] 110

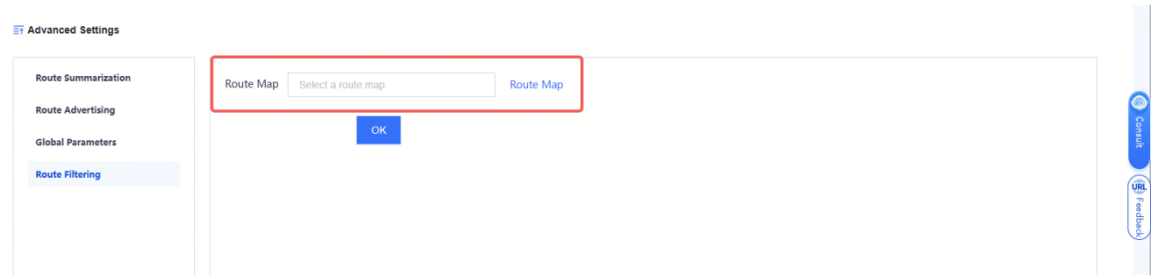
c Click **OK**.

(4) Configure route filtering.

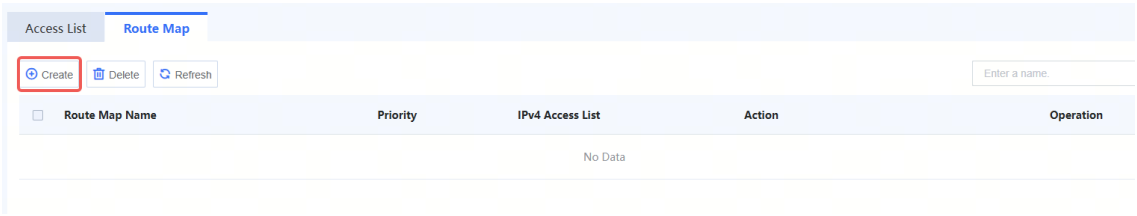
a Choose **Advanced Settings** > **Route Filtering**.



b Select an existing route map or click **Route Map** to add a route map.



c To add a route map, click **Create** to configure the route map. For details about the route map configuration, see 6.3.5 Configuring a Routing Policy.



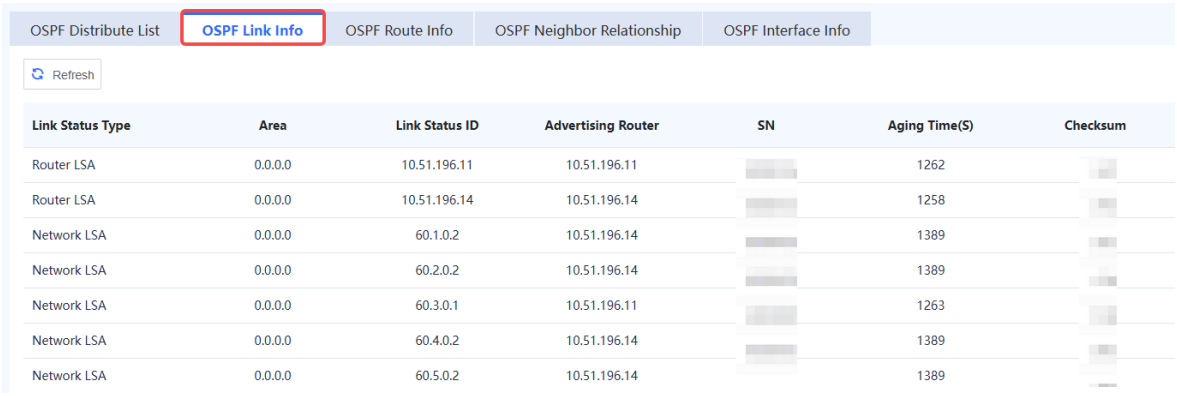
d After the route map is added, return to the OSPF process list and click **Edit** to bind the route map.



4. Viewing OSPF Link Information

(1) Choose **Network** > **Routing/Load Balancing** > **OSPF**.

(2) Click the **OSPF Link Info** tab.

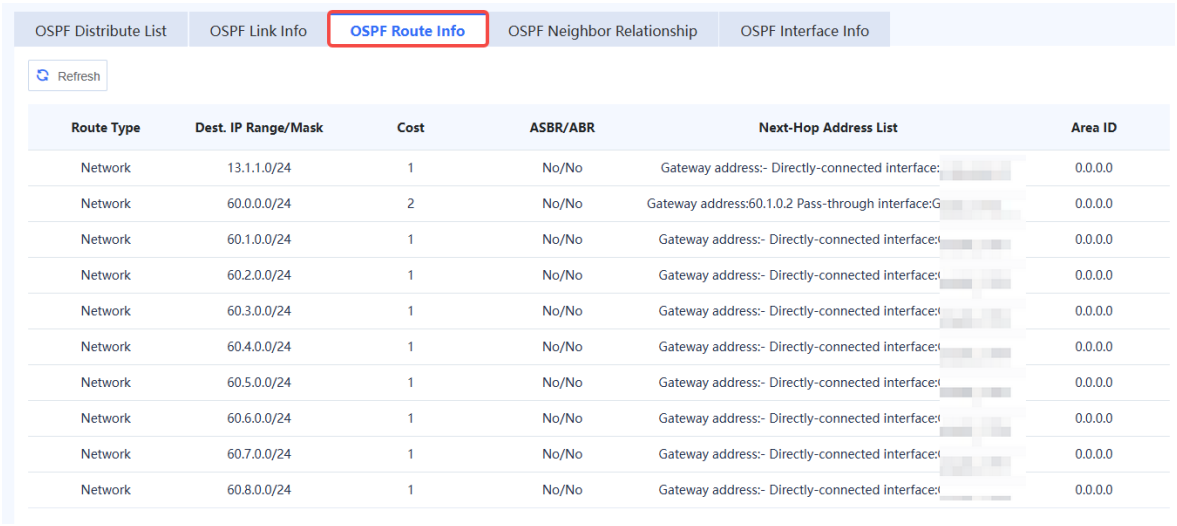


Link Status Type	Area	Link Status ID	Advertising Router	SN	Aging Time(S)	Checksum
Router LSA	0.0.0.0	10.51.196.11	10.51.196.11		1262	
Router LSA	0.0.0.0	10.51.196.14	10.51.196.14		1258	
Network LSA	0.0.0.0	60.1.0.2	10.51.196.14		1389	
Network LSA	0.0.0.0	60.2.0.2	10.51.196.14		1389	
Network LSA	0.0.0.0	60.3.0.1	10.51.196.11		1263	
Network LSA	0.0.0.0	60.4.0.2	10.51.196.14		1389	
Network LSA	0.0.0.0	60.5.0.2	10.51.196.14		1389	

5. Viewing OSPF Route Information

(1) Choose **Network** > **Routing/Load Balancing** > **OSPF**.

(2) Click the **OSPF Route Info** tab.

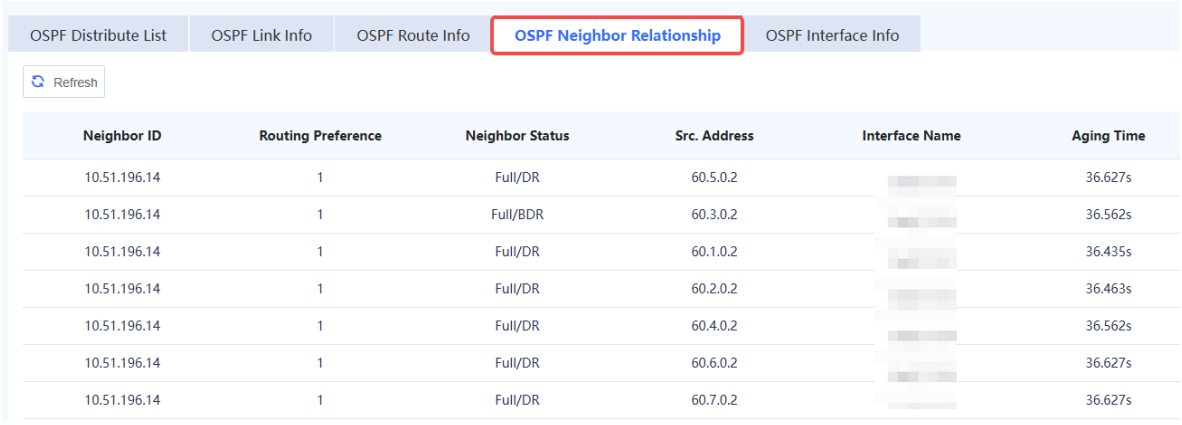


Route Type	Dest. IP Range/Mask	Cost	ASBR/ABR	Next-Hop Address List	Area ID
Network	13.1.1.0/24	1	No/No	Gateway address:- Directly-connected interface:	0.0.0.0
Network	60.0.0.0/24	2	No/No	Gateway address:60.1.0.2 Pass-through interface:G	0.0.0.0
Network	60.1.0.0/24	1	No/No	Gateway address:- Directly-connected interface:	0.0.0.0
Network	60.2.0.0/24	1	No/No	Gateway address:- Directly-connected interface:	0.0.0.0
Network	60.3.0.0/24	1	No/No	Gateway address:- Directly-connected interface:	0.0.0.0
Network	60.4.0.0/24	1	No/No	Gateway address:- Directly-connected interface:	0.0.0.0
Network	60.5.0.0/24	1	No/No	Gateway address:- Directly-connected interface:	0.0.0.0
Network	60.6.0.0/24	1	No/No	Gateway address:- Directly-connected interface:	0.0.0.0
Network	60.7.0.0/24	1	No/No	Gateway address:- Directly-connected interface:	0.0.0.0
Network	60.8.0.0/24	1	No/No	Gateway address:- Directly-connected interface:	0.0.0.0

6. Viewing OSPF Neighbor Relationships

(1) Choose **Network** > **Routing/Load Balancing** > **OSPF**.

(2) Click the **OSPF Neighbor Relationship** tab.

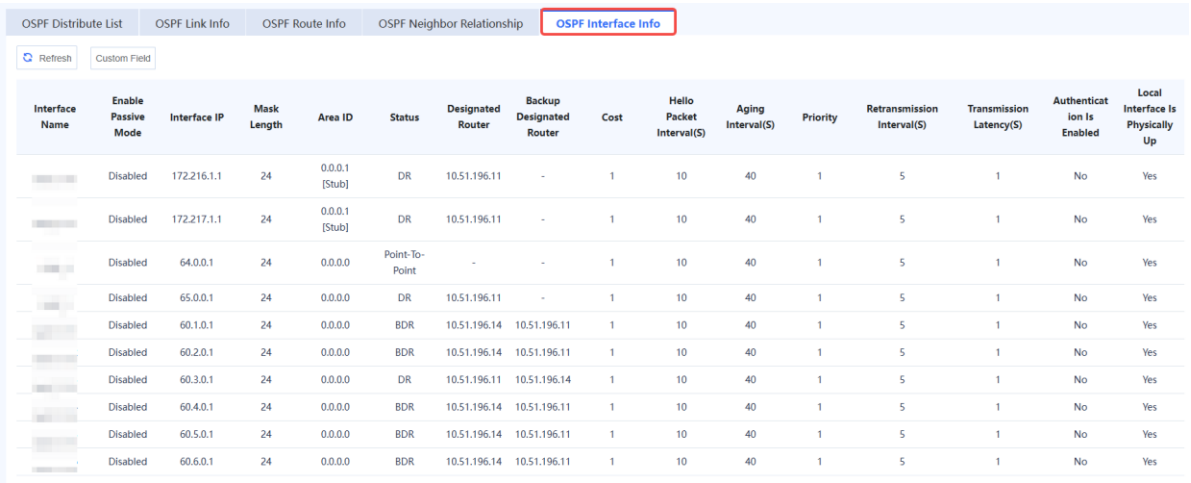


Neighbor ID	Routing Preference	Neighbor Status	Src. Address	Interface Name	Aging Time
10.51.196.14	1	Full/DR	60.5.0.2		36.627s
10.51.196.14	1	Full/BDR	60.3.0.2		36.562s
10.51.196.14	1	Full/DR	60.1.0.2		36.435s
10.51.196.14	1	Full/DR	60.2.0.2		36.463s
10.51.196.14	1	Full/DR	60.4.0.2		36.562s
10.51.196.14	1	Full/DR	60.6.0.2		36.627s
10.51.196.14	1	Full/DR	60.7.0.2		36.627s

7. Viewing OSPF Interface Information

(1) Choose **Network** > **Routing/Load Balancing** > **OSPF**.

(2) Click the **OSPF Interface Info** tab.



Interface Name	Enable Passive Mode	Interface IP	Mask Length	Area ID	Status	Designated Router	Backup Designated Router	Cost	Hello Packet Interval(S)	Aging Interval(S)	Priority	Retransmission Interval(S)	Transmission Latency(S)	Authentication Is Enabled	Local Interface Is Physically Up
	Disabled	172.216.1.1	24	0.0.0.1 [Stub]	DR	10.51.196.11	-	1	10	40	1	5	1	No	Yes
	Disabled	172.217.1.1	24	0.0.0.1 [Stub]	DR	10.51.196.11	-	1	10	40	1	5	1	No	Yes
	Disabled	64.0.0.1	24	0.0.0.0	Point-To-Point	-	-	1	10	40	1	5	1	No	Yes
	Disabled	65.0.0.1	24	0.0.0.0	DR	10.51.196.11	-	1	10	40	1	5	1	No	Yes
	Disabled	60.1.0.1	24	0.0.0.0	BDR	10.51.196.14	10.51.196.11	1	10	40	1	5	1	No	Yes
	Disabled	60.2.0.1	24	0.0.0.0	BDR	10.51.196.14	10.51.196.11	1	10	40	1	5	1	No	Yes
	Disabled	60.3.0.1	24	0.0.0.0	DR	10.51.196.11	10.51.196.14	1	10	40	1	5	1	No	Yes
	Disabled	60.4.0.1	24	0.0.0.0	BDR	10.51.196.14	10.51.196.11	1	10	40	1	5	1	No	Yes
	Disabled	60.5.0.1	24	0.0.0.0	BDR	10.51.196.14	10.51.196.11	1	10	40	1	5	1	No	Yes
	Disabled	60.6.0.1	24	0.0.0.0	BDR	10.51.196.14	10.51.196.11	1	10	40	1	5	1	No	Yes

6.5 OSPFv3

6.5.1 Overview

The Open Shortest Path First Version 3 (OSPFv3) protocol based on IPv6 is an IGP based on the link state and is used within an AS to allow devices to obtain routes to a remote network.

OSPFv3 and OSPFv2 have similar protocol running mechanisms and most configurations are the same. Their major differences are as follows:

- OSPFv2 is used on IPv4 networks, whereas OSPFv3 is used on IPv6 networks.
- OSPFv3 has two new types of LSAs: Link LSA and Intra Area Prefix LSA. They are used to advertise the IPv6 global address information of a link or an area.

6.5.2 Concepts

1. Router ID

The router ID uniquely identifies a router in an OSPFv3 area. Router IDs of any two routers cannot be the same.

2. OSPFv3 Area

An area is a logical group of routers, and each group is identified by an area ID.

OSPFv3 areas fall into the following types:

- Common area

Common areas include a backbone area and normal areas. Area 0 is the backbone area, and other areas are normal areas. Normal areas must be directly connected to the backbone area.

- Stub area

Configuring a stub area can reduce the number of LSAs in the area. The stub area does not allow any ASBR. The ABR in the stub area does not transfer Type 5 LSAs (external routes), and advertises the default route to the stub area.

- Totally stub area

A totally stub area is upgraded from a stub area. The router in the totally stub area does not transfer Type 3 LSAs (inter-domain routes) and Type 5 LSAs (external routes), and advertises the default route to the stub area.

- NSSA

An NSSA is similar to a stub area, but can contain an ASBR. The route redistributed by an ASBR is transferred in the NSSA in the form of Type 7 LSA, and the Type 7 LSA is translated into Type 5 LSA on the ABR and then transferred to other areas. The ABR also advertises the default route to the NSSA.

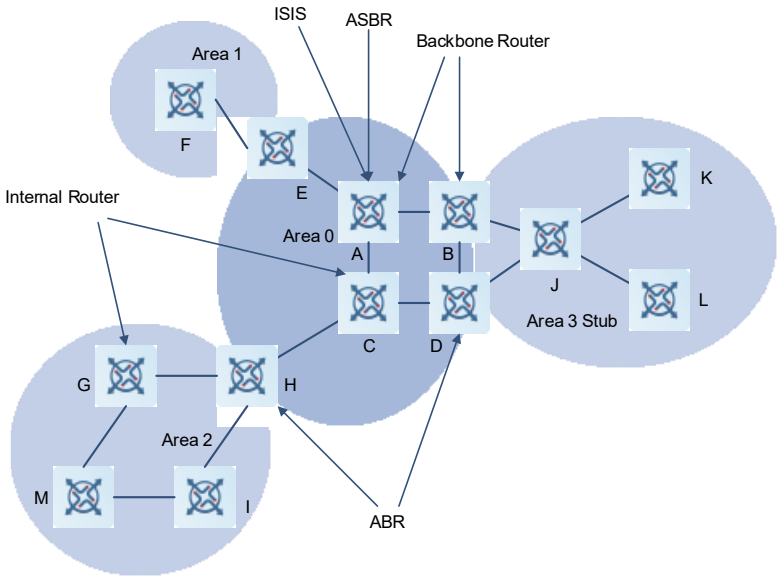
- Totally NSSA

The relationship between the totally NSSA and NSSA is similar to that between the totally stub area and stub area. Different from an NSSA, a totally NSSA forbids transfer of Type 3 LSAs (inter-domain routes).

Note

- The current version does not support the configuration of totally stub area and totally NSSA.
- A backbone area cannot be configured as a stub area, totally stub area, NSSA, or totally NSSA.
- A stub area or totally stub area cannot contain any ASBR.

Figure 6-7 Different Types of OSPFv3 Areas and Routers



3. OSPFv3 Device Role

The following device roles are defined in OSPFv3, and assigned with different responsibilities:

- Internal router

All interfaces of an internal router belong to the same area, for example, routers A, C, F, G, I, M, J, K, and L in Figure 6-7.

- ABR

An ABR connects a normal area to the backbone area. An ABR belongs to two or more areas, and one of the areas must be the backbone area, for example, routers B, D, E, and H in Figure 6-7.

Caution

In the current version, OSPFv3 supports only one area and the device cannot be deployed as an ABR.

- Backbone router

A backbone router has at least one interface that belongs to the backbone area. All ABRs and all internal routers in Area 0 are backbone routers, for example, routers A, B, C, D, E, and H in Figure 6-7.

- ASBR

An ASBR exchanges routing information with other ASs. An ASBR is not necessarily located on the border of an area. It can be an internal router or ABR, for example, router A in Figure 6-7.

4. OSPFv3 LSA

OSPFv3 encapsulates and advertises routing information description by using LSAs. Table 6-5 lists common LSA types.

Table 6-5 OSPFv3 LSA Types

LSA Type	Description
Router-LSA (Type 1)	This LSA is generated by each router. It describes the link state and cost of the router, and is advertised in the area to which the router belongs.
Network-LSA (Type 2)	This LSA is generated by a DR. It describes the link states, and is advertised in the area to which the DR belongs.
Inter-Area-Prefix-LSA (Type 3)	This LSA is generated by an ABR. It describes a route to another area, and is advertised to areas other than the totally stub areas and NSSAs.
Inter-Area-Router-LSA (Type 4)	This LSA is generated by an ABR. It describes a route to an ASBR, and is advertised to all areas except the area to which the ASBR belongs.
AS-external-LSA (Type 5)	This LSA is generated by an ASBR. It describes a route to a destination outside the AS, and is advertised to all areas except stub areas and NSSAs.
NSSA LSA (Type 7)	This LSA is generated by an ASBR. It describes a route to a destination outside the AS, and is advertised only in the NSSA.

LSA Type	Description
Link-LSA (Type 8)	This LSA is generated by every router. It describes the link-local address and IPv6 prefix address of each link, and provides the link option that will be set in the Network-LSA. It is advertised only on the current link.
Intra-Area-Prefix-LSA (Type 9)	Every router or DR generates one or more this type of LSAs, which are advertised in the area to which the router or DR belongs. ● The LSAs generated by a router describe the prefix of an IPv6 address associated with the Router-LSA. ● The LSAs generated by a DR describe the prefix of an IPv6 address associated with the Network-LSA.

5. OSPFv3 Packet

Five OSPFv3 packet types are available, as listed in Table 6-6.

Table 6-6 OSPFv3 Packet Types

Packet Type	Description
Hello	Hello packets are sent periodically to discover and maintain OSPFv3 neighbor relationships.
DD	Database Description (DD) packets carry brief information about the local LSDB and are used to synchronize LSDBs between OSPFv3 neighbors.
LSR	Link State Request (LSR) packets are used to request the required LSAs from neighbors. LSR packets are sent only after DD packets are exchanged successfully between OSPF neighbors.
LSU	Link State Update (LSU) packets are used to send the required LSAs to neighbors.
LSAck	Link State Acknowledgement (LSAck) packets are used to acknowledge the receipt of an LSA.

6. OSPFv3 Network Type

The device supports the following OSPFv3 network types.

Table 6-7 OSPFv3 Network Types

Network Type	Neighbor Relationship and DR Election
Broadcast	● Neighbors are automatically discovered, and the DR and backup designated router (BDR) are elected. ● The DR or BDR exchanges LSAs with all the other routers to establish adjacencies. ● Except for the DR and BDR, all the other routers do not exchange LSAs with each other, and no adjacency is established.
P2P	● Neighbors are automatically discovered, and the DR or BDR is not elected. ● Routers at both ends exchange LSAs to establish an adjacency.

6.5.3 Working Principle of OSPFv3

1. OSPFv3 Neighbor States

On the OSPFv3 network, neighbor devices need to establish adjacencies before exchanging link information. There are several OSPFv3 neighbor states listed below. When a neighbor enters the full state, the adjacency relationship is established.

Table 6-8 OSPFv3 Neighbor State Machine and Description

Neighbor State Machine	Description
Down	Initial OSPFv3 neighbor state, which indicates that a router fails to receive Hello packets from its neighbor before the dead interval expires.
Init	The local router receives a Hello packet sent from its neighbor, but the peer router does not receive a Hello packet sent from the local router.
Two-Way	Mutual neighbors: Both ends receive the Hello packet sent from the peer end, and establish a neighbor relationship.
Exstart	Negotiation on the primary/secondary relationship: ● The initial sequence number is selected for establishing an adjacency. ● The primary/secondary relationship ensures sequential transmission of DD packets.
Exchange	DD packets are exchanged to check whether the neighbor can provide new or updated link state information.
Loading	The LSDBs are being synchronized. Routers exchange LSR and LSU packets to synchronize LSDBs.

Neighbor State Machine	Description
Full	The LSDBs of the two routers have been synchronized, and the local router establishes an adjacency with its neighbor.

2. OSPFv3 Working Process

OSPFv3 is a link-state routing protocol. Its working process consists of three phases:

(1) Neighbor discovery → Bidirectional communication

Adjacent routers establish an OSPFv3 neighbor relationship and maintain bidirectional communication.

Routers send Hello packets through all OSPF-enabled interfaces. If Hello packets can be exchanged between two routers, and parameters carried in the Hello packets can be successfully negotiated, the two routers establish a neighbor relationship. When routers that are mutual neighbors find their own router IDs in Hello packets sent from neighbors, bidirectional communication is set up.

A hello packet includes, but is not limited to, the following information:

- ID of the originating router
- Area ID of the originating router interface
- Instance ID of the originating router interface
- Interface ID of the originating router interface
- Priority of the originating router interface (used for DR/BDR election)
- Hello interval of the originating router interface
- Neighbor dead interval of the originating router interface
- DR and BDR router IDs.
- Router ID of the neighbor of the originating router

(2) Database synchronization → Full adjacency

A router uses LSAs to advertise its link-state information. Neighbors exchange LSAs to synchronize LSDBs and achieve full adjacency.

After bidirectional communication is set up between neighbor routers, the routers use DD, LSR, LSU, and LSAck packets to exchange LSAs and establish adjacencies. The brief process is as follows:

- A router generates an LSA to describe all link states on the router.
- Neighbor routers exchange LSAs. When receiving an LSA from its neighbor, a router copies the LSA and saves the copy in the local LSDB, and then advertises the LSA to other neighbors.
- When the router and its neighbors obtain the same LSDB, full adjacency is achieved.

Note

If no changes in link costs or network changes (addition/deletion) occur, OSPFv3 will be very stable. If any change takes place, the changed link states are advertised to quickly synchronize LSDBs.

(3) SPT calculation → Routing table generation

The router calculates the shortest path to each destination network based on the LSDB and forms an OSPFv3 routing table.

After the complete LSDB is obtained from the router, the Dijkstra algorithm is run to generate an SPT from the local router to each destination network. The SPT records the destination networks, next-hop addresses, and costs. OSPFv3 generates a routing table based on the SPT.

If any change in link costs or network change (addition/deletion) occurs, the LSDB is updated. The router runs the Dijkstra algorithm again, generates a new SPT, and updates the routing table.

6.5.4 OSPFv3 Route Advertisement

1. Route Redistribution

Route redistribution refers to the process of introducing default routes, static routes, and direct routes on the device to an OSPFv3 process so that these routes can be advertised to neighbors using Type 5 and Type 7 LSAs.

Route redistribution is often used for inter-AS interconnection. You can configure route redistribution on an ASBR to advertise route information outside an AS to the inside of the AS, or route information inside an AS to the outside of the AS.

2. OSPFv3 Route Types

Each OSPF route is preceded by an identifier that indicates the type of the route. Route advertisement on the device supports the following two OSPFv3 route types:

- E1: Type 1 external route

This type of route describes how to reach a destination network outside an AS. The cost of this type of route is the addition of the route cost from the local router to the ASBR and the route cost from the ASBR to the destination network. This type of route does not exist on routers in the stub area or NSSA.

- E2: Type 2 external route

This type of route describes how to reach a destination network outside an AS. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub area or NSSA.

Note

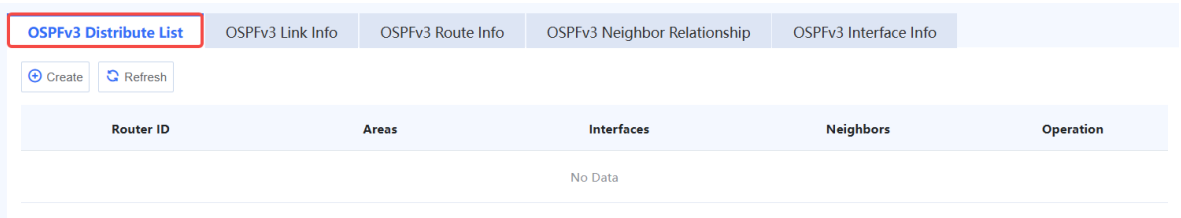
The reliability of E2 routes is lower. OSPFv3 considers that the route cost from the ASBR to a destination outside an AS is far higher than the route cost from the local router to the ASBR within the AS. Therefore, when the route cost is calculated, only the route cost from the ASBR to a destination outside an AS is considered.

6.5.5 OSPFv3 Configurations

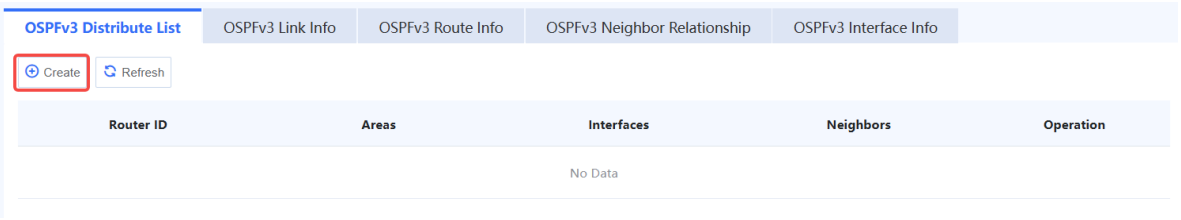
1. Configuring a Router ID

(1) Choose **Network** > **Routing/Load Balancing** > **OSPFv3**.

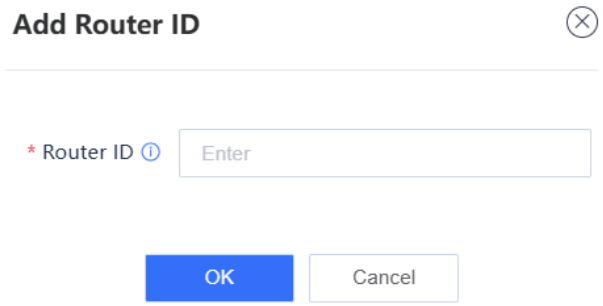
(2) Click the **OSPFv3 Distribute List** tab.



(3) Click **Create**.



(4) In the **Add Router ID** dialog box that is displayed, configure a router ID.



Item	Description	Remarks
Configuring the Router ID	Unique ID of the router. Enter a valid IP address except 0.0.0.0.	Enter a valid IP address. [Example] 192.168.1.1

(5) Click **OK**.

2. Setting Basic OSPFv3 Configurations

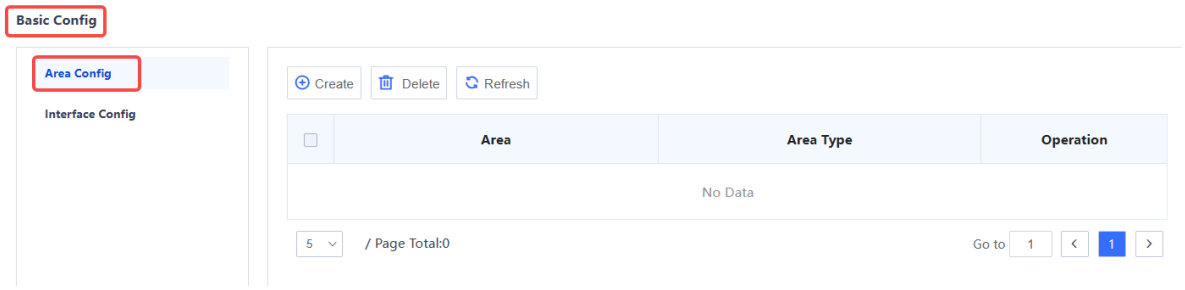
(1) Configure an area.

> **Caution**
>
> Only one zone can be configured.

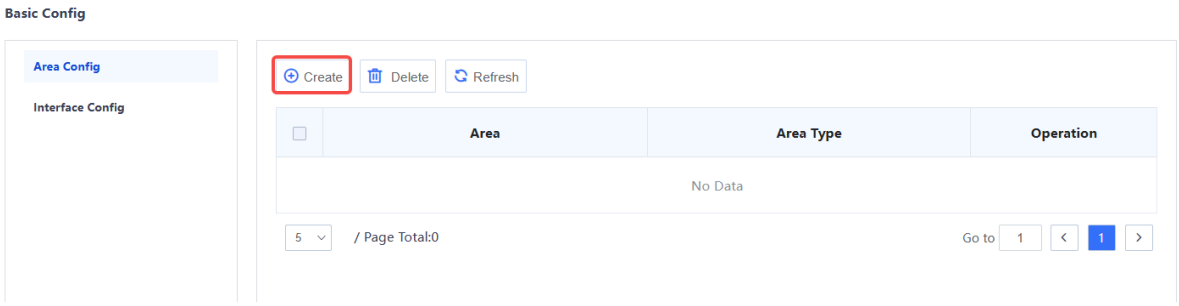
a Click **Edit** in the **Operation** column of a router.



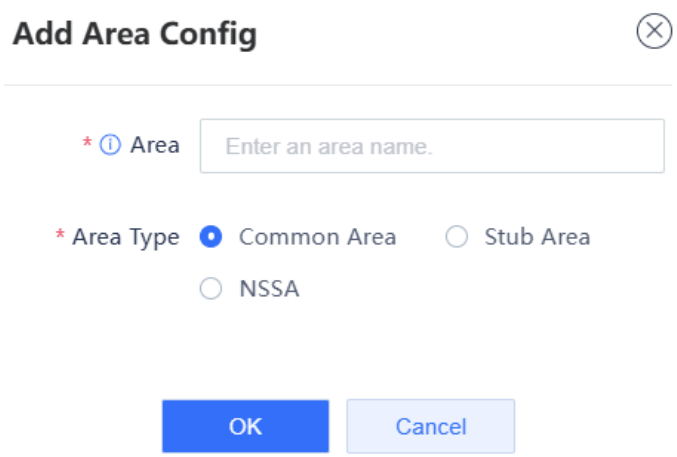
b Choose **Basic Config** > **Area Config**.



c Click **Create**.



d In the dialog box that is displayed, configure an area.



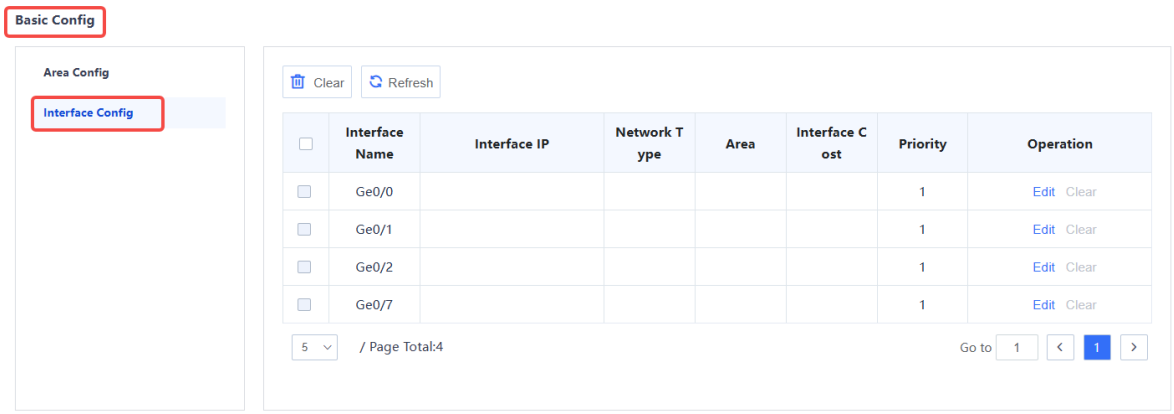
Item	Description	Remarks
Area	Area ID. To create a backbone area, set the value to 0.0.0.0. Only one backbone area can be established.	Enter a valid IPv4 address. [Example] 1.1.1.1

Area Type	The following three types are supported: ● **Common Area**: Set **Area** to 0.0.0.0 to create a backbone area. Set **Area** to another valid IP address to create a normal area. The default cost value is not displayed for both backbone and normal areas. ● **Stub Area**: Click **Stub Area** to create a stub area. ● **NSSA**: Click **NSSA** to create an NSSA.	[Example] Stub Area

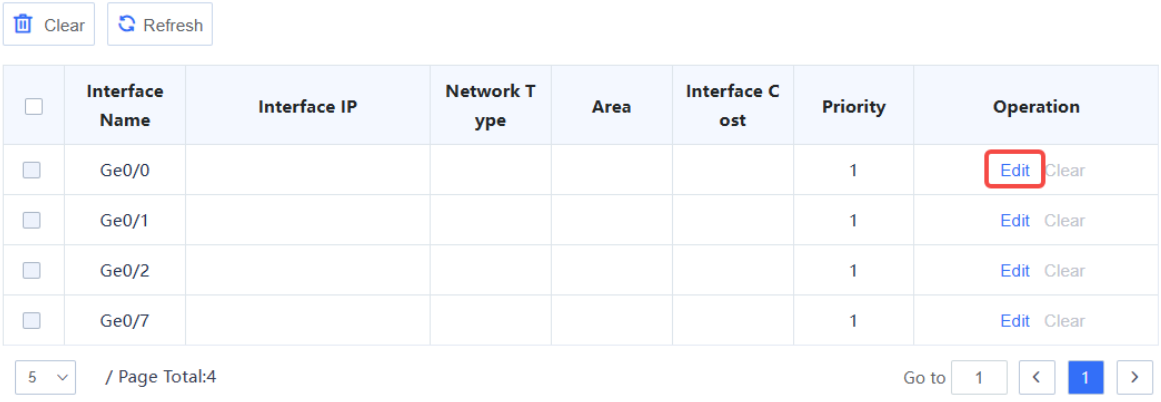
e Click **OK**.

(2) Configure an interface.

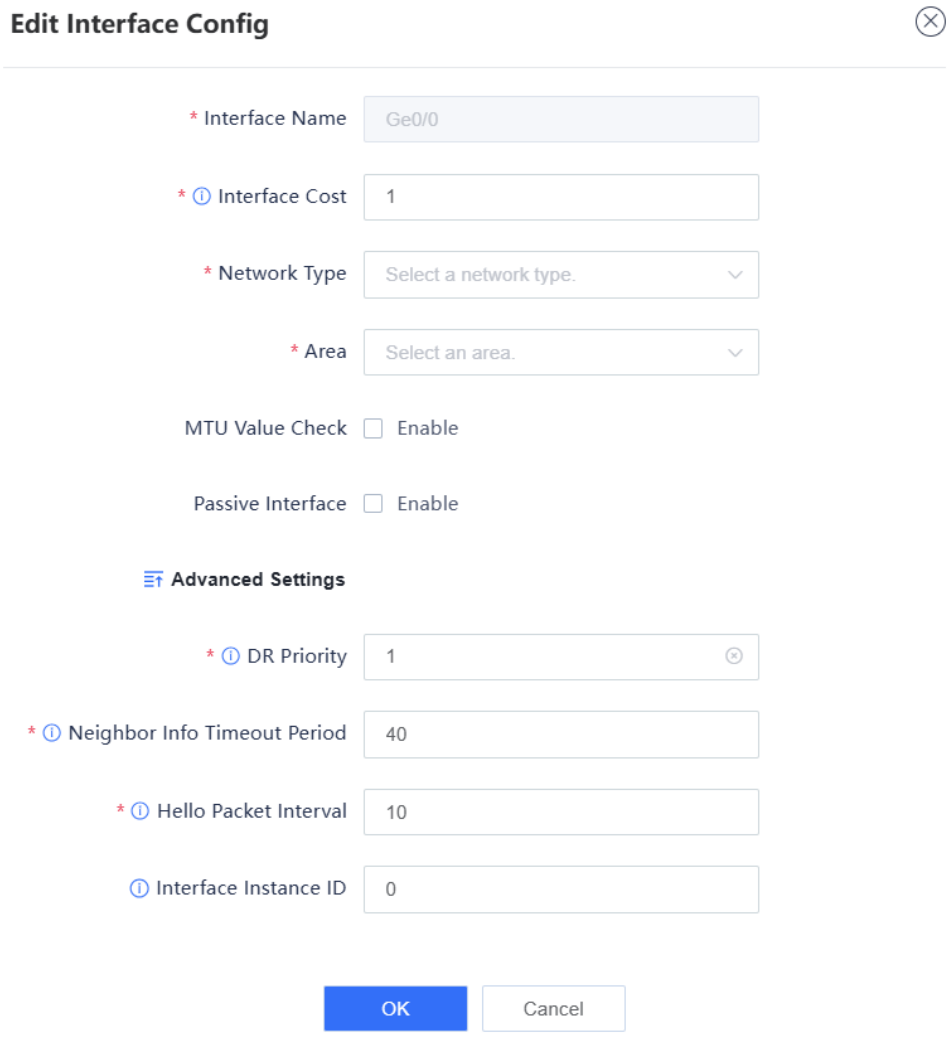
a Choose **Basic Config** > **Interface Config**.



b Click **Edit** in the **Operation** column of the interface.



c Configure interface settings.



Item	Description	Remarks
Interface Name	Name of an OSPFv3 interface.	The system automatically displays the interface name. [Example] Ge0/0
Interface Cost	Cost required to run the OSPFv3 protocol on the interface. The interface cost value is determined by dividing the bandwidth reference value by the interface bandwidth. If the result is smaller than 0, the integer value 1 should be used.	[Example] 1
Network Type	Network type of the OSPFv3 interface. ● **Broadcast**: The network type is broadcast. ● **Point-to-Point**: The network type is P2P.	Select from the drop-down list.

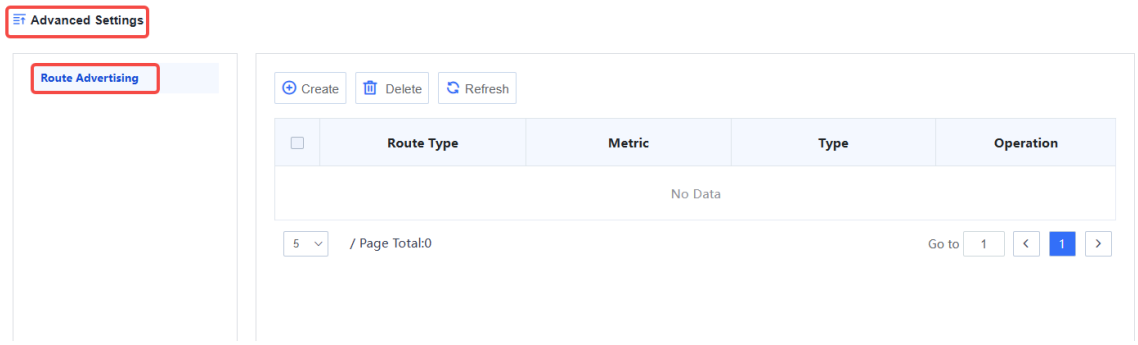
Item	Description	Remarks
Area	Associated area of the interface. If an associated area is deleted, a message is displayed indicating that the area is referenced by an interface.	Select from the drop-down list.
MTU Value Check	When receiving a DD packet, OSPFv3 checks whether the MTU value of the interface on the neighbor is the same as that of the local interface. If the interface MTU value in the received DD packet is larger than that of the local interface, the adjacency cannot be established. To resolve this problem, you can disable MTU value check. By default, this option is not selected.	[Example] Disable
Passive Interface	To prevent other routers on the network from learning the routing information of the local router, you can configure a specified network interface on the local router as a passive interface. The passive interface cannot send or receive OSPFv3 packets. By default, this option is not selected.	[Example] Disable
(Optional) Advanced Settings		
DR Priority	The router with the highest priority becomes the DR, and the router with the second highest priority becomes the BDR. A router with the DR priority of 0 does not participate in the DR/BDR election. The default value is 1.	[Example] 1
Neighbor Info Timeout Period	The neighbor information timeout period must be longer than the Hello packet interval. The default value is 40 seconds. If the values on both ends are different, they cannot establish a neighbor relationship.	[Example] 40
Hello Packet Interval	A shorter interval indicates that OSPFv3 can detect topology changes more quickly, but the network traffic increases. The Hello packet interval must be shorter than the neighbor information timeout period. The default value is 10 seconds. If the values on both ends are different, they cannot establish a neighbor relationship.	[Example] 10

Item	Description	Remarks
Interface Instance ID	ID that is encapsulated in the OSPFv3 header and used to identify an independent OSPFv3 instance on the same link. Instances with different IDs are isolated from each other, and a neighbor relationship can be established only between instances with the same ID at both ends. The default value is 0.	The value range is from 0 to 255. [Example] 0

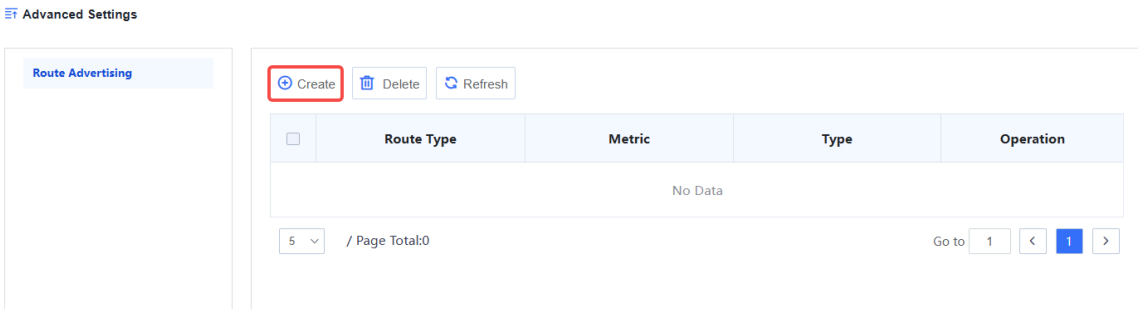
d Click **OK**.

3. (Optional) Configuring Advanced OSPFv3 Settings

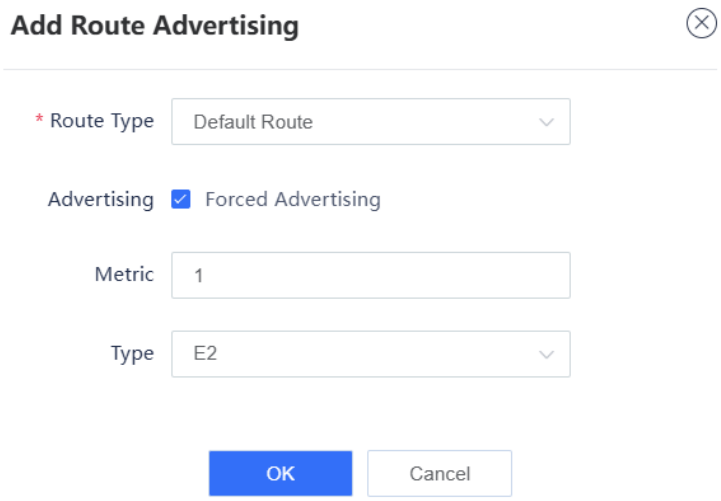
a Choose **Advanced Settings** > **Route Advertising**.



b Click **Create**.



c Configure route advertisement settings.



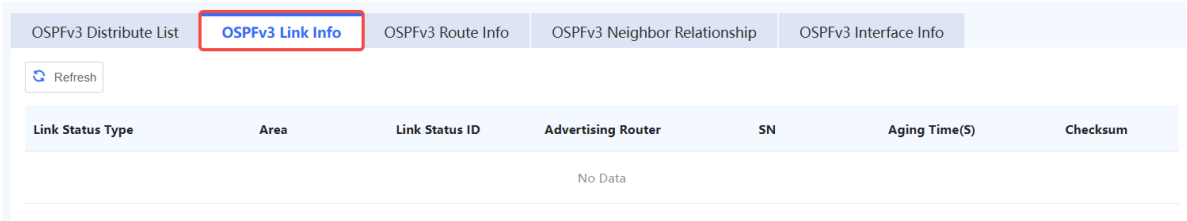
Item	Description	Remarks
Route Type	Select **Default Route**, **Static Route**, or **Direct Route**.	[Example] Default Route
Advertising	Whether to advertise routes to neighbors.	This parameter can be configured when **Route Type** is set to **Default Route**. [Example] Forced Advertising
Metric	Link metric.	[Example] 1
Type	The following two types are supported: ● **E1**: Type 1 external route ● **E2**: Type 2 external route	[Example] E2

d Click **OK**.

4. Viewing OSPFv3 Link Information

(1) Choose **Network** > **Routing/Load Balancing** > **OSPFv3**.

(2) Click the **OSPFv3 Link Info** tab.



5. Viewing OSPFv3 Route Information

(1) Choose **Network** > **Routing/Load Balancing** > **OSPFv3**.

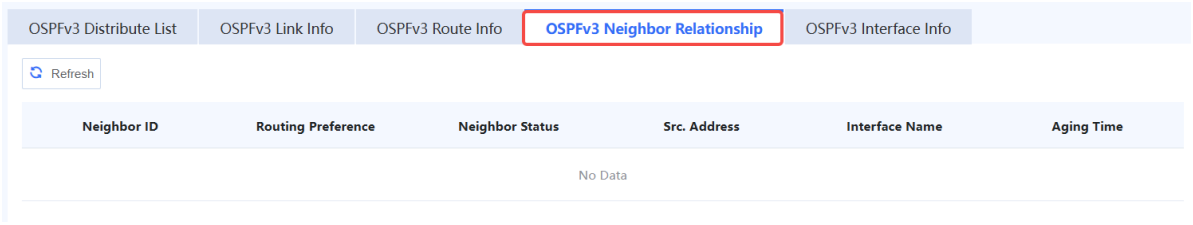
(2) Click the **OSPFv3 Route Info** tab.



6. Viewing OSPFv3 Neighbor Relationships

(1) Choose **Network** > **Routing/Load Balancing** > **OSPFv3**.

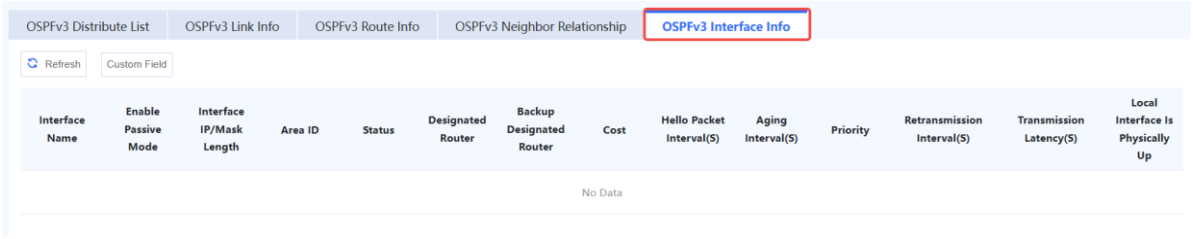
(2) Click the **OSPFv3 Neighbor Relationship** tab.



7. Viewing OSPFv3 Interface Information

(1) Choose **Network** > **Routing/Load Balancing** > **OSPFv3**.

(2) Click the **OSPFv3 Interface Info** tab.



6.6 Outbound Interface Load Balancing

6.6.1 Overview

When there are multiple equivalent egresses (that is, multiple links) for intranet users to access the external network, 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: When there are multiple static routes with the same priority and administrative distance to a destination network, equal-cost static routes exist.
- ISP address library-based routing: When multiple interfaces reference the same address library, equal-cost routes exist.
- DNS transparent proxy: When the link to the DNS server is congested, multiple standby links exist.
- Intelligent routing: When traffic hits a policy, multiple egress links exist.

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 multiple load balancing modes. 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 age.

By default, the device performs load balancing based on the source IP address. The following load balancing modes are supported:

- **Based on Bandwidth+Session**: New traffic is distributed to the link with the lowest session usage (the number of real-time sessions divided by the configured maximum number of sessions) and with a link bandwidth lower than the threshold. When the number of sessions or bandwidth of the link exceeds the configured threshold, the link does not participate in load balancing. This load balancing mode applies to scenarios where the connection number of an asymmetric digital subscriber line (ADSL) is limited, such as a scenario where home broadband and private line services coexist.
- **Based on Src. IP**: Services with the same source address are transmitted over the same link. This mode applies to scenarios such as online banking and gaming.
- **Based on Src. IP+Dest. IP**: Services with the same source and destination IP addresses are transmitted over the same link. This mode applies to scenarios such as online banking and gaming.
- **Based on Bandwidth - Uplink Load**: New traffic is distributed to the link with the smallest uplink bandwidth usage (real-time uplink traffic divided by the uplink bandwidth). Links with the uplink bandwidth usage higher than the uplink load threshold do not participate in load balancing.
- **Based on Bandwidth - Downlink Load**: New traffic is distributed to the link with the smallest downlink bandwidth usage (real-time downlink traffic divided by the downlink bandwidth). Links with the downlink bandwidth usage higher than the downlink load threshold do not participate in load balancing.
- **Based on Bandwidth - Bidirectional Load**: New traffic is distributed to the link with the smallest ratio of the uplink (or downlink) bandwidth usage to the uplink (or downlink) bandwidth. Links with the bandwidth usage higher than the load threshold in the corresponding direction do not participate in load balancing.
- **Based on Bandwidth - Uplink Bandwidth**: New traffic is distributed based on the uplink bandwidth weight. Links with the bandwidth usage higher than the uplink load threshold do not participate in load balancing. The usage weight is not considered before overload.
- **Based on Bandwidth - Downlink Bandwidth:** New traffic is distributed based on the downlink bandwidth ratio. Links with the bandwidth usage higher than the downlink load threshold do not participate in load balancing. The usage weight is not considered before overload.

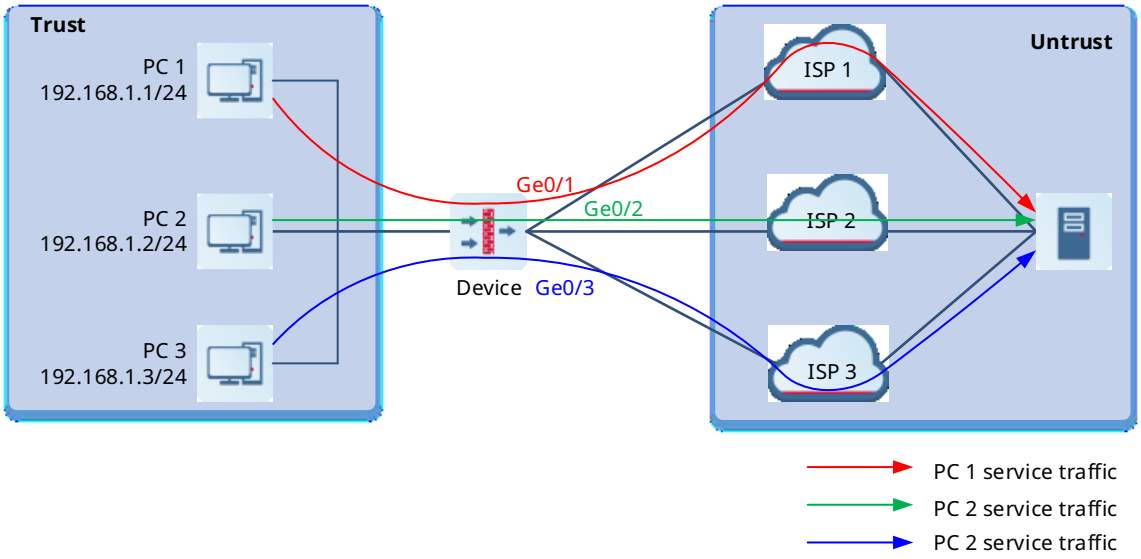
- **Based on Link Weight**: Load balancing is performed among links based on the link weight. Links with larger weights are prioritized in load balancing.
- **Based on Link Priority**: The link with the highest priority is selected for load balancing. This mode applies to scenarios where active and standby lines are deployed.
- **Based on Session**: The link with the lowest session usage (the number of real-time sessions divided by the configured maximum number of sessions) is selected for load balancing.

6.6.2 Configuring Load Balancing Based on the Source IP Address

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

- Multiple 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.

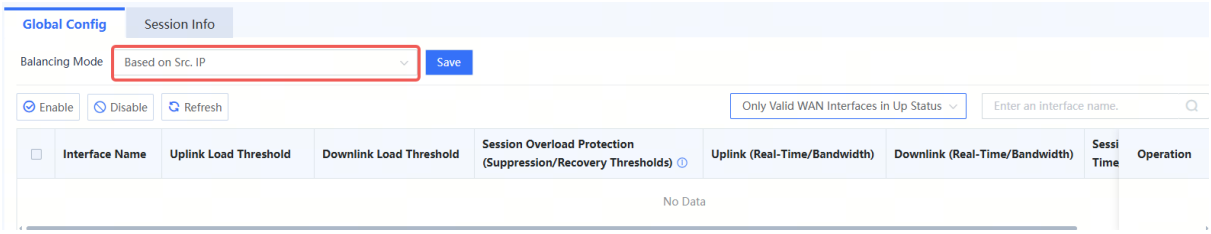
Precautions

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/Load Balancing** > **Egress Load Balancing** > **Global Config**.

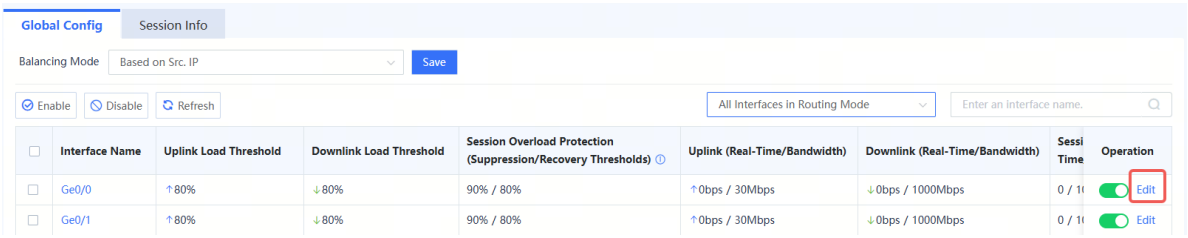
(2) Select **Based on Src. IP** from the **Balancing Mode** drop-down list and click **Save**.



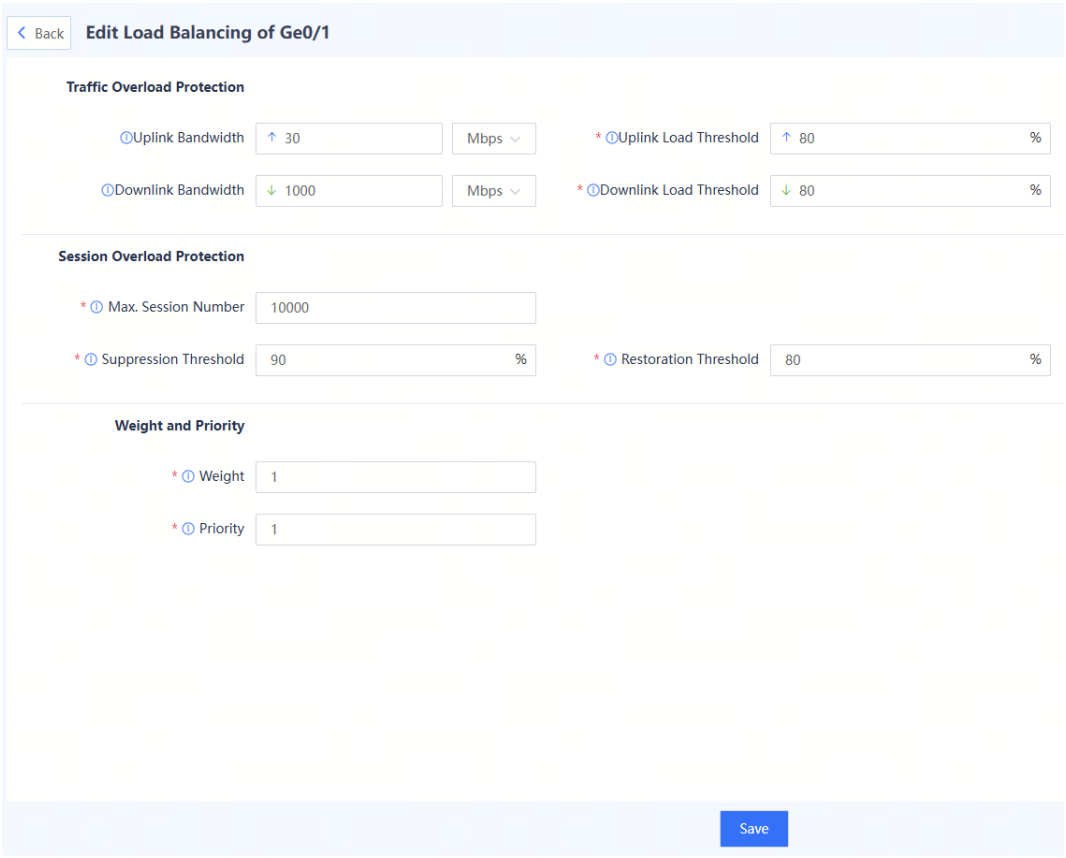
(3) (Optional) Click **Edit** in the **Operation** column to modify parameters of the interface.

Note

The Interface column displays only valid WAN interfaces that are powered on by default. To display other interfaces, select **All Interfaces in Routing Mode** from the drop-down list in the upper right corner.



a Modify the interface bandwidth, load threshold, and maximum number of sessions based on actual service requirements.



Item	Description	Remarks
Traffic Overload Protection		
Uplink/Downlink Bandwidth	Bandwidth values that the ISP provides for a link, including the upload bandwidth and download bandwidth.	Enter the bandwidth value and select the corresponding unit. [Example] 100 Mbps
Uplink/Downlink Load Threshold	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.	[Example] 80%
Session Overload Protection		

Item	Description	Remarks
Max. Session Number	This parameter refers to the maximum number of created connections. If the maximum number of sessions is exceeded, connections may fail to be set up. This parameter is used to calculate the session usage and affects policies such as egress load balancing.	[Example] 10000
Suppression Threshold	When the session usage of a link exceeds the suppression threshold, the link does not participate in traffic balancing.	Session usage = Real-time number of sessions/Maximum number of sessions [Example] 90%
Restoration Threshold	When the session usage of a link falls below the restoration threshold, the link participates in traffic load balancing again. The restoration threshold must be smaller than the suppression threshold.	[Example] 80%

Note

The **Weight** or **Priority** parameter takes effect only when the load balancing mode is set to **Based on Weight** and **Based on Priority** respectively, and is not involved in this scenario.

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

6.6.3 Configuring Load Balancing Based on the Source IP Address and Destination IP Address

Application Scenario

When load balancing based on the source IP address and destination IP address is enabled, packets with the same source IP address and destination 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. Different from source IP-based load balancing, in load balancing based on the source IP address and destination IP address, packets with different destination IP addresses may be sent by different interfaces, and traffic is more evenly distributed among outbound interfaces.

Prerequisites

- Multiple 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/Load Balancing** > **Egress Load Balancing** > **Global Config**.

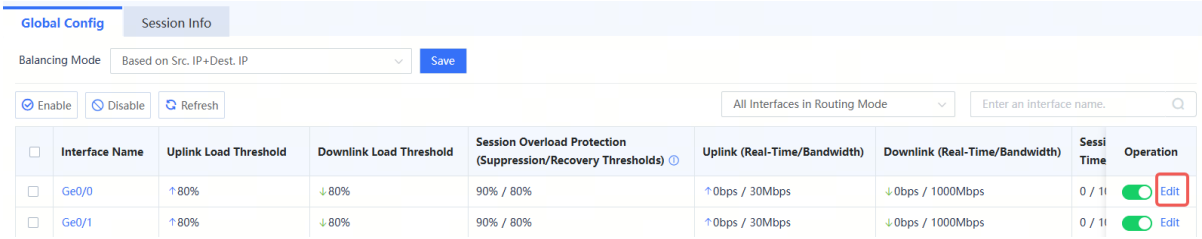
(2) Select **Based on Src. IP+Dest. IP** from the **Balancing Mode** drop-down list and click **Save**.



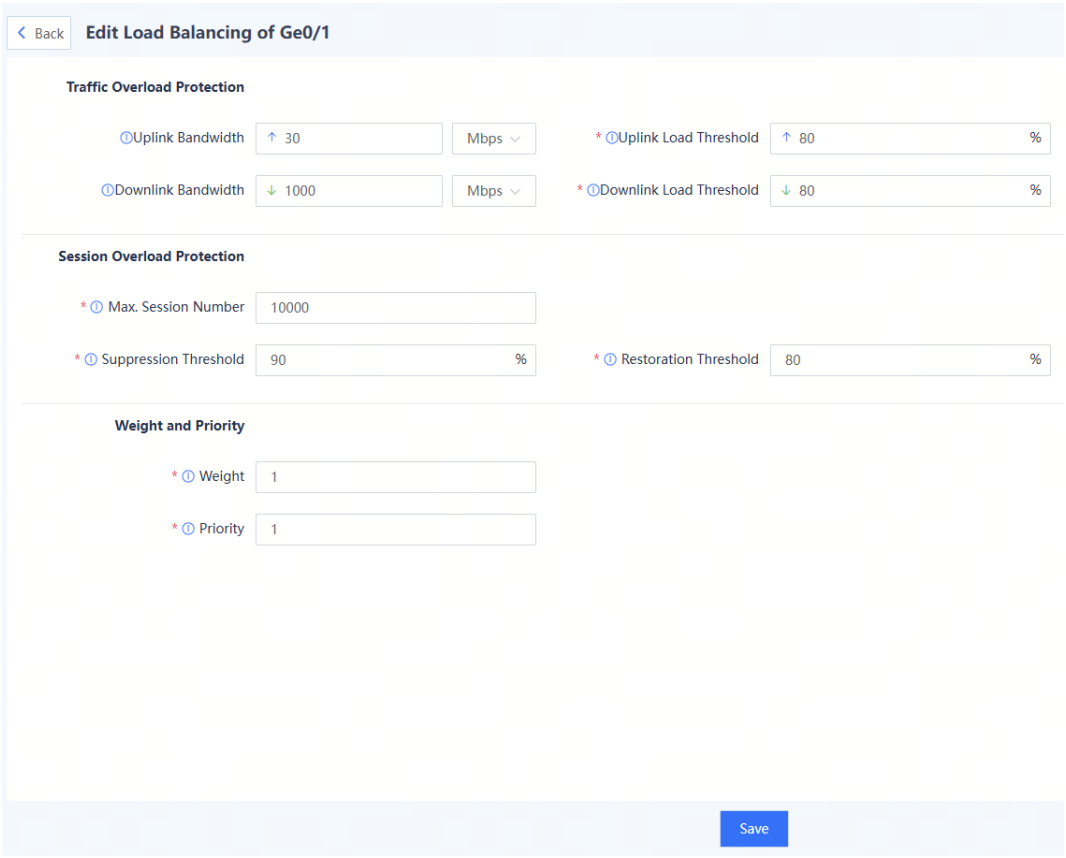
(3) (Optional) Click **Edit** in the **Operation** column to modify the parameters of the interface.

Note

The Interface column displays only valid WAN interfaces that are powered on by default. To display other interfaces, select **All Interfaces in Routing Mode** from the drop-down list in the upper right corner.



a Modify the interface bandwidth, load threshold, and maximum number of sessions based on actual service requirements.



Item	Description	Remarks
Traffic Overload Protection		
Uplink/Downlink Bandwidth	Bandwidth values that the ISP provides for a link, including the upload bandwidth and download bandwidth.	Enter the bandwidth value and select the corresponding unit. [Example] 100 Mbps
Uplink/Downlink Load Threshold	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.	[Example] 80%
Session Overload Protection		

Item	Description	Remarks
Max. Session Number	This parameter refers to the maximum number of created connections. If the maximum number of sessions is exceeded, connections may fail to be set up. This parameter is used to calculate the session usage and affects policies such as egress load balancing.	[Example] 10000
Suppression Threshold	When the session usage of a link exceeds the suppression threshold, the link does not participate in traffic balancing.	Session usage = Real-time number of sessions/Maximum number of sessions [Example] 90%
Restoration Threshold	When the session usage of a link falls below the restoration threshold, the link participates in traffic load balancing again. The restoration threshold must be smaller than the suppression threshold.	[Example] 80%

Note

The **Weight** or **Priority** parameter takes effect only when the load balancing mode is set to **Based on Weight** and **Based on Priority** respectively, and is not involved in this scenario.

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

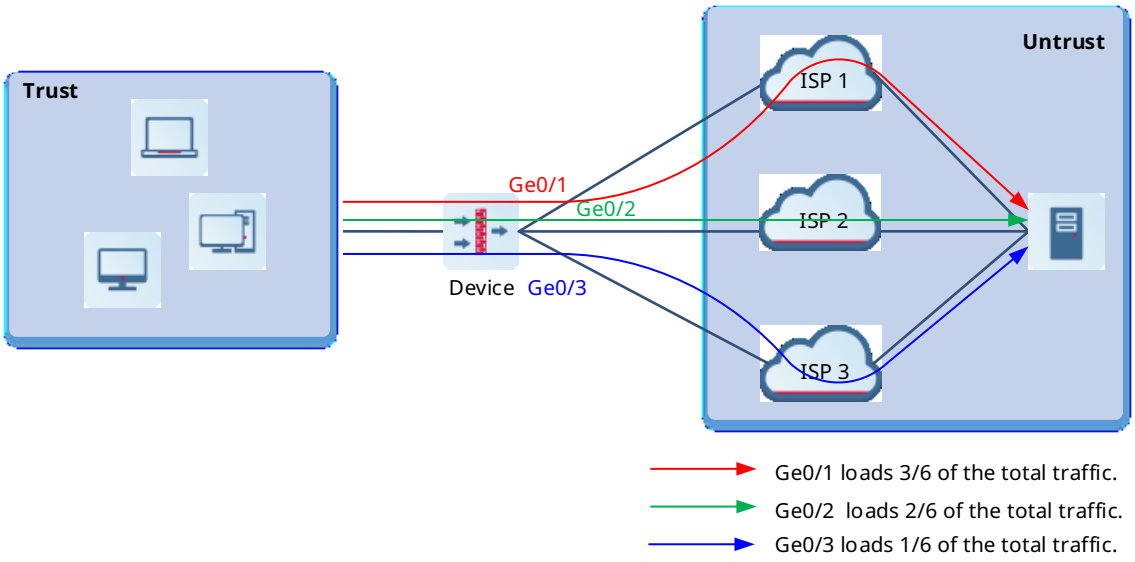
6.6.4 Configuring Load Balancing Based on Bandwidth

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%. The same session suppression thresholds (90%) are set for the three interfaces.

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

- Multiple 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

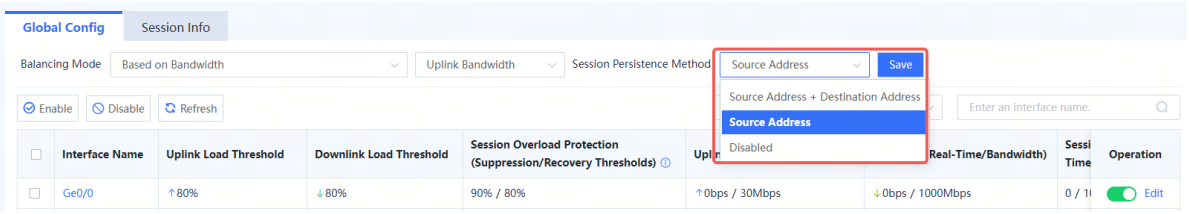
(1) Choose **Network** > **Routing/Load Balancing** > **Egress Load Balancing** > **Global Config**.

(2) Select **Based on Bandwidth** from the **Balancing Mode** drop-down list, and set the bandwidth metric to **Uplink Load, Downlink Load**, **Bidirectional**, **Uplink Bandwidth**, or **Downlink Bandwidth**. (The following uses **Uplink Bandwidth** as an example.) **Session Persistence Method** can be set to **Source Address + Destination Address**, **Source Address**, or **Disabled**. (The following uses **Source Address** as an example.) Click **Save**.

On the device, a caching scheme (that is, a session persistence method) can be configured. If network congestion occurs during traffic forwarding, the current load balancing policy for the line may need to be adjusted. For example, when Ge0/1 is overloaded, traffic originally loaded by Ge0/1 may need to be switched to Ge0/2. In such cases, the cache needs to be recorded in a short period to redirect subsequent traffic to Ge0/2. The following cache recording modes can be selected:

- **Source Address + Destination Address**: Cache is recorded by both source and destination addresses to ensure that subsequent traffic of the same combination of the source and destination addresses is not steered to the overloaded line (for example, Ge0/1), but is uniformly redirected to the new available line (for example, Ge0/2).
- **Source Address**: Cache is recorded by source address to ensure that subsequent traffic from the same source address is not steered to the overloaded line (for example, Ge0/1), but is uniformly redirected to the new available line (for example, Ge0/2).

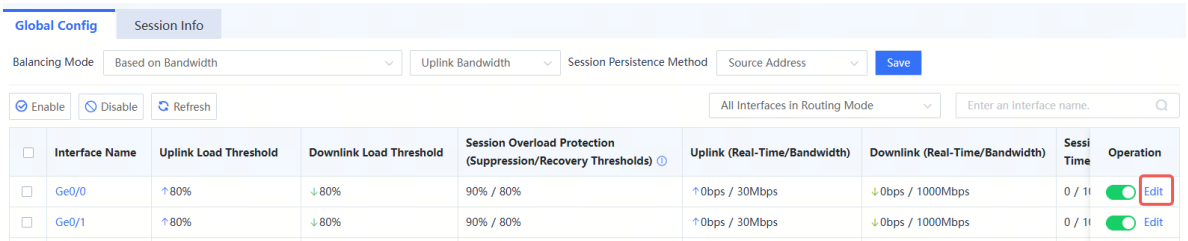
- **Disabled**: No cache recording (that is, session persistence is disabled). Traffic forwarding entirely depends on real-time load balancing. This mode applies to scenarios where session continuity is not required.



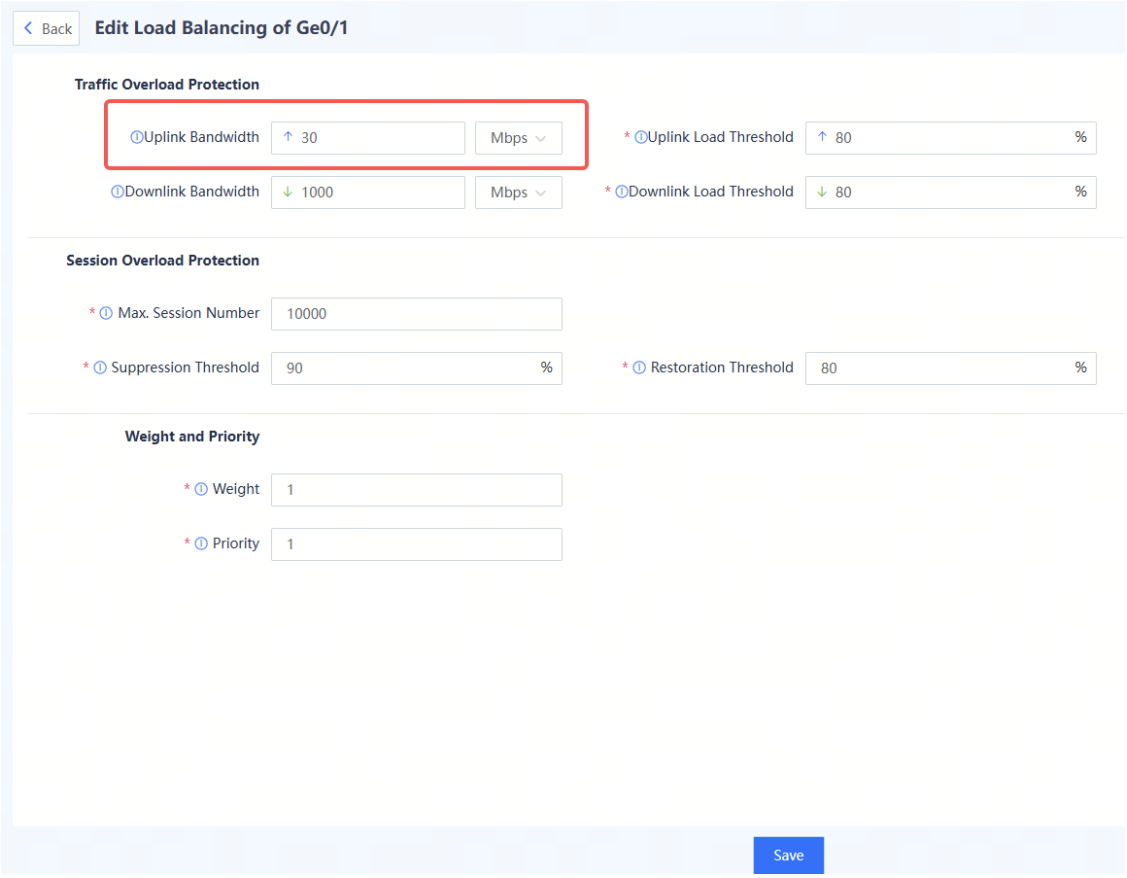
(3) Click **Edit** in the **Operation** column to modify the parameters of the interface.

Note

The Interface column displays only valid WAN interfaces that are powered on by default. To display other interfaces, select **All Interfaces in Routing Mode** from the drop-down list in the upper right corner.



a Modify the interface uplink bandwidth, load threshold, and maximum number of sessions based on actual service requirements.



Item	Description	Remarks
Traffic Overload Protection		
Uplink/Downlink Bandwidth	Bandwidth values that the ISP provides for a link, including the upload bandwidth and download bandwidth.	Enter the bandwidth value and select the corresponding unit. [Example] 100 Mbps
Uplink/Downlink Load Threshold	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.	[Example] 80%
Session Overload Protection		

Item	Description	Remarks
Max. Session Number	This parameter refers to the maximum number of created connections. If the maximum number of sessions is exceeded, connections may fail to be set up. This parameter is used to calculate the session usage and affects policies such as egress load balancing.	[Example] 10000
Suppression Threshold	When the session usage of a link exceeds the suppression threshold, the link does not participate in traffic balancing.	Session usage = Real-time number of sessions/Maximum number of sessions [Example] 90%
Restoration Threshold	When the session usage of a link falls below the restoration threshold, the link participates in traffic load balancing again. The restoration threshold must be smaller than the suppression threshold.	[Example] 80%

Note

The **Weight** or **Priority** parameter takes effect only when the load balancing mode is set to **Based on Weight** and **Based on Priority** respectively, and is not involved in this scenario.

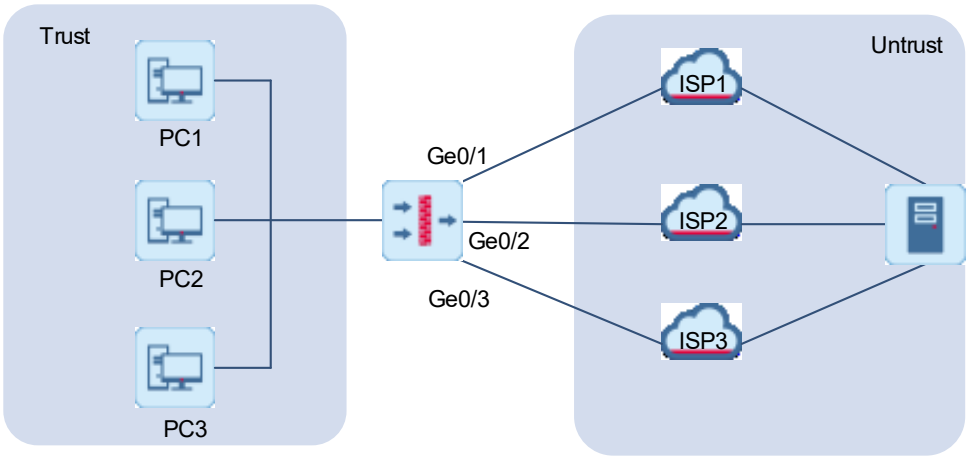
b After verifying the configuration, click **Save**.

6.6.5 Configuring Load Balancing Based on the Link Weight

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. The cost of the ISP1 link is low, and the weight is set to the highest value 5 for Ge0/1. The cost of the ISP2 link is high, and the weight is set to a lower value 2 for Ge0/2. The cost of the ISP3 link is the same as that of the ISP2 link, but the bandwidth is only half of that of the ISP2 link. Therefore, the weight is set to the lowest value 1 for Ge0/3. The load threshold and session suppression threshold of Ge0/1, Ge0/2, and Ge0/3 are all set to 80% and 90%, respectively.

When traffic of all interfaces does not reach the thresholds, the traffic is distributed on Ge0/1, Ge0/2, and Ge0/3 at a ratio of 5:2:1. When the traffic on Ge0/1 reaches its load threshold, Ge0/1 does not participate in load balancing of newly generated traffic, and subsequent traffic is distributed between Ge0/2 and Ge0/3 at a ratio of 2:1. When the traffic of all interfaces exceeds the thresholds, subsequent traffic is distributed among Ge0/1, Ge0/2, and Ge0/3 at a ratio of 5:2:1 again.



Prerequisites

- Multiple 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.

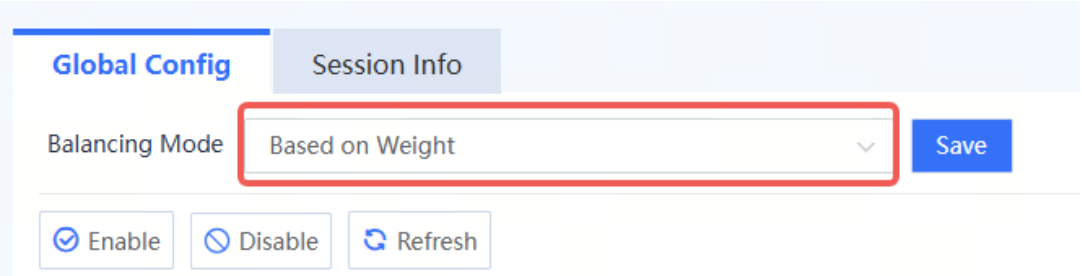
Precautions

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/Load Balancing** > **Egress Load Balancing** > **Global Config**.

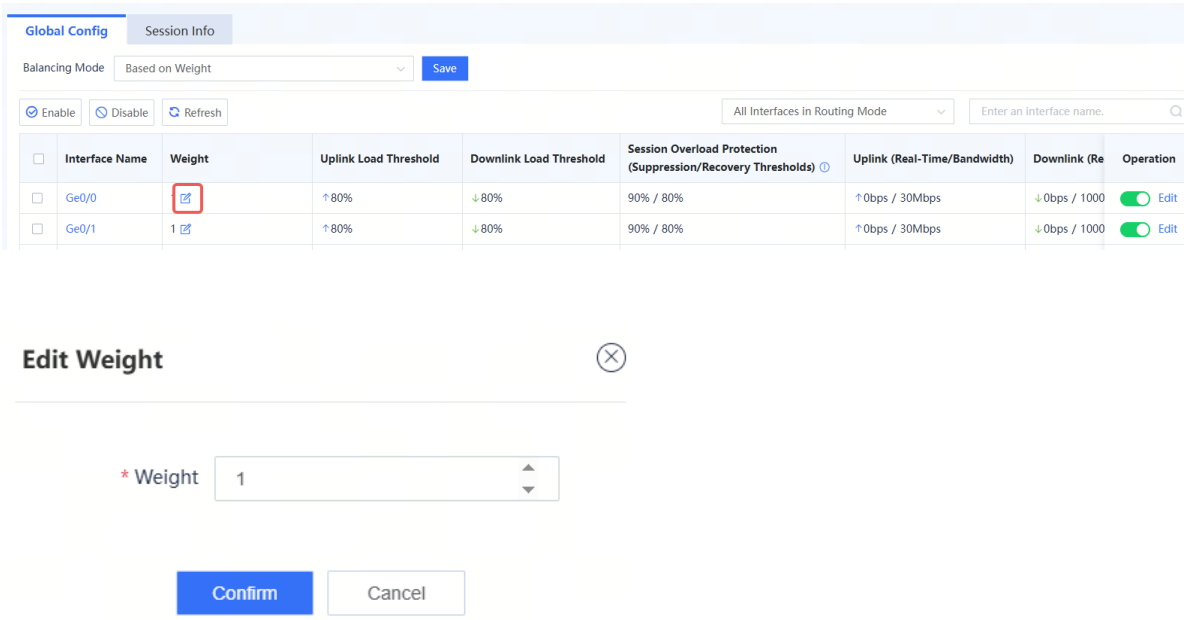
(2) Select **Based on Weight** from the **Balancing Mode** drop-down list and click **Save**.



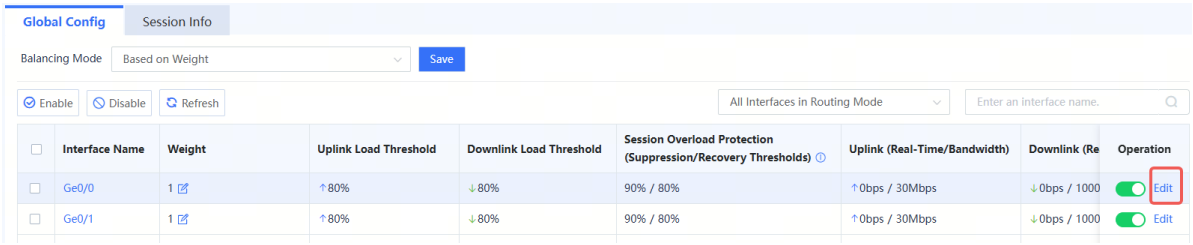
(3) Click the icon under **Weight** to modify the link weight.

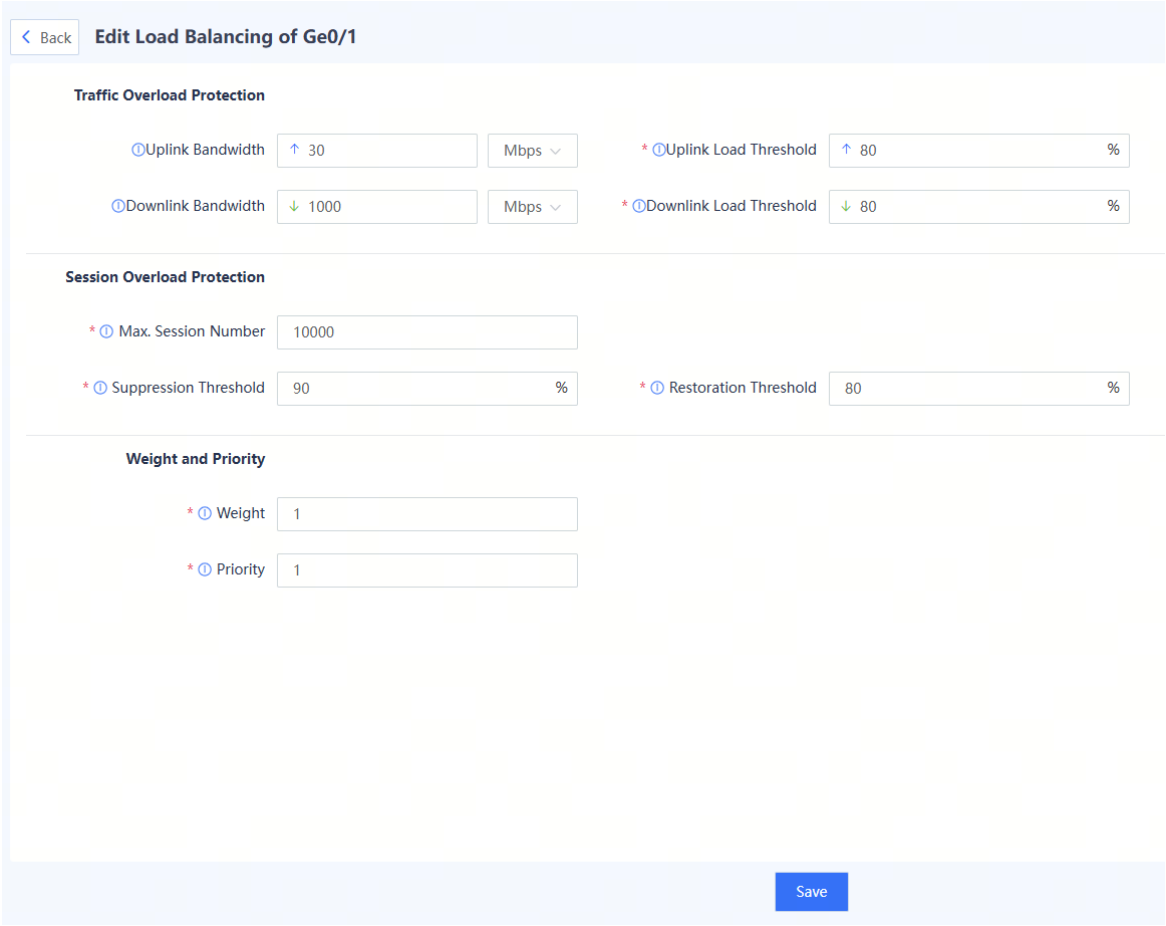
Note

The Interface column displays only valid WAN interfaces that are powered on by default. To display other interfaces, select **All Interfaces in Routing Mode** from the drop-down list in the upper right corner.



(4) (Optional) To modify other link parameters, click **Edit** in the **Operation** column.





Item	Description	Remarks
Traffic Overload Protection		
Uplink/Downlink Bandwidth	Bandwidth values that the ISP provides for a link, including the upload bandwidth and download bandwidth.	Enter the bandwidth value and select the corresponding unit. [Example] 100 Mbps
Uplink/Downlink Load Threshold	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.	[Example] 80%
Session Overload Protection		

Item	Description	Remarks
Max. Session Number	This parameter refers to the maximum number of created connections. If the maximum number of sessions is exceeded, connections may fail to be set up. This parameter is used to calculate the session usage and affects policies such as egress load balancing.	[Example] 10000
Suppression Threshold	When the session usage of a link exceeds the suppression threshold, the link does not participate in traffic balancing.	Session usage = Real-time number of sessions/Maximum number of sessions [Example] 90%
Restoration Threshold	When the session usage of a link falls below the restoration threshold, the link participates in traffic load balancing again. The restoration threshold must be smaller than the suppression threshold.	[Example] 80%

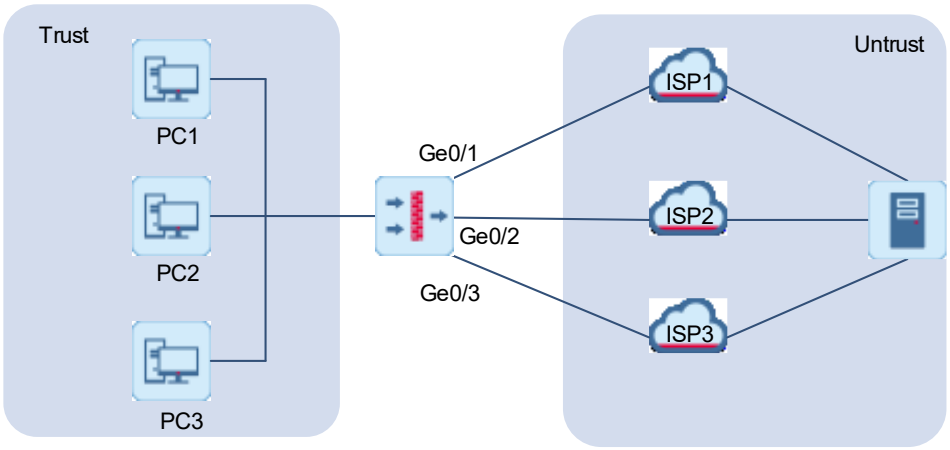
(5) After verifying the configuration, click **Save**.

6.6.6 Configuring Load Balancing Based on the Link Priority

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. The quality of the ISP1 link is high, and the highest priority is set for Ge0/1. The quality of the ISP2 link is lower, and a lower priority is set for Ge0/2. The quality of the ISP3 link is the lowest, and the lowest priority is set for Ge0/3. The load threshold and session suppression threshold of Ge0/1, Ge0/2, and Ge0/3 are all set to 80% and 90%, respectively.

When traffic does not reach the load threshold, all the traffic is preferentially distributed on Ge0/1. When the traffic exceeds the load threshold of Ge0/1, the traffic is load balanced on Ge0/2 and Ge0/1: Old traffic is distributed on Ge0/1, and newly generated traffic is distributed on Ge0/2. When the traffic exceeds the load thresholds of both Ge0/1 and Ge0/2, Ge0/3 also participates in load balancing: Old traffic is distributed on Ge0/1 and Ge0/2, and newly generated traffic is distributed on Ge0/3. When the traffic exceeds the load thresholds of all the three interfaces, newly generated traffic is preferentially distributed on the interface with a higher priority again.



Prerequisites

- Multiple 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.

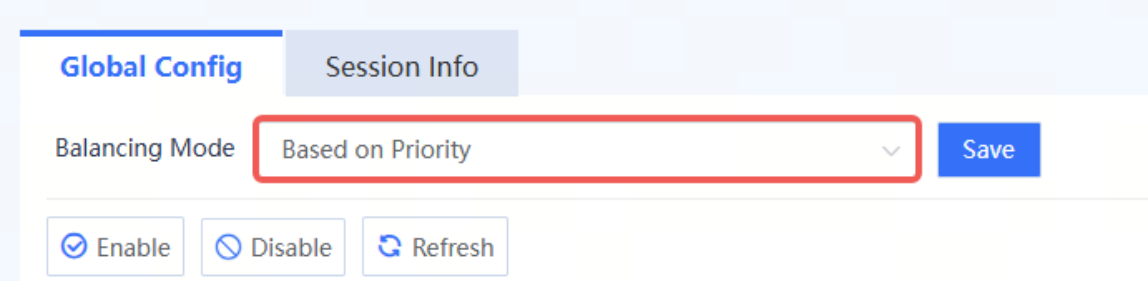
Precautions

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/Load Balancing** > **Egress Load Balancing** > **Global Config**.

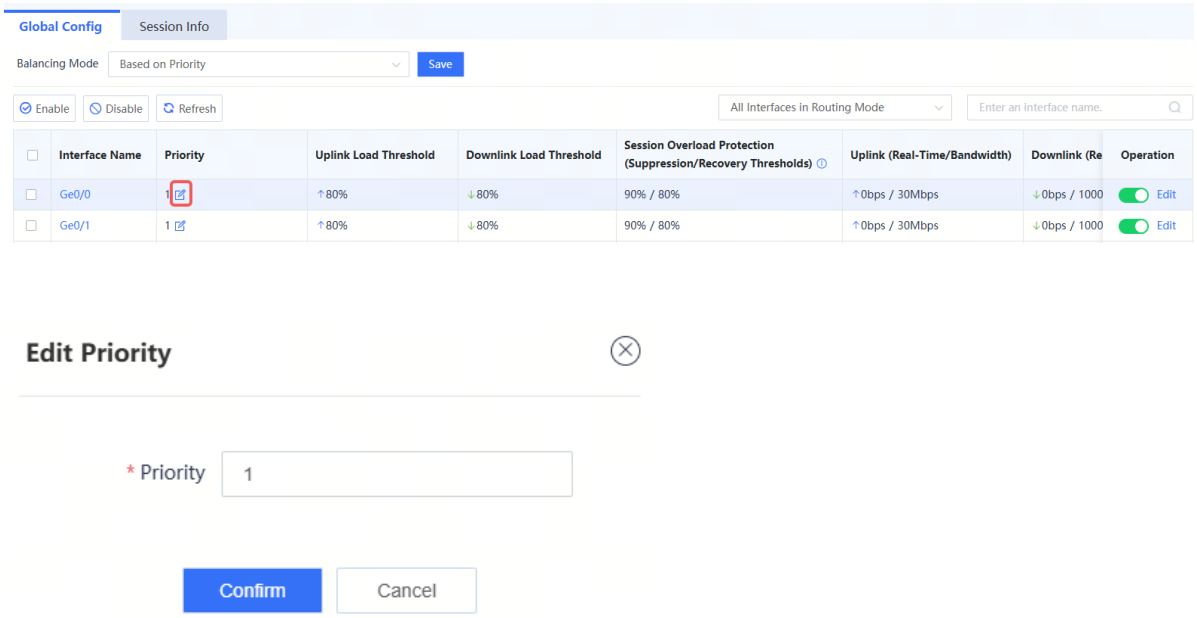
(2) Select **Based on Priority** from the **Balancing Mode** drop-down list and click **Save**.



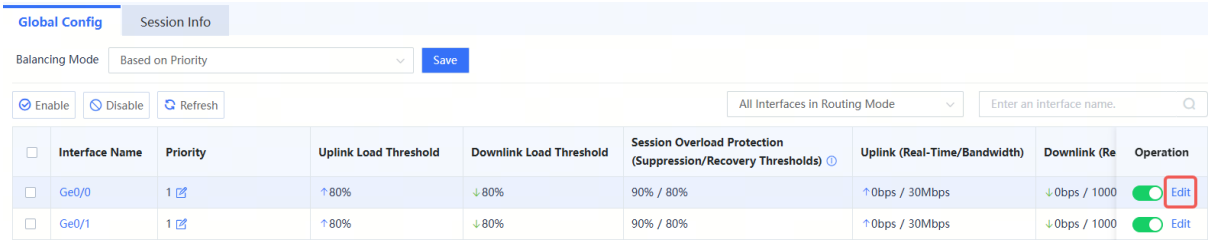
(3) Click the icon in the **Priority** column to modify the priority.

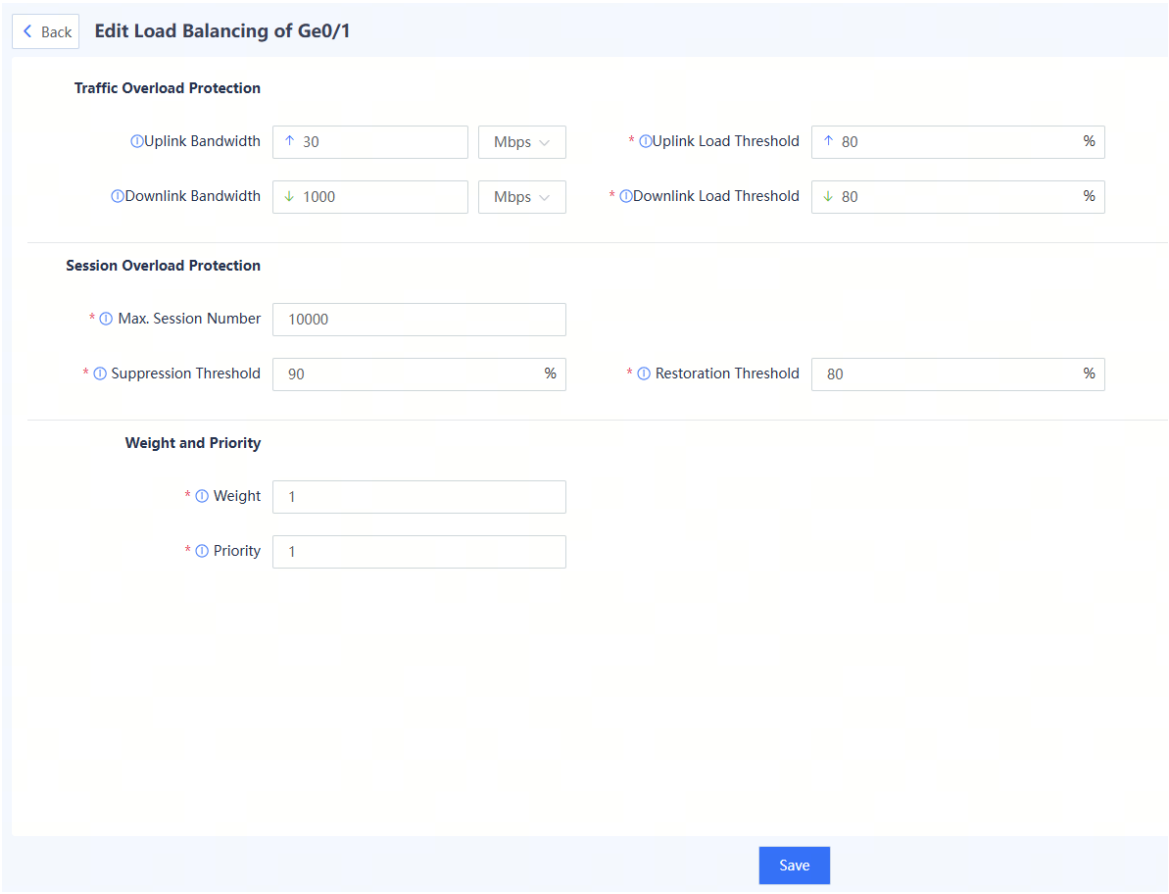
Note

The Interface column displays only valid WAN interfaces that are powered on by default. To display other interfaces, select **All Interfaces in Routing Mode** from the drop-down list in the upper right corner.



(4) (Optional) To modify other link parameters, click **Edit** in the **Operation** column.





Item	Description	Remarks
Traffic Overload Protection		
Uplink/Downlink Bandwidth	Bandwidth values that the ISP provides for a link, including the upload bandwidth and download bandwidth.	Enter the bandwidth value and select the corresponding unit. [Example] 100 Mbps
Uplink/Downlink Load Threshold	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.	[Example] 80%
Session Overload Protection		

Item	Description	Remarks
Max. Session Number	This parameter refers to the maximum number of created connections. If the maximum number of sessions is exceeded, connections may fail to be set up. This parameter is used to calculate the session usage and affects policies such as egress load balancing.	[Example] 10000
Suppression Threshold	When the session usage of a link exceeds the suppression threshold, the link does not participate in traffic balancing.	Session usage = Real-time number of sessions/Maximum number of sessions [Example] 90%
Restoration Threshold	When the session usage of a link falls below the restoration threshold, the link participates in traffic load balancing again. The restoration threshold must be smaller than the suppression threshold.	[Example] 80%

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

6.6.7 Configuring Load Balancing Based on the Number of Sessions

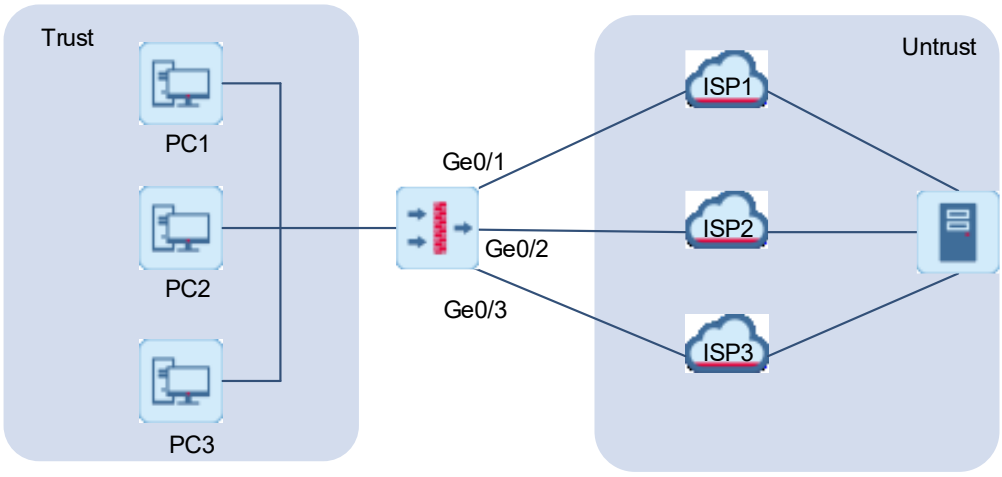
Application Scenario

As shown in the following figure, interfaces Ge0/1, Ge0/2, and Ge0/3 on the firewall are configured with the same routing rule. Ge0/1 supports a maximum of 3,000 sessions, Ge0/2 supports a maximum of 4,000 sessions, and Ge0/3 supports a maximum of 5,000 sessions. The session suppression threshold and session recovery threshold of Ge0/1, Ge0/2, and Ge0/3 are all set to 90% and 80%, respectively.

The maximum number of sessions supported by each link varies, and the lifetimes, creation time points, and connection loads of different sessions also vary. If newly generated traffic is always distributed on the link with the smallest number of sessions, the link with the smallest maximum number of sessions (Ge0/1 in this example) will be fully occupied within a short period. To distribute traffic among interfaces more evenly, enable load balancing based on the session. In this case, traffic is preferentially distributed on the link with the weighted smallest number of sessions, that is, the smallest ratio of the real-time session number to the configured maximum number of sessions.

Note

The maximum number of sessions indicates the maximum number of connections that can be established on a link. If the maximum number of sessions is exceeded, services may be interrupted. To obtain the specific value of the maximum number of sessions, contact the provider of the external network line, such as an ISP.



Prerequisites

- Multiple 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

Traffic that enters SSL VPN tunnels and IPsec VPN tunnels is not load balanced but forwarded through the specified tunnel interface.

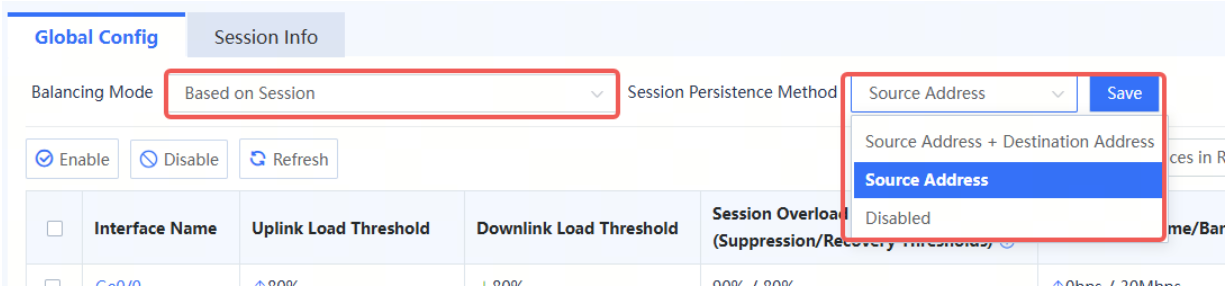
Procedure

(1) Choose **Network** > **Routing/Load Balancing** > **Egress Load Balancing** > **Global Config**.

(2) Select **Based on Session** from the **Balancing Mode** drop-down list. **Session Persistence Method** can be set to **Source Address + Destination Address**, **Source Address**, or **Disabled**. (The following uses **Source Address** as an example.) Click **Save**.

On the device, a caching scheme (that is, a session persistence method) can be configured. If network congestion occurs during traffic forwarding, the current load balancing policy for the line may need to be adjusted. For example, when Ge0/1 is overloaded, traffic originally loaded by Ge0/1 may need to be switched to Ge0/2. In such cases, the cache needs to be recorded in a short period to redirect subsequent traffic to Ge0/2. The following cache recording modes can be selected:

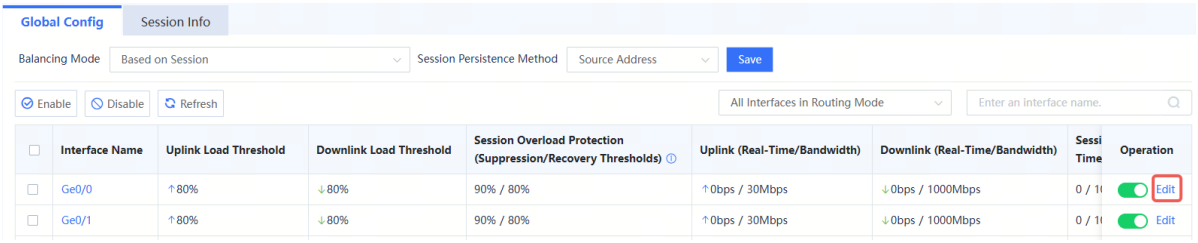
- **Source Address + Destination Address**: Cache is recorded by both source and destination addresses to ensure that subsequent traffic of the same combination of the source and destination addresses is not steered to the overloaded line (for example, Ge0/1), but is uniformly redirected to the new available line (for example, Ge0/2).
- **Source Address**: Cache is recorded by source address to ensure that subsequent traffic from the same source address is not steered to the overloaded line (for example, Ge0/1), but is uniformly redirected to the new available line (for example, Ge0/2).
- **Disabled**: No cache recording (that is, session persistence is disabled). Traffic forwarding entirely depends on real-time load balancing. This mode applies to scenarios where session continuity is not required.



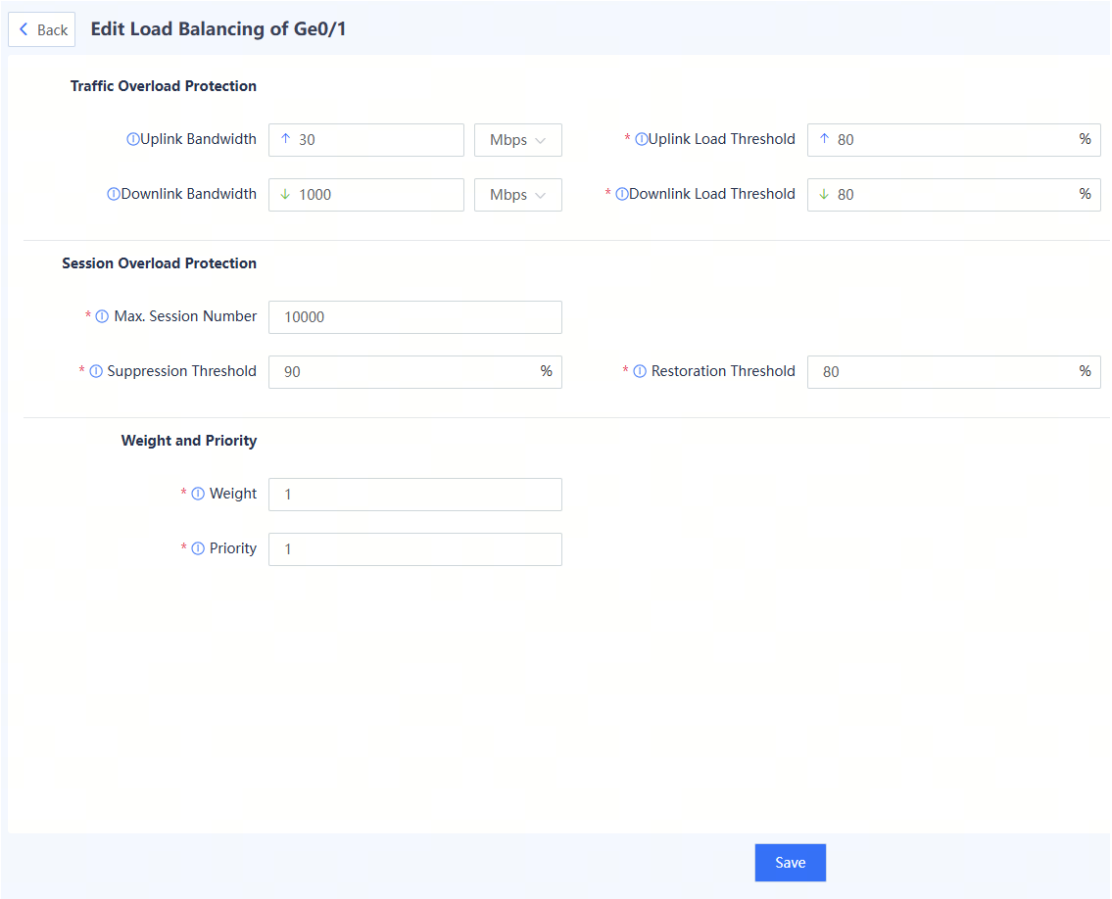
(3) (Optional) Click **Edit** in the **Operation** column to modify the maximum number of sessions, load thresholds, and other parameters of the interface.

Note

The Interface column displays only valid WAN interfaces that are powered on by default. To display other interfaces, select **All Interfaces in Routing Mode** from the drop-down list in the upper right corner.



a Modify the interface bandwidth, load threshold, and maximum number of sessions based on actual service requirements.



Item	Description	Remarks
Traffic Overload Protection		
Uplink/Downlink Bandwidth	Bandwidth values that the ISP provides for a link, including the upload bandwidth and download bandwidth.	Enter the bandwidth value and select the corresponding unit. [Example] 100 Mbps
Uplink/Downlink Load Threshold	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.	[Example] 80%
Session Overload Protection		

Item	Description	Remarks
Max. Session Number	This parameter refers to the maximum number of created connections. If the maximum number of sessions is exceeded, connections may fail to be set up. This parameter is used to calculate the session usage and affects policies such as egress load balancing.	[Example] 10000
Suppression Threshold	When the session usage of a link exceeds the suppression threshold, the link does not participate in traffic balancing.	Session usage = Real-time number of sessions/Maximum number of sessions [Example] 90%
Restoration Threshold	When the session usage of a link falls below the restoration threshold, the link participates in traffic load balancing again. The restoration threshold must be smaller than the suppression threshold.	[Example] 80%

Note

The **Weight** or **Priority** parameter takes effect only when the load balancing mode is set to **Based on Weight** and **Based on Priority** respectively, and is not involved in this scenario.

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

6.6.8 Configuring Load Balancing Based on Bandwidth and Sessions

Application Scenario

For load balancing based on the bandwidth and session, new traffic will be forwarded over the link with the lowest session usage and bandwidth usage. When the session usage or bandwidth usage of a link exceeds the threshold, the link will no longer carry traffic. This load balancing mode can fully utilize the advantages of different lines and solve the problem of poor Internet access experience of users. It is applicable to scenarios where multiple broadband lines or home broadband and private lines coexist. When the number of sessions on home broadband lines has reached the upper limit and the private line bandwidth is still sufficient, permit Internet access traffic of home users to pass through the private line to ensure the user's Internet access experience. When the private line bandwidth is fully occupied, permit key services to be carried over the home broadband line to preferentially guarantee core services and make full use of bandwidth resources.

Prerequisites

- Multiple 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

Traffic that enters SSL VPN tunnels and IPsec VPN tunnels is not load balanced but forwarded through the specified tunnel interface.

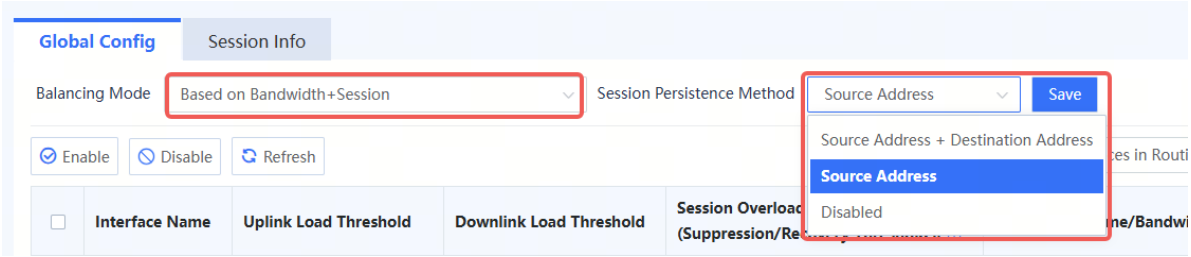
Procedure

(1) Choose **Network** > **Routing/Load Balancing** > **Egress Load Balancing** > **Global Config**.

(2) Select **Based on Bandwidth+Session** from the **Balancing Mode** drop-down list. **Session Persistence Method** can be set to **Source Address + Destination Address**, **Source Address**, or **Disabled**. (The following uses **Source Address** as an example.) Click **Save**.

On the device, a caching scheme (that is, a session persistence method) can be configured. If network congestion occurs during traffic forwarding, the current load balancing policy for the line may need to be adjusted. For example, when Ge0/1 is overloaded, traffic originally loaded by Ge0/1 may need to be switched to Ge0/2. In such cases, the cache needs to be recorded in a short period to redirect subsequent traffic to Ge0/2. The following cache recording modes can be selected:

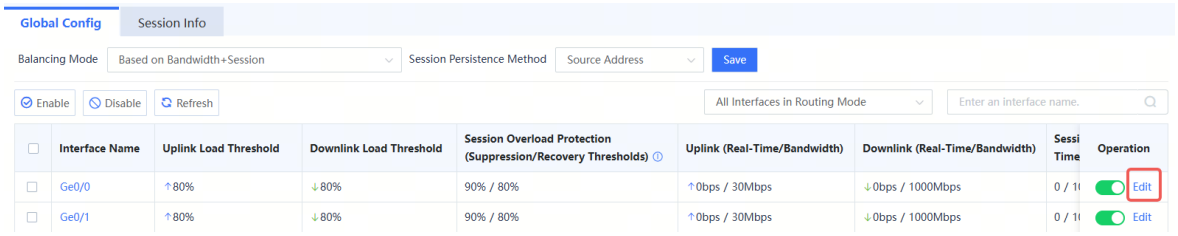
- **Source Address + Destination Address**: Cache is recorded by both source and destination addresses to ensure that subsequent traffic of the same combination of the source and destination addresses is not steered to the overloaded line (for example, Ge0/1), but is uniformly redirected to the new available line (for example, Ge0/2).
- **Source Address**: Cache is recorded by source address to ensure that subsequent traffic from the same source address is not steered to the overloaded line (for example, Ge0/1), but is uniformly redirected to the new available line (for example, Ge0/2).
- **Disabled**: No cache recording (that is, session persistence is disabled). Traffic forwarding entirely depends on real-time load balancing. This mode applies to scenarios where session continuity is not required.



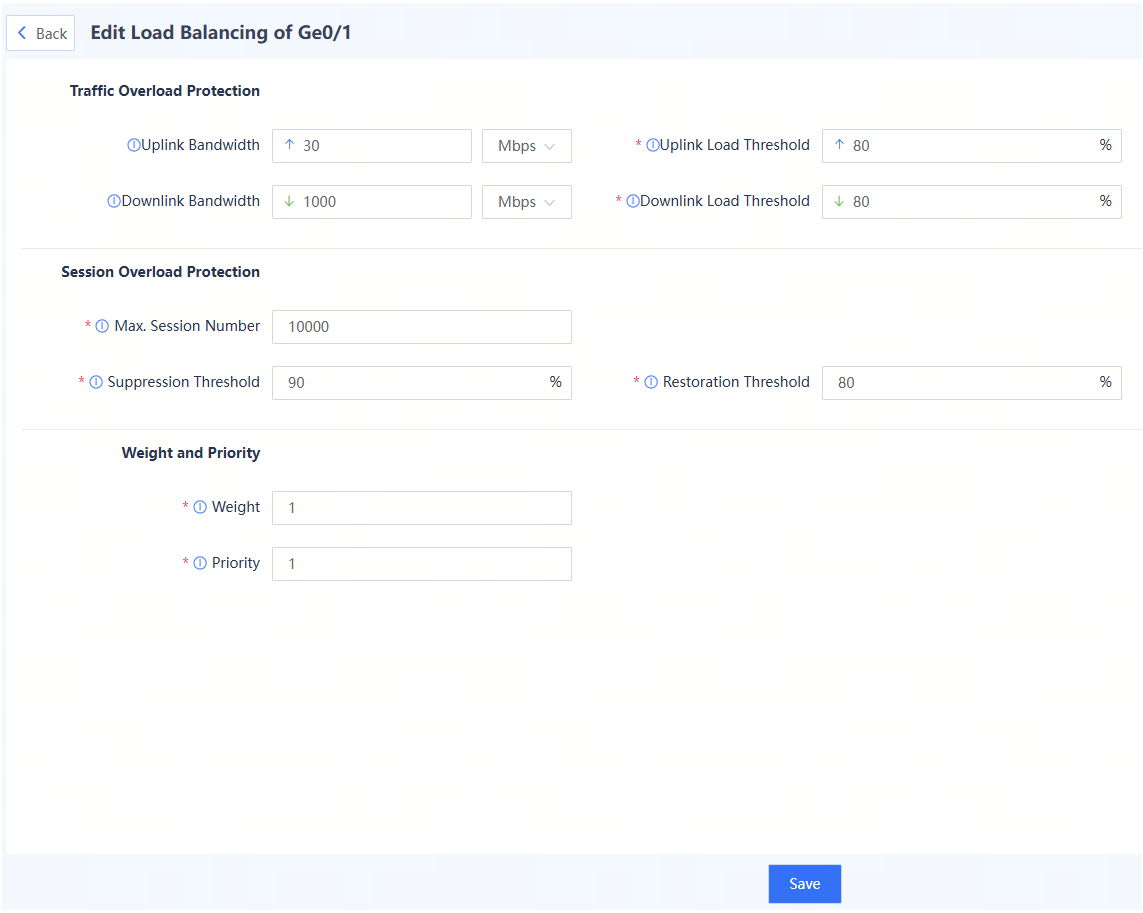
(3) (Optional) Click **Edit** in the **Operation** column to modify the maximum number of sessions, load thresholds, and other parameters of the interface.

Note

The Interface column displays only valid WAN interfaces that are powered on by default. To display other interfaces, select **All Interfaces in Routing Mode** from the drop-down list in the upper right corner.



a Modify the interface bandwidth, load threshold, and maximum number of sessions based on actual service requirements.



Item	Description	Remarks
Traffic Overload Protection		
Uplink/Downlink Bandwidth	Bandwidth values that the ISP provides for a link, including the upload bandwidth and download bandwidth.	Enter the bandwidth value and select the corresponding unit. [Example] 100 Mbps

Item	Description	Remarks
Uplink/Downlink Load Threshold	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.	[Example] 80%
Session Overload Protection		
Max. Session Number	This parameter refers to the maximum number of created connections. If the maximum number of sessions is exceeded, connections may fail to be set up. This parameter is used to calculate the session usage and affects policies such as egress load balancing.	[Example] 10000
Suppression Threshold	When the session usage of a link exceeds the suppression threshold, the link does not participate in traffic balancing.	Session usage = Real-time number of sessions/Maximum number of sessions [Example] 90%
Restoration Threshold	When the session usage of a link falls below the restoration threshold, the link participates in traffic load balancing again. The restoration threshold must be smaller than the suppression threshold.	[Example] 80%

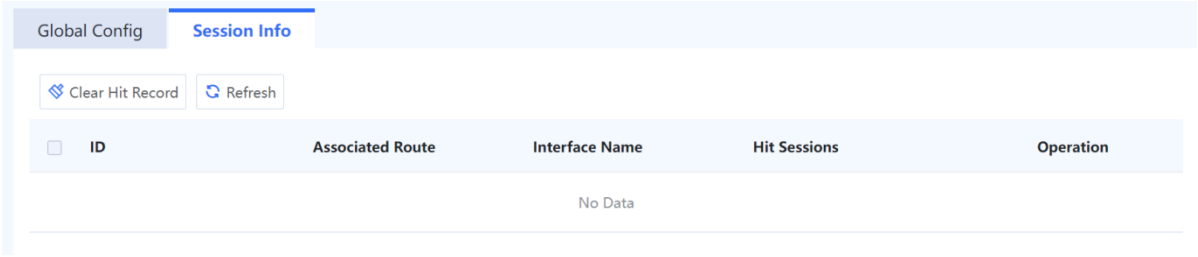
b After verifying the configuration, click **Save**.

6.6.9 Viewing Load Balancing Session Information

Procedure

(1) Choose **Network** > **Routing/Load Balancing** > **Egress Load Balancing** > **Session Info**.

(2) On the tab page, information about the sessions involved in load balancing is displayed.



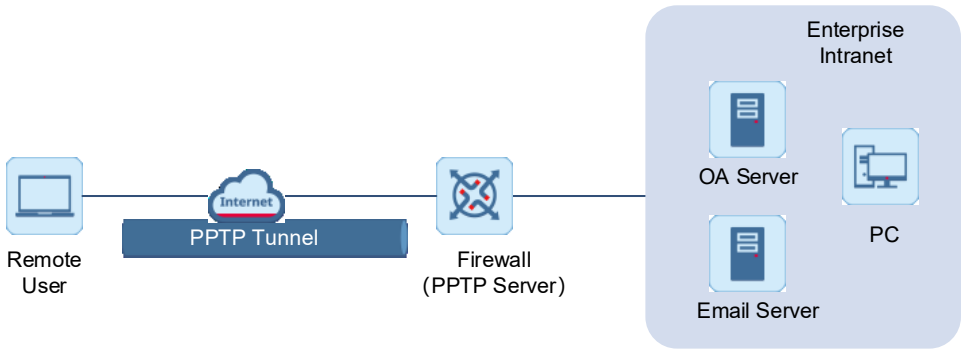
6.7 PPTP VPN

6.7.1 Overview

Point-to-Point Tunneling Protocol (PPTP) is a network tunneling protocol extended based on the Point-to-Point Protocol (PPP), and is also one of the implementation technologies of the virtual private network (VPN). A PPTP VPN establishes encrypted communication tunnels on the public network (such as the Internet) to connect remote clients to private networks, implementing cross-network data transmission. In scenarios such as mobile office and remote office, external users and employees can securely access internal resources of an enterprise through the PPTP VPN tunnel.

The device can serve as a PPTP server to accept PPTP connection requests initiated by remote clients and negotiate to establish VPN tunnels, so remote users can securely access intranet resources. This ensures security and privacy of data transmission.

Figure 6-8 PPTP VPN Networking



6.7.2 Configuring the PPTP Server

Application Scenario

When the PPTP function is enabled on the device, the device can function as the PPTP VPN server to provide PPTP tunnel access service for remote users so that the users can remotely access internal networks and internal resources.

Precautions

- When the PPTP server function is configured on the device, the PPTP client can connect to the VPN server through the external interface IP address (public network IP address) of the device.
- Disabling, deleting, or modifying the PPTP configuration may cause online users to be forcibly disconnected. Therefore, exercise caution when performing these operations.

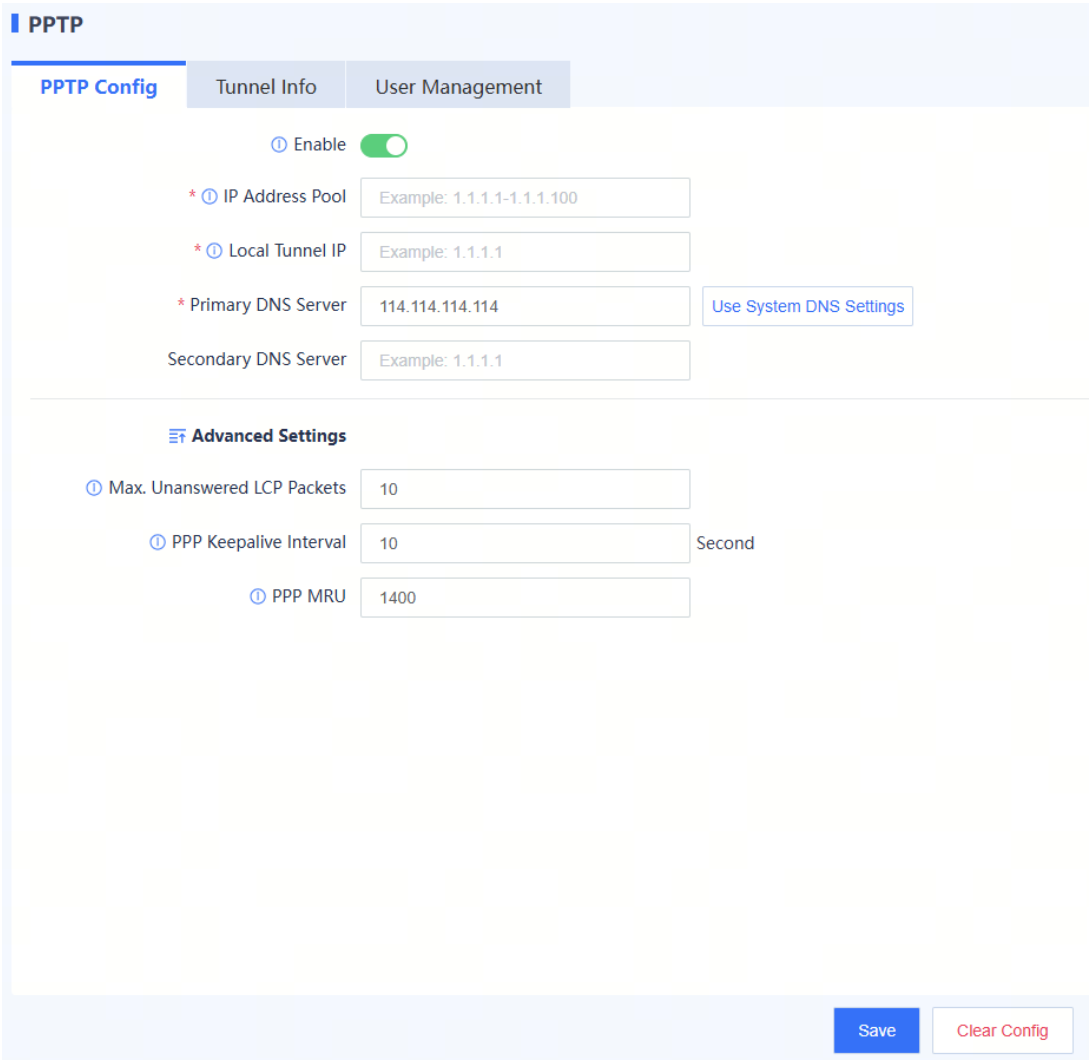
Prerequisites

- Before enabling the PPTP server function, create a VPN user and configure at least one login VPN user account by choosing **Network** > **VPN Mgmt** > **PPTP** > **User Management**. For details, see 6.7.4 Performing PPTP VPN Client Management.

Procedure

(1) Choose **Network** > **VPN Mgmt** > **PPTP** > **PPTP Config**.

(2) Configure PPTP server parameters.



Item	Description	Remarks
Enable	Whether the PPTP server function is enabled globally.	By default, this function is disabled. [Example] Enabled

Item	Description	Remarks
IP Address Pool	Range of IP addresses allocated to PPTP clients.	Enter the IP address range. Use the hyhen (-) to separate the start IP address and end IP address. Format: start IP address-end IP address. [Example] 10.20.1.1-10.20.1.254
Local Tunnel IP	IP address used by the device (PPTP server) to transmit data with the PPTP client after a VPN tunnel is established successfully.	● By default, the first IP address in an IP address pool is used as the local tunnel address of the server. ● The IP address must be in the same range as the IP address pool. [Example] 10.20.1.1
Primary DNS Server	Primary DNS server address allocated to a PPTP client.	Click **Use System DNS Settings**. The DNS server configuration of the device is automatically entered. [Example] 114.114.114.114
Secondary DNS Server	Secondary DNS server address allocated to a PPTP client.	[Example] 8.8.8.8
Advanced Settings Configure keepalive parameters for PPTP connections. If the PPTP server fails to receive any response from the client within the timeout interval, the PPTP server automatically closes the PPTP session. PPTP connection timeout interval = Max. Unanswered LCP Packets x PPP Keepalive Interval		
Max. Unanswered LCP Packets	The number of unanswered LCP packets increases by 1 if the PPTP server fails to receive any response packet from the client after sending the LCP packets. When the number of consecutive unanswered LCP packets exceeds the specified maximum value, the PPTP server automatically disconnects	The default value is 10. That is, when a device does not receive any response from the client after sending LCP packets 10 consecutive times, the device automatically disconnects the VPN connection. [Example] 10

Item	Description	Remarks
PPP Keepalive Interval	Interval at which a device sends PPP link maintenance detection packets (LCP Echo-Request packets). After a PPTP tunnel is established, the device periodically transmits LCP Echo-Request packets to detect the PPP link state and ensure normal operation of the PPTP tunnel.	The default value is 10s. That is, the device sends LCP Echo-Request packets to the remote end of the tunnel at an interval of 10s. [Example] 10s
PPP MRU	The PPP maximum receive unit (MRU) is used to limit the maximum PPP frame length (in bytes) of the local device (PPTP server) to prevent packet loss or performance deterioration caused by large-sized frames.	[Example] 1400

(3) Click **Save**. A message is displayed, asking you whether to create a security policy. Click **Create**. The device automatically generates a security policy with the source address set to the IP address pool name and name set to **pptp-server0**. The policy is used to permit traffic from the PPTP client to the local device (PPTP server) that accesses IP addresses in the address pool.

Note

If a PPTP client uses an IP address not in the address pool (namely, the source IP address of the client) to access the device (PPTP server), you need to manually add a security policy.

Follow-up Procedure

- Click **Clear Config** to clear the current PPTP server configuration and restore the device to the unconfigured state. The automatically created security policy **pptp-server0** will also be deleted.
- Enter the public IP address, username, and password of the device on the PPTP client to initiate a PPTP dial-up connection with the PPTP server.

6.7.3 Viewing PPTP Tunnel Information

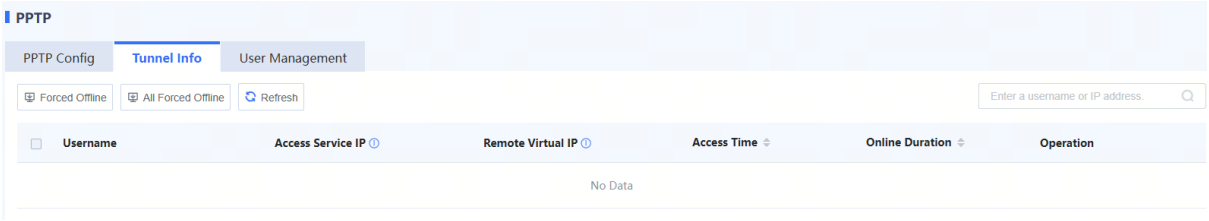
Application Scenario

After PPTP clients successfully access the PPTP server and establish PPTP tunnels, the administrator can view details about online PPTP users and forcibly disconnect PPTP users.

Procedure

(1) Choose **Network** > **VPN Mgmt** > **PPTP** > **Tunnel Info**.

(2) The **Tunnel Info** page displays information about all online PPTP users.



(3) Click Forced Offline to forcibly disconnect corresponding users.

To disconnect multiple users, select multiple records and click **Forced Offline**.

To disconnect all users, click **All Forced Offline**.

6.7.4 Performing PPTP VPN Client Management

Application Scenario

Configure a PPTP VPN user account as the access voucher for the PPTP VPN client. When a client requests to access the VPN server, it needs to provide a valid identity voucher (such as the username and password) for authentication. Only authenticated clients are allowed to access the internal network and internal resources. Proper configuration and management of VPN users can guarantee internal network security and prevent unauthorized access.

Procedure

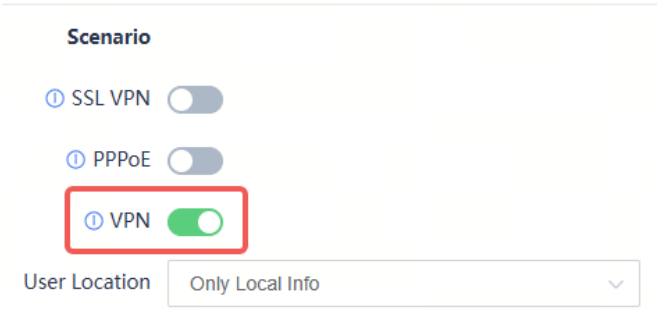
(1) Choose **Network** > **VPN Mgmt** > **PPTP** > **User Management**.

(2) (Optional) Configure the authentication domain for the PPTP VPN server.

The PPTP VPN server uses the authentication domain **vpn** by default, that is, it authenticates PPTP VPN clients based on user information in the authentication domain **vpn**. To change the authentication domain used by the PPTP VPN server, click **Switch authentication domain**.

Caution

- Toggle **VPN** on in **Scenario** for the authentication domain used by the PPTP VPN server. Otherwise, VPN users cannot log in to the VPN.

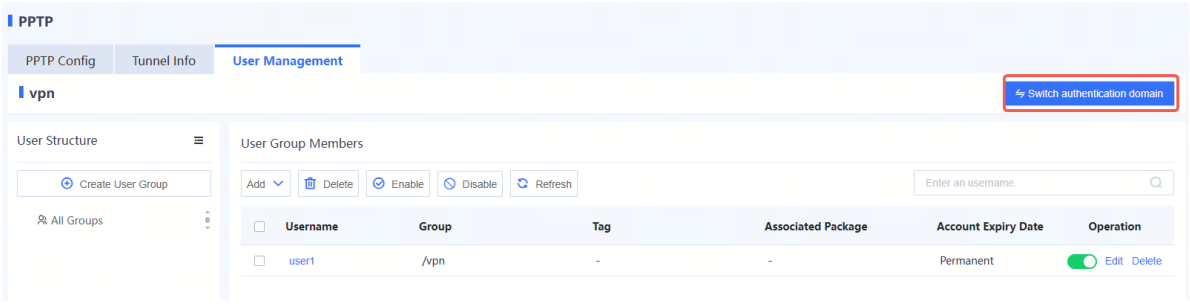


- Modifying the PPTP authentication domain will cause all online users to go offline. Exercise caution when performing this operation.

Note

- By default, the authentication domain named **vpn** uses only local user information for VPN access authentication, that is, VPN user information needs to be configured and managed on the local device. If an external server is used to manage VPN user accounts, you can modify the authentication domain configuration, use server user information and configure authentication server information.

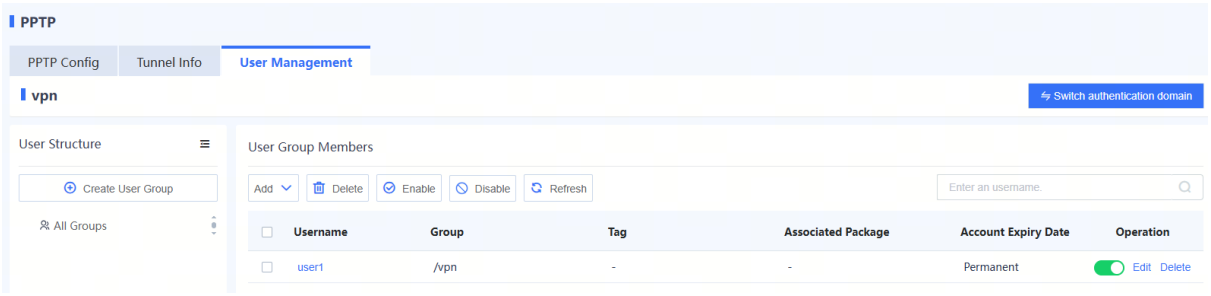
- To add an authentication domain or modify the authentication domain configuration, choose **Object** > **User Authentication** > **Authentication Domain**. For more information about authentication domains, see 5.8.7 Authentication Domain Management.



(3) Configure VPN users.

The overall operation logic of the VPN client management page is similar to that of the authenticated client management page. You can configure user groups, add single users, batch add users, and export user information. For details about user management operations, see 5.8.2 User Management.

Follow-up Procedure



- Click **Edit** in the **Operation** to modify user information.
- Toggle on the switch to enable or disable the user account.
- Select multiple users and click **Delete** to delete user information in a batch. Then authenticated users go offline and cannot pass authentication again.
- Select multiple users and click **Disable** to disable the user. Authenticated users will go offline and cannot pass authentication again.
- Select multiple users and click **Enable** to enable multiple users in a batch.

6.8 L2TP VPN

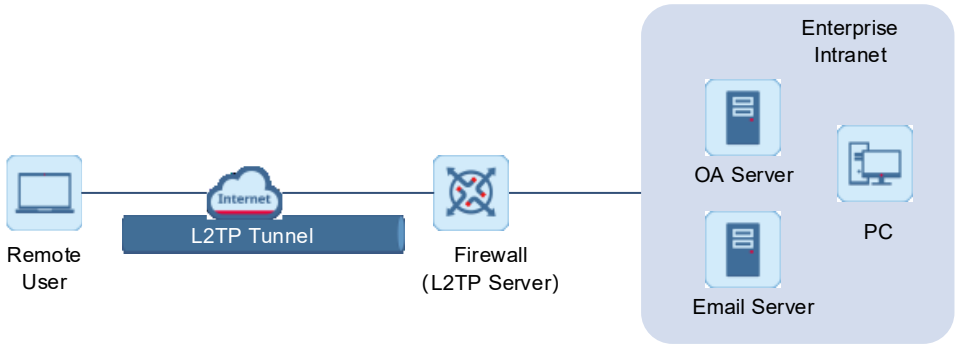
6.8.1 Overview

Layer 2 Tunneling Protocol (L2TP) is a network tunneling protocol developed by integrating and extending PPTP and Layer 2 Forwarding (L2F), and is also one of the implementation technologies of the VPN. L2TP VPN establishes a communication tunnel on the public network (such as the Internet) to connect a remote terminal to a private network, implementing cross-network data transmission. In scenarios such as mobile office and remote office, L2TP VPN can be used with IPsec to implement data encryption and authentication, allowing

external users and employees to securely access internal resources of enterprises through L2TP over IPsec tunnels.

The device can serve as an L2TP server to accept L2TP connection requests initiated by remote clients and negotiate to establish VPN tunnels, so remote users can securely access intranet resources. This ensures security and privacy of data transmission.

Figure 6-9 L2TP VPN Networking



6.8.2 Configuring the L2TP Server

Application Scenario

When L2TP is enabled on the device, the device can function as an L2TP VPN server to provide L2TP tunnel access for remote users so that the users can remotely access internal networks and resources.

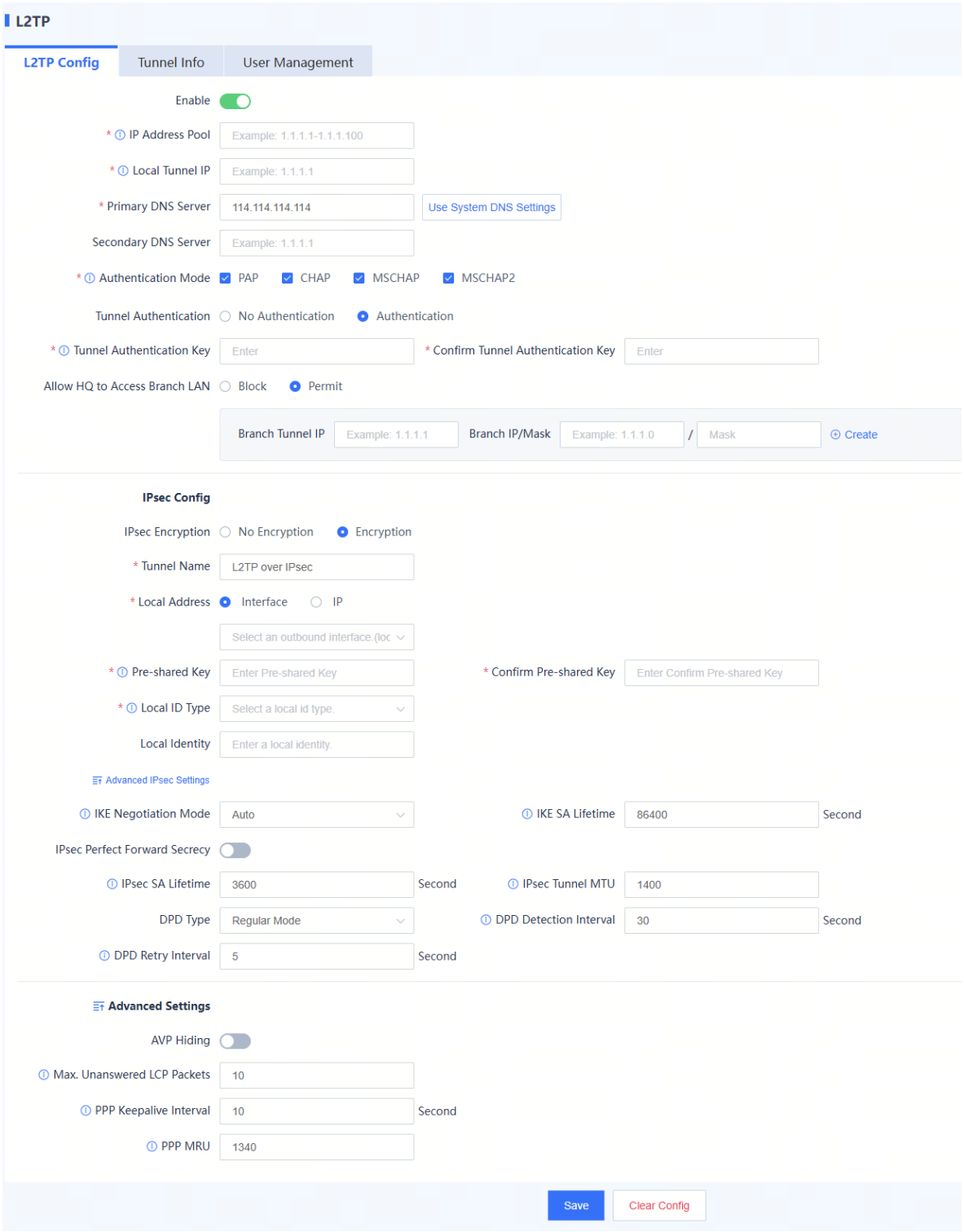
Precautions

- When the L2TP server function is configured on the device, the L2TP client can connect to the VPN server through the the external interface IP address (public network IP address) of the device.
- Disabling, deleting, or modifying the L2TP configuration may cause online users to be forcibly disconnected. Therefore, exercise caution when performing these operations.

Procedure

(1) Choose **Network** > **VPN Mgmt** > **L2TP** > **L2TP Config**.

(2) Configure L2TP server parameters.



Item	Description	Remarks
Enable	Whether the L2TP server function is enabled globally.	By default, this function is disabled. [Example] Enabled

Item	Description	Remarks
IP Address Pool	Range of IP addresses allocated to L2TP clients.	Enter the IP address range. Use the hyhen (-) to separate the start IP address and end IP address. Format: start IP address-end IP address. [Example] 10.20.1.1-10.20.1.254
Local Tunnel IP	IP address used by the device (L2TP server) to transmit data with the L2TP client after a VPN tunnel is established successfully.	• By default, the first IP address in an IP address pool is used as the local tunnel address of the server. • IP addresses in the same range as the IP address pool need to be configured. [Example] 10.20.1.1
Primary DNS Server	Primary DNS server address allocated to an L2TP client.	Click **Use System DNS Settings**. The DNS server configuration of the device is automatically entered. [Example] 114.114.114.114
Secondary DNS Server	Secondary DNS server address allocated to an L2TP client.	[Example] 8.8.8.8
Authentication Mode	Mode for authenticating an L2TP client. The options are **PAP**, **CHAP**, **MSCHAP**, and **MSCHAP2**.	• Multiple authentication modes can be selected. • The authentication mode of the L2TP client must be the same as that of the L2TP server. To be compatible with different types of clients, you are advised to enable multiple authentication modes.
Tunnel Authentication	Whether L2TP tunnel authentication is enabled.	[Example] Authentication
Tunnel Authentication Key/Confirm Tunnel Authentication Key	If tunnel authentication is enabled, you need to configure the L2TP tunnel authentication key. A tunnel connection can be established only when the authentication key of the L2TP client is the same as that of the server.	The same tunnel authentication key must be configured at both ends of an L2TP tunnel. [Example] Ruijie123

Item	Description	Remarks
Allow HQ to Access Branch LAN	Whether to permit the L2TP server (local device) to access the internal subnet of the L2TP client.	[Example] Permit
Branch Tunnel IP	IP address of the L2TP client to be accessed by the device.	The IP address must be in the same range as the IP address pool. [Example] 10.20.1.2
Branch IP/Mask	Internal subnet of the L2TP client to be accessed by the device.	A network segment that overlaps an IP address pool cannot be configured. [Example] 10.20.11.0/255.255.255.0
IPsec Config ● L2TP itself does not provide encryption and needs to be used with IPsec to achieve data encryption, integrity checksum, and anti-replay to ensure transmitter security. ● After the configuration is complete, the device automatically generates an IPsec VPN tunnel. Choose **Network** > **VPN Mgmt** > **IPsec VPN** > **Custom Tunnel** to view the IPsec VPN connection status.		
IPsec Encryption	Whether to enable the device to encrypt data transmitted by a tunnel through IPsec.	[Example] Encryption
Tunnel Name	Name of an IPsec VPN tunnel.	The default tunnel name is L2TP over IPsec, which can be changed manually.
Local Address	Outbound interface used by the local device to establish an IPsec tunnel with the remote device. The data flow protected by IPsec is forwarded to the remote end of the tunnel through this interface.	Select the routed interface configured with an IPv4 address or manually enter a valid IPv4 address configured for the local device.
Pre-shared Key	Key used for identity authentication. The L2TP client can communicate with the L2TP server only when the key on the L2TP client is the same as that on the L2TP server.	[Example] Ruijie123

Item	Description	Remarks
Local ID Type	The local ID is used to authenticate the identity of the local device. The following types are supported: ● **IPV4_ADDRESS**: The IPv4 address is used as the local ID in IKE negotiation. ● **FQDN**: The fully qualified domain name (FQDN) is used as the local ID in IKE negotiation. ● **USER_FQDN**: The user FQDN is used as the local ID during IKE negotiation. ● **KEY_ID**: The specified key identifier is used as the local ID in IKE negotiation.	● The ID type of the local device must be the same as that of the remote device. ● If the local interface is of the PPPoE or DHCP type, you are advised to set this parameter to **FQDN** or **IPV4_ADDRESS** (in this case, do not enter the local ID). [Example] IPV4_ADDRESS
Local Identity	A string that identifies the identity of the local device for authentication.	● The local ID must be the same as the remote ID configured on the remote device. ● Based on the local ID type, fill in a string in the corresponding format: ○ **IPv4_ADDRESS**: Local IPv4 address, for example, 6.6.6.2. ○ **FQDN**: Local domain name, for example, aaa.com. ○ **USER_FQDN**: Local user domain name, for example, julia@aaa.com. ○ **KEY_ID**: Specific string that can identify the local identity, such as the private ID of vendor. ● If this field is empty, the IP address of the local interface is used by default. Do not enter this parameter if the local interface is of the PPPoE or DHCP type.
Advanced IPsec Settings		
IKE Negotiation Mode	IKE negotiation mode configured in phase 1: ● **Auto**: The main mode and aggressive mode can be used in response to negotiation, and the main mode is used for initiating negotiation. ● **IKEv1 Main Mode**: Identity information is encrypted for higher security. ● **IKEv1 Aggressive Mode**: Negotiation is fast but identity information is not encrypted.	[Example] **IKEv1 Main Mode**

Item	Description	Remarks
IKE SA Lifetime	IKE SA lifetime. After the lifetime of an IKE SA expires, the device replaces the IKE SA with a new SA. The actual IKE SA lifetime depends on the negotiation result.	[Example] 86400
IPsec Perfect Forward Secrecy	Whether to enable perfect forward secrecy (PFS). PFS ensures security of IPsec SAs even if the key used by an IKE SA is cracked, as an additional DH exchange is performed.	[Example] Enabled
IPsec DH Group	DH group used by PFS: ● **GROUP1**: The 768-bit DH group is used. ● **GROUP2**: The 1024-bit DH group is used. ● **GROUP5**: The 1536-bit DH group is used. ● **GROUP14**: The 2048-bit DH group is used. ● **GROUP15**: The 3072-bit DH group is used. ● **GROUP16**: The 4096-bit DH group is used. A larger group ID indicates higher security and longer time required for key calculation.	● Click the drop-down list and select a value. ● After PFS is enabled, **GROUP5** is used by default. [Example] **GROUP14**
IPsec SA Lifetime	IPsec SA lifetime. When the lifetime of an IPsec SA exceeds the value, the device replaces the IPsec SA with a new SA. The actual IPsec SA lifetime depends on the negotiation result at both ends.	By default, IPsec SAs with the lifetime of 3600s can be established for the windows client. Changing this parameter will cause negotiation failures. [Example] 3600
IPsec Tunnel MTU	Maximum number of bytes of data packets that can be transmitted by the IPsec tunnel at a time.	The tunnel MTU must be smaller than the MTU of the outbound interface. [Example] 1480

Item	Description	Remarks
DPD Type	Dead Peer Detection (DPD) is used to detect the peer end of an IPsec tunnel, so that the tunnel can be removed in a timely manner if the peer end is unreachable. DPD supports two modes: ● **Idle Mode**: If the local end does not receive any response message from the remote end after sending a packet, it periodically sends DPD packets to the remote end. ● **Regular Mode**: DPD packets are sent at the configured DPD detection interval.	[Example] **Idle Mode**
DPD Detection Interval	Interval between two DPD operations in **Regular Mode**, in seconds.	[Example] 30
DPD Retry Interval	Interval at which DPD packets are retransmitted. When the local end sends a DPD request packet and does not receive a response packet within the retry interval, it retransmits the DPD request packet. If it still does not receive a response packet from the remote end after three retransmissions, it considers that the remote end is unreachable and automatically removes the IPsec tunnel.	[Example] 3
Advanced Settings Configure keepalive parameters for L2TP connections. If the L2TP server fails to receive any response from the client within the timeout interval, the L2TP server automatically closes the L2TP session. L2TP connection timeout interval = Max. Unanswered LCP Packets x PPP Keepalive Interval		
Max. Unanswered LCP Packets	The number of unanswered LCP packets increases by 1 if the L2TP server fails to receive any response packet from the client after sending the LCP packets. When the number of consecutive unanswered LCP packets exceeds the specified maximum value, the L2TP server automatically disconnects the VPN tunnel.	The default value is 10. That is, when a device does not receive any response from the client after sending LCP packets 10 consecutive times, the device automatically disconnects the VPN connection. [Example] 10

Item	Description	Remarks
PPP Keepalive Interval	Interval at which a device sends PPP link maintenance detection packets (LCP Echo-Request packets). After an L2TP tunnel is established, the device periodically transmits LCP Echo-Request packets to detect the PPP link state and ensure normal operation of the L2TP tunnel.	The default value is 10s. That is, the device sends LCP Echo-Request packets to the remote end of the tunnel at an interval of 10s. [Example] 10s
PPP MRU	The PPP maximum receive unit (MRU) is used to limit the maximum PPP frame length (in bytes) of the local device (L2TP server) to prevent packet loss or performance deterioration caused by large-sized frames.	[Example] 1400

(3) Click **Save**. A message is displayed, asking you whether to create a security policy. Click **Create**. The device automatically generates a security policy with the source address set to the IP address pool name and name set to **l2tp-server0_in**. The policy is used to permit traffic from the L2TP client to the local device (L2TP server) that accesses IP addresses in the address pool.

Note

If an L2TP client uses an IP address not in the address pool (namely, the source IP address of the client) to access the device (L2TP server), you need to manually add a security policy.

If the headquarters (L2TP server) is allowed to access the branch (L2TP client), the device automatically creates security policy **l2tp-server0_out** whose destination address is the IP address/network mask of the branch to permit traffic from the device to the internal subnet of the L2TP client.

Follow-up Procedure

- Click **Clear Config** to clear the current L2TP server configuration and restore the device to the unconfigured state. The automatically created security policies and IPsec VPN tunnel will also be deleted.
- Enter the public IP address, username, and password of the device on the L2TP client to initiate an L2TP dial-up connection with the L2TP server.

6.8.3 Viewing L2TP Tunnel Information

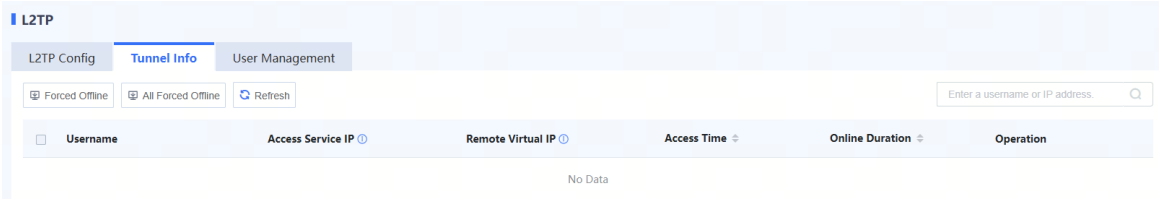
Application Scenario

After L2TP clients access the L2TP server and establish L2TP tunnels, you can view detailed information about the online L2TP users and forcibly disconnect L2TP users.

Procedure

(1) Choose **Network** > **VPN Mgmt** > **L2TP** > **Tunnel Info**.

(2) This tab page displays information about all online L2TP users.



(3) Find the target user and click the buton in the **Operation** column to log out the user

If you need to log out multiple users, select multiple records and click **Forced Offline**.

To force all users offline, click **All Forced Offline**.

6.8.4 Performing L2TP VPN User Management

Application Scenario

Configure an L2TP VPN user account as the access credential for the L2TP VPN client. When a client requests to access the VPN server, it needs to provide a valid identity credential (such as the username and password) for authentication. Only authenticated clients are permitted to access the internal network and access internal resources. Proper configuration and management of VPN users can guarantee internal network security and prevent unauthorized access.

Procedure

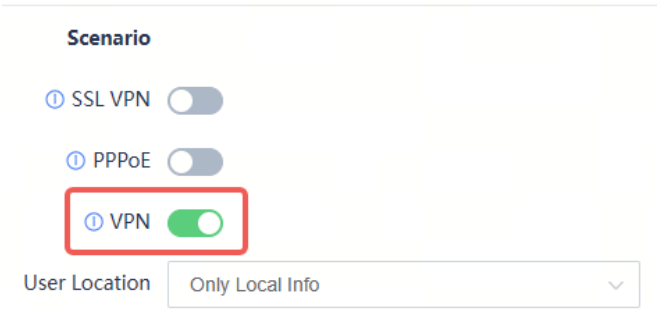
(1) Choose **Network** > **VPN Mgmt** > **L2TP** > **User Management**.

(2) (Optional) Configure an authentication domain for the L2TP VPN server.

By default, the L2TP VPN server authenticates access terminals using the authentication domain named vpn, that is, the user information under this domain. To modify the authentication domain used by the L2TP VPN server, click **Switch authentication domain**.

Caution

- Toggle **VPN** on in **Scenario** for the authentication domain used by the L2TP VPN server. Otherwise, VPN users cannot log in to the network.

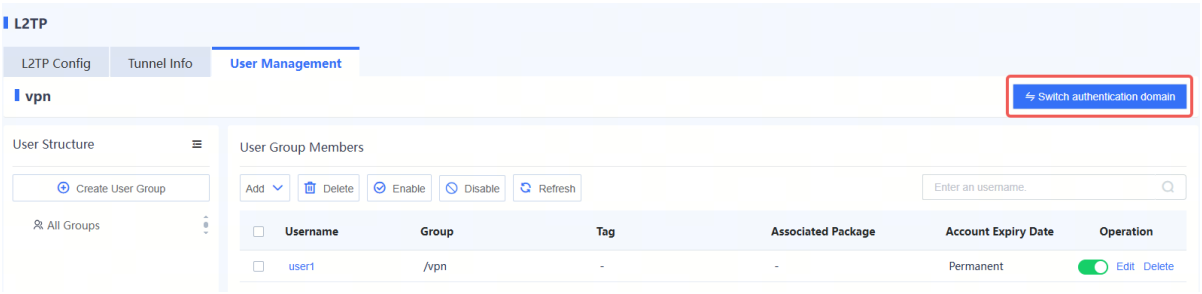


- Modifying the L2TP authentication domain will disconnect all online users. Exercise caution when performing this operation.

Note

- By default, the authentication domain named vpn uses only local user information for VPN access authentication, that is, VPN user information needs to be configured and managed on the local device. If an external server is used to manage VPN user accounts, you can modify the authentication domain configuration, set **Use server user information**, and configure the authentication server information.

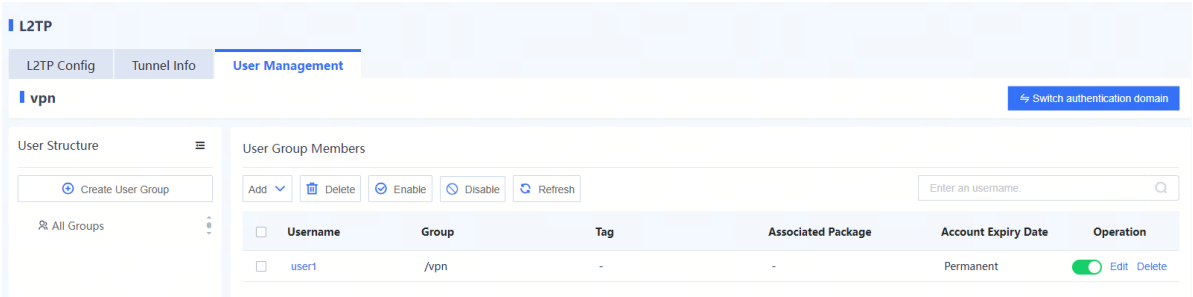
- To add an authentication domain or modify the authentication domain configuration, choose **Object** > **User Authentication** > **Authentication Domain**. For more information about authentication domains, see 5.8.7 Authentication Domain Management.



(3) Configure VPN users.

The overall operation logic of the VPN user management page is similar to that of the authenticated user management page. You can configure user groups, add a single user, add users in batches, and export user information. For details about user management operations, see 5.8.2 User Management.

Follow-up Procedure

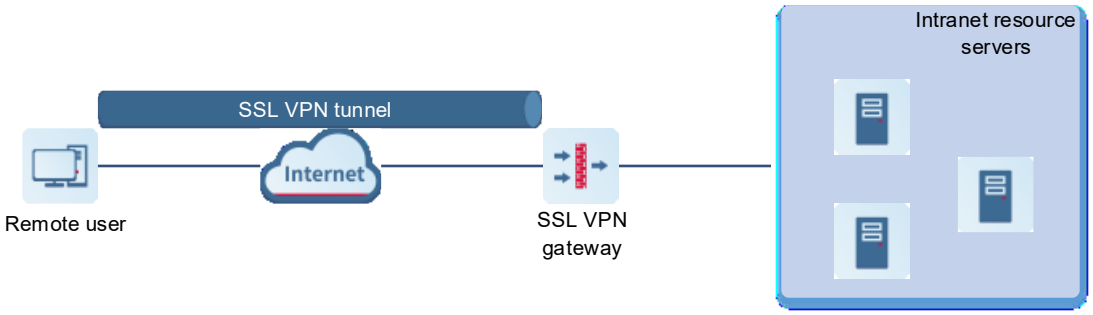


- Click **Edit** in the **Operation** column to modify user information.
- Toggle on or off the switch in the **Operation** column to enable or disable the user account.
- Select multiple users and click **Delete** to delete user information in a batch. After deletion, if authenticated users go offline, they cannot pass authentication again.
- Select multiple users and click **Disable** to disable the users in a batch. After this operation, if authenticated users go offline, they cannot pass authentication again.
- Select multiple users and click **Enable** to enable the users in a batch.

6.9 SSL VPN

6.9.1 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 (through username and password, username and password+hardware signature, or username and password+SMS authentication) 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.

6.9.2 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 is authorized to access network resources on multiple SSL VPN gateways, they can log in to the gateways concurrently.
- Disabling, deleting, or modifying the configuration of an SSL VPN gateway can force users to go offline. Therefore, perform these operations with caution.
- By default, the untrusted self-signed certificate **default** on the local certificate page is used as the gateway certificate. You can import a trusted certificate on the local certificate page. For details on how to import a gateway certificate, see 5.9.2 Local Certificate.
- When the firewall functions as the egress gateway, you are advised to use the IP address (public IP address) of the device's external interface as the SSL VPN gateway address.
- When the firewall is deployed behind the egress gateway, you need to manually configure a gateway address. Typically, the gateway address is set to the IP address (public IP address) of the external interface on the egress gateway. In addition, you need to add another gateway address and select the firewall interface connected to the egress gateway for sending and receiving SSL VPN packets.

Prerequisites

Before configuring SSL VPN, complete the following tasks:

(1) Ensure that there are reachable routes between the two devices at both ends of an SSL VPN tunnel to be established.

(2) The user authentication domain has been configured. For details, see 5.8.7 Authentication Domain Management.

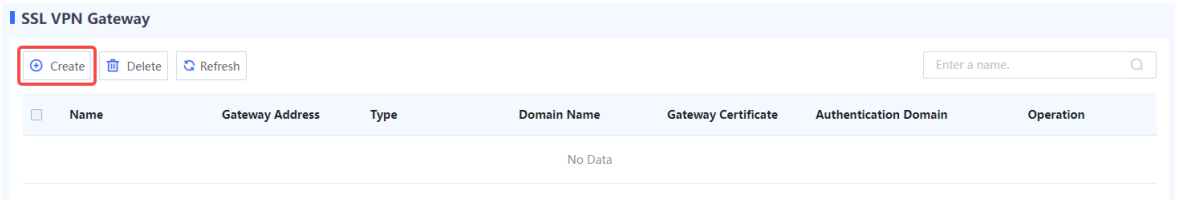
(3) User information configuration is completed. For details, see 5.8.2 User Management.

(4) To enable SMS two-factor authentication, complete the SMS server configuration first. For details, see 5.8.14 SMS Authentication Server.

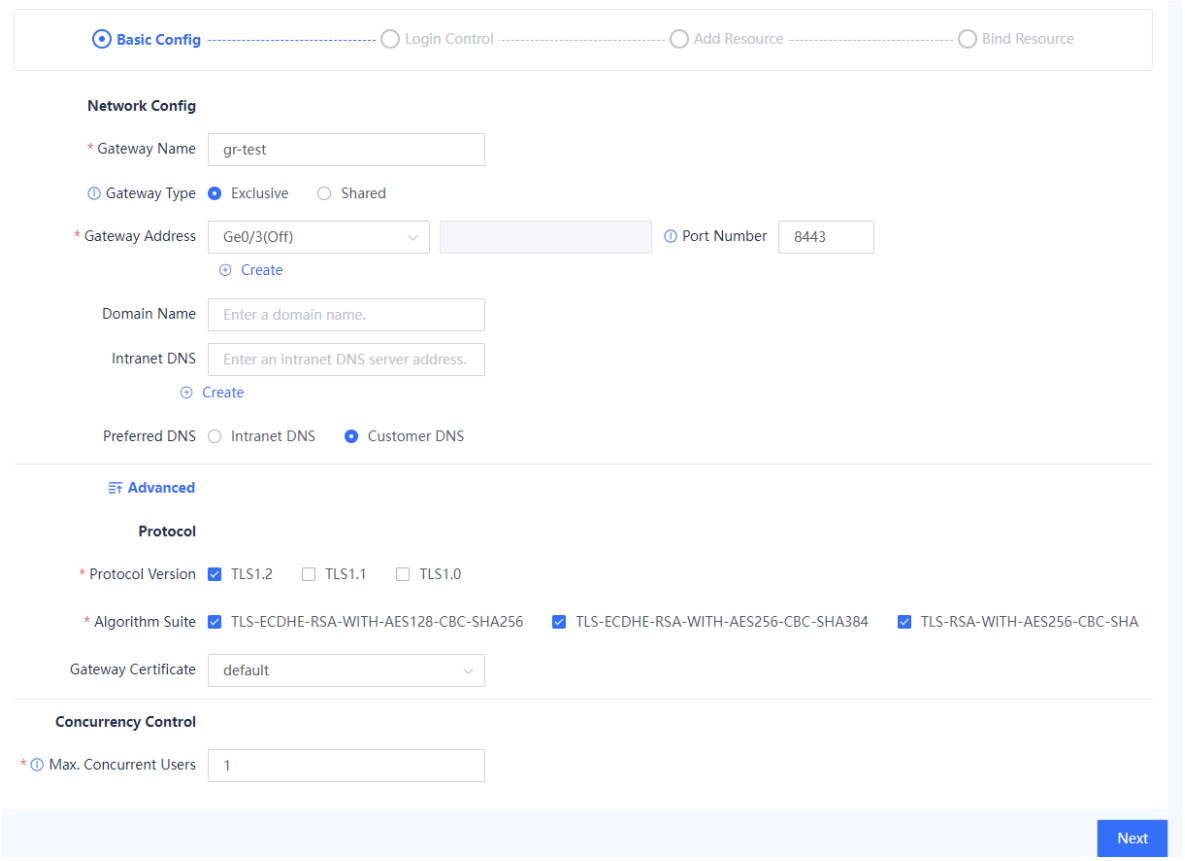
Procedure

(5) Choose **Network** > **VPN Mgmt** > **SSL VPN** > **SSL VPN Gateway**.

(6) Click **Create** to access the **Add SSL VPN Gateway** page.



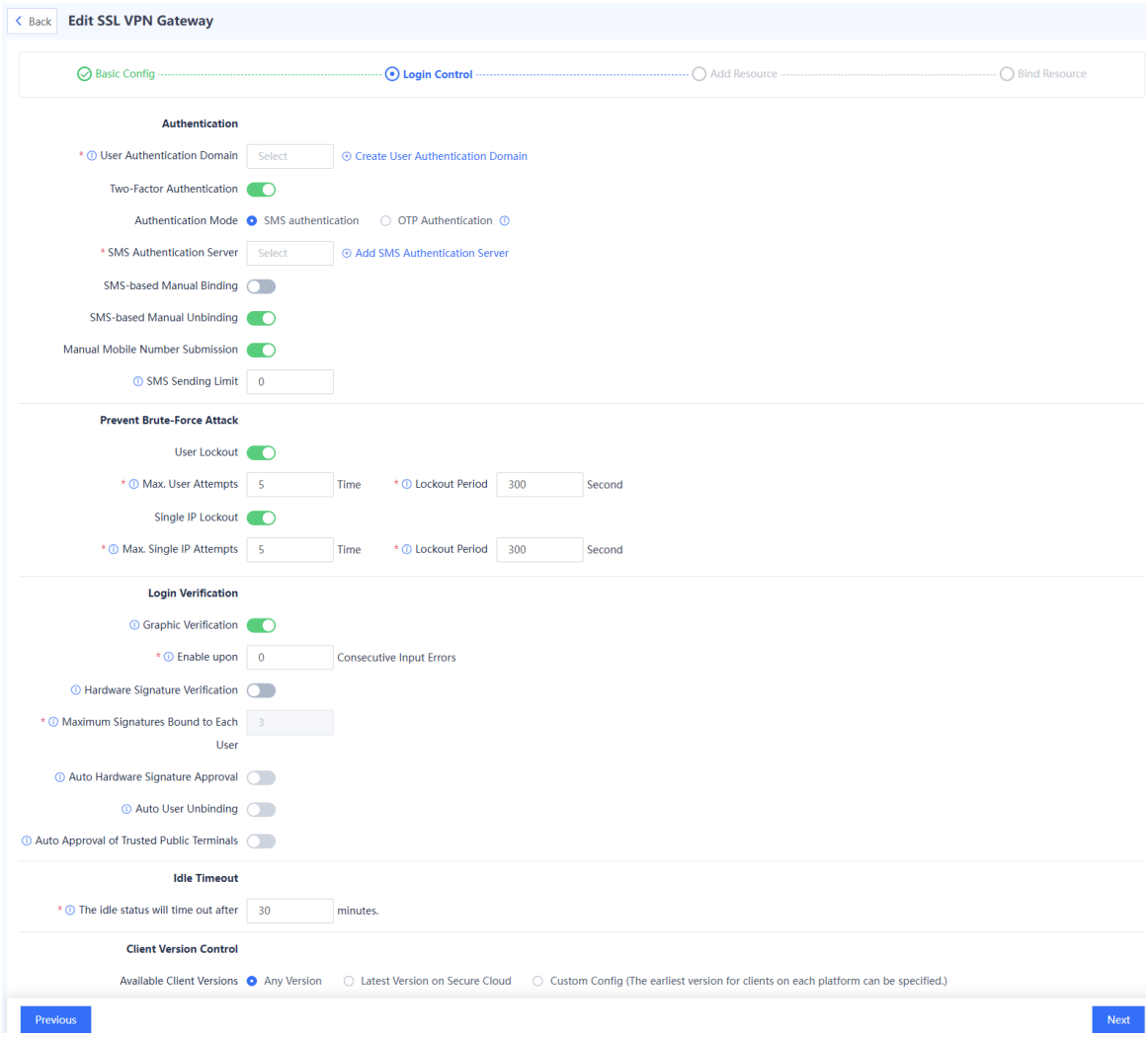
(7) Configure basic information of an SSL VPN gateway.



Item	Description	Remarks
Network Config		
Gateway Name	Name of the SSL VPN gateway.	[Example] gateway1
Gateway Type	● **Exclusive**: The system allocates a unique IP address and domain name to the virtual gateway, and users can log in to the SSL VPN gateway by using the IP address (or domain name) and port number. ● **Shared**: The system allocates a shared IP address and domain name to the virtual gateway, and users can log in to the SSL VPN gateway by using the domain name and port number.	[Example] Shared
Gateway Address	Address for accessing the SSL VPN gateway. You can choose an interface address or configure it manually. A gateway can be configured with a maximum of three addresses, each of which can be used for login. To select an interface address, ensure that reverse path limited (RPL) has been configured on the interface. If the interface is a bridge interface, you need to manually configure a security zone for the bridge interface to ensure normal traffic forwarding.	● The value can be an IPv4 or IPv6 address. ● After you select an interface, the interface address is automatically displayed. [Example] 1234::100
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] TSL1.2

Item	Description	Remarks
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. The **default** certificate is untrusted. You can import a trusted certificate on the local certificate page. For details on how to import the certificate, see 5.9.2 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

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



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. When referencing an authentication domain, ensure that the authentication domain is correctly configured and enabled. For details about how to configure an authentication domain, see 5.8.7 Authentication Domain Management.	[Example] default
Two-Factor Authentication	Whether to enable two-factor authentication. If this function is enabled, additional identity authentication (SMS or OTP authentication) is performed upon successful username and password authentication to enhance SSL VPN user authentication security.	[Example] Enable

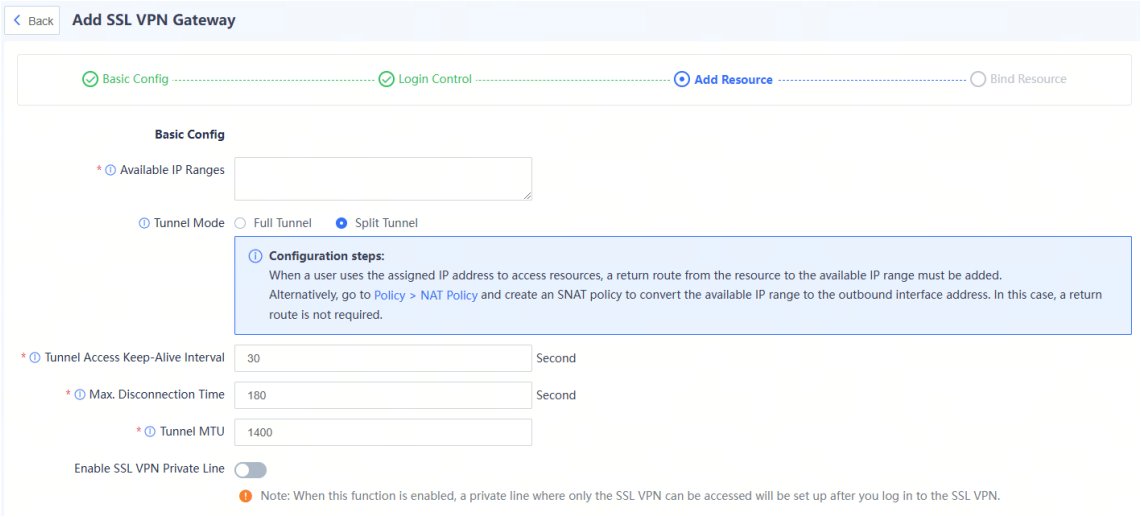
Item	Description	Remarks
Authentication Mode	● SMS authentication: Perform SMS authentication upon successful username and password authentication. ● One-Time Password (OTP) authentication: Upon successful username and password authentication, a user needs to enter an OTP dynamically generated by an authentication tool (Google Authenticator or Microsoft Authenticator) to improve security. The system time of the gateway must be correct and consistent with the system time of the authentication tool to ensure normal OTP authentication. **Note** The authentication tool needs to be downloaded and installed on the mobile phone by the user. When a user logs in to the SSL VPN gateway for the first time, the SSL VPN client displays a pop-up window showing the OTP authentication key. The user needs to copy the key and bind it to an authentication tool to obtain an OTP. When logging in to the SSL VPN gateway next time, the user can directly view the OTP generated by the authentication tool without binding the OTP authentication key again. To reset OTP keys, access the **User Management** page and reset the keys. After the reset, the keys bound to the users will become invalid and must be bound again upon the next login to the SSL VPN gateway.	[Example] SMS Authentication
SMS Authentication Server	Select or add an SMS authentication server for two-factor authentication. For details about the SMS authentication server, see 5.8.14 SMS Authentication Server.	-
SMS-based Manual Binding	If no hardware signature has been approved, users can manually submit hardware signatures. If this function is enabled, the users need to pass SMS two-factor authentication before binding hardware signatures, thereby preventing malicious hardware signature binding.	[Example] Enable
SMS-based Manual Unbinding	Users can manually unbind the hardware signatures of terminals. If this function is enabled, the users need to pass SMS two-factor authentication before unbinding hardware signatures.	[Example] Enable

Item	Description	Remarks
Manual Mobile Number Submission	If a local user does not have a mobile number, the user can submit a mobile number. After the mobile number is submitted, an SMS verification code is sent for authentication. User information is modified only after the authentication succeeds.	[Example] Enable
SMS Sending Limit	Maximum number of SMS verification code requests for each user per day. The value 0 indicates no limit.	[Example] 1
Prevent Brute-Force Attack		
User Lockout	Specifies whether to enable user lockout after a certain number of consecutive failed login attempts. During the lockout period, the user cannot log in to the gateway.	[Example] Enable
Max. User Attempts	Maximum number of consecutive login failures that a user is allowed before being locked out.	[Example] 5
Lockout Period	Lockout period during which the user cannot log in to the gateway.	[Example] 300 seconds
Single IP Lockout	Specifies whether to enable locking out of a specific IP address on which a certain number of consecutive login failures are detected. During the lockout period, the user cannot log in to the gateway from this IP address.	[Example] Enable
Max. Single IP Attempts	Maximum number of consecutive login failures that are allowed from a specific IP address before it is locked out.	[Example] 5
Lockout Period	Lockout period during which the user cannot log in to the gateway from the locked IP address.	[Example] 300 seconds
Login Verification		
Graphic Verification	Specifies whether to display a graphic verification code on the gateway login page after a certain number of consecutive login failures. This function can prevent 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

Item	Description	Remarks
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 6.9.3 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		
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	Version of the SSL VPN client that connects to the SSL VPN gateway. Currently, only Ruijie SSL VPN client is supported. ● **Any Version**: no limit on the version of the SSL VPN client ● **Latest Version on Secure Cloud**: the latest version released on Ruijie Secure Cloud Platform ● **Custom Config (The earliest version for clients on each platform can be specified.)**: custom client versions for each type of system	[Example] Any Version

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

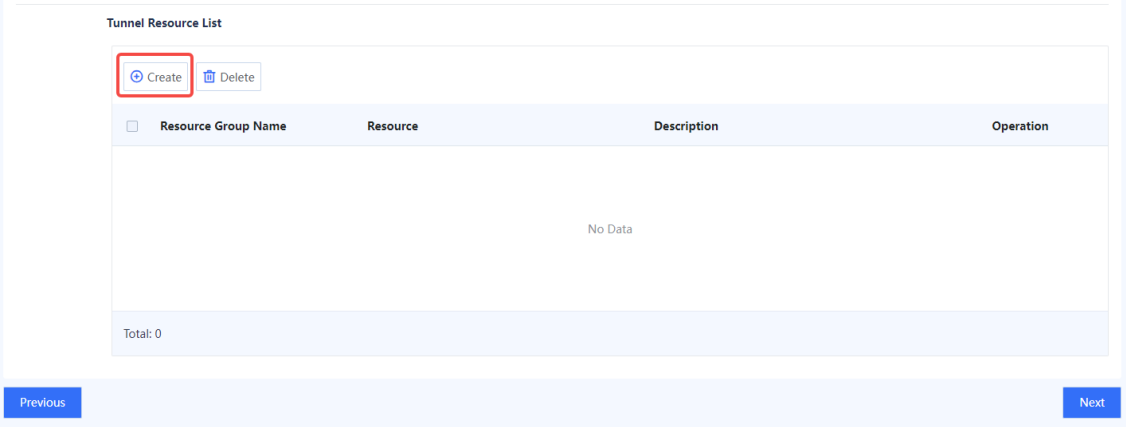
a Configure basic information:

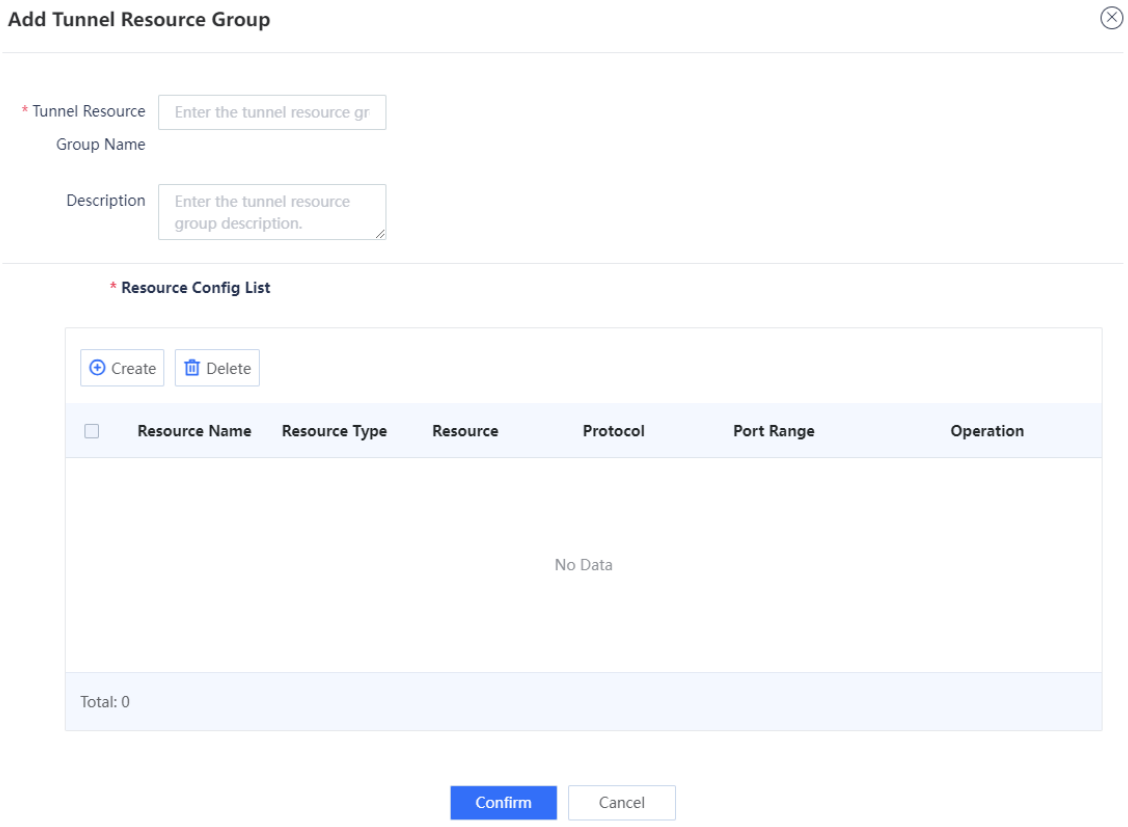


Item	Description	Remarks
Available IP Ranges	IP address range allocated to the client. The client uses the assigned IP address to establish a tunnel with the SSL VPN gateway. Once the available IP addresses are exhausted, new users cannot log in, and the IP address is released after the user logs out.	[Example] 1.1.1.0/255.255.255.0
Tunnel Mode	Supports two modes: ● **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
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
Tunnel MTU	MTU for downlink traffic transmitted through the SSL VPN tunnel. This parameter specifies the maximum number of bytes in a single packet sent by the SSL VPN gateway to the SSL VPN client.	The default value is 1400, and the unit is byte. [Example] 1400

Item	Description	Remarks
Enable SSL VPN Private Line	If this function is enabled, only resource traffic and local communication traffic authorized to users can enter the SSL VPN tunnel, and the Internet access traffic of users cannot enter the tunnel.	[Example] Disable

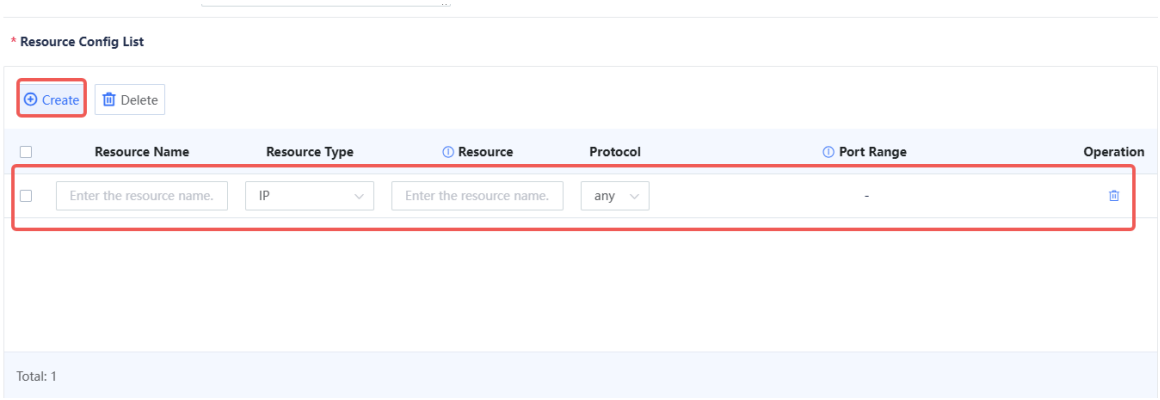
b If you set **Tunnel Mode** to **Split Tunnel**, you need to create a tunnel resource group. Click Create to configure the information of resources that can be accessed through this tunnel.





Item	Description	Remarks
Tunnel Resource Name	Name of the resource that can be accessed through this tunnel.	[Example] IP address
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.

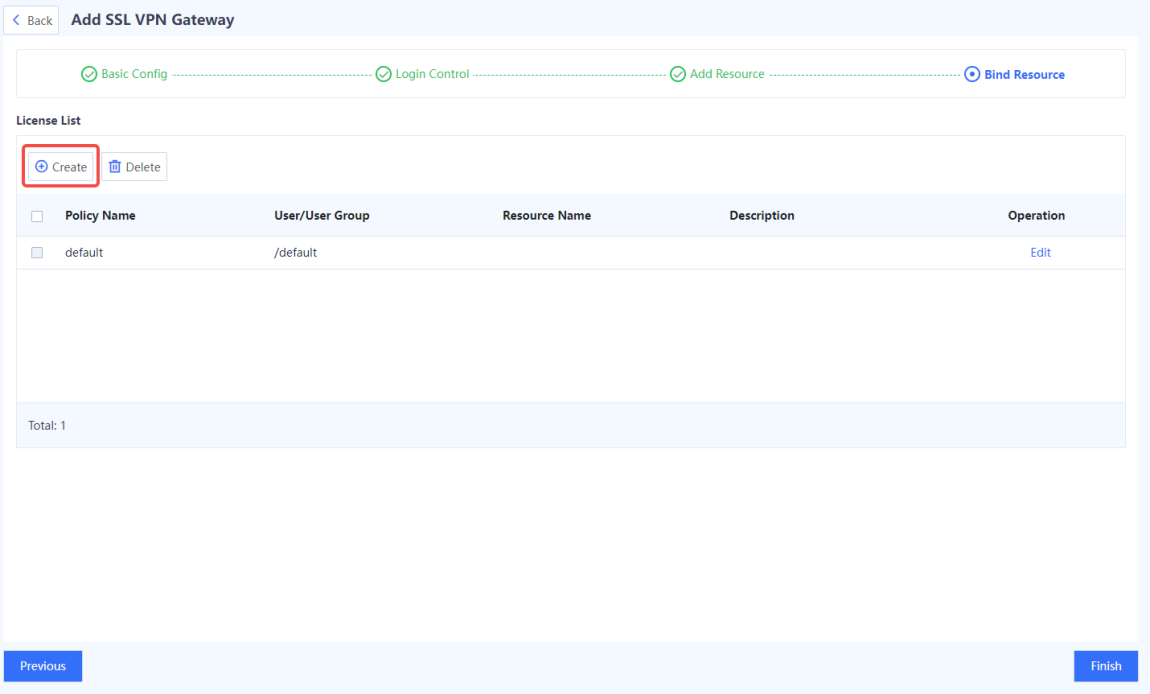


Item	Description	Remarks
Resource Name	Name of the resource that can be access through this tunnel.	[Example] IP address
Resource Type	Supported resource types are as follows: ● **IP**: Only a single IP address is supported. Example: 192.168. 1.1. ● **Subnet**: IP/Mask length. Example: 192.168.1.0/24. ● **Domain Name**: Domain name. Example: www.abc.com. ● **URI**: URI. Example: <proto://ip[:port]>.	N/A
Resource	Resource to be entered based on the selected resource type. For example, enter an IP address if **Resource Type** is set to **IP**.	N/A
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

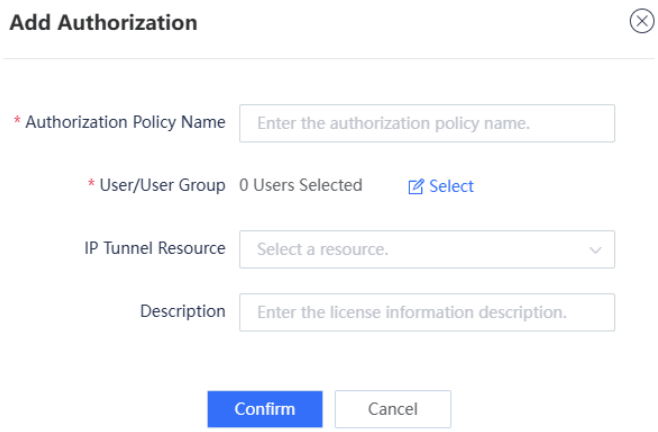
d Verify the configuration and click **Confirm** to return to the **Add Tunnel Resource Group** page.

(10) 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.



Item	Description	Remarks
Authorization Policy Name	Name of an authorization policy.	[Example] Policy_1

Item	Description	Remarks
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**.

(11) Verify the configuration and click **Finish**.

Follow-up Procedure

- If a tunnel is disconnected, you can diagnose and detect the fault cause by SSL VPN. For details, see 8.6.14. SSL VPN Fault Diagnosis.
- 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.

6.9.3 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.

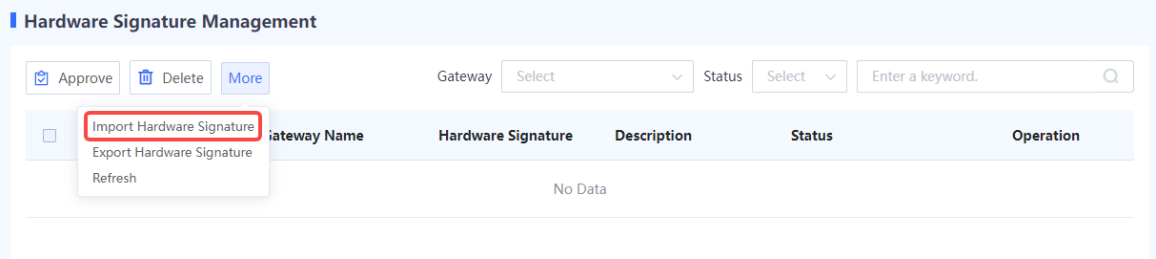
Precautions

- 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** > **VPN Mgmt** > **SSL VPN** > **Hardware Signature Management**.

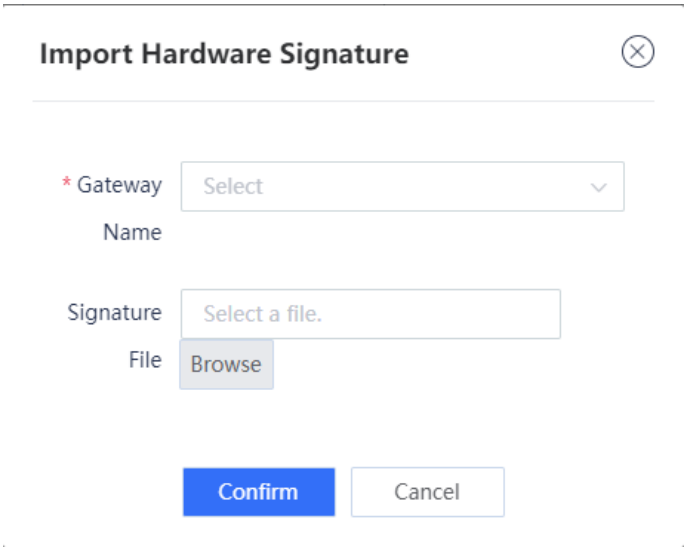
(2) Click **More** and select **Import Hardware Signature**.



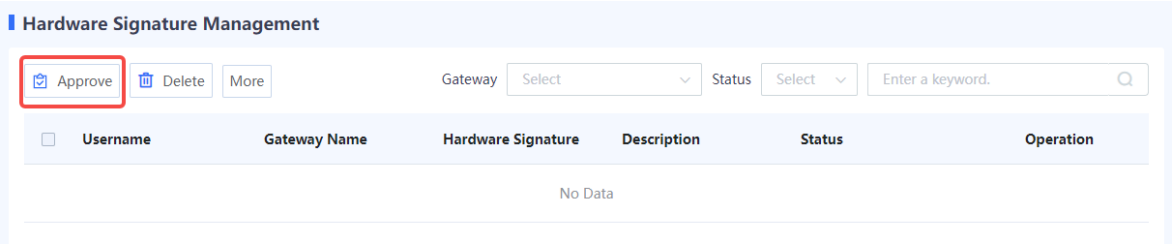
(3) Select the gateway to which the hardware signature is imported. Click **Browse** to select the hardware signature file and upload it.

Note

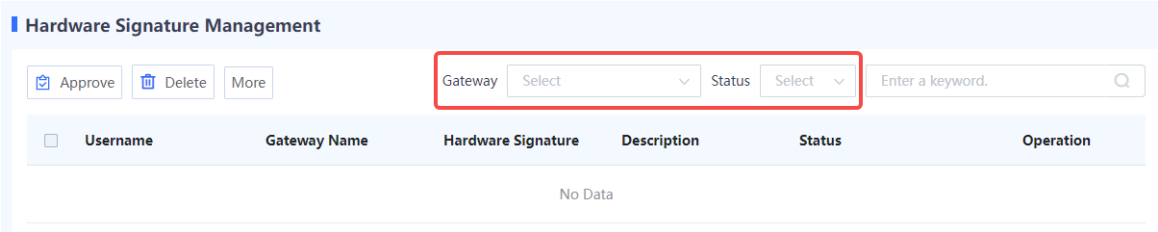
The format of the hardware signature file is .data. To import hardware signatures in batches, contact a technical engineer for help.



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



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



6.9.4 Operation Monitoring

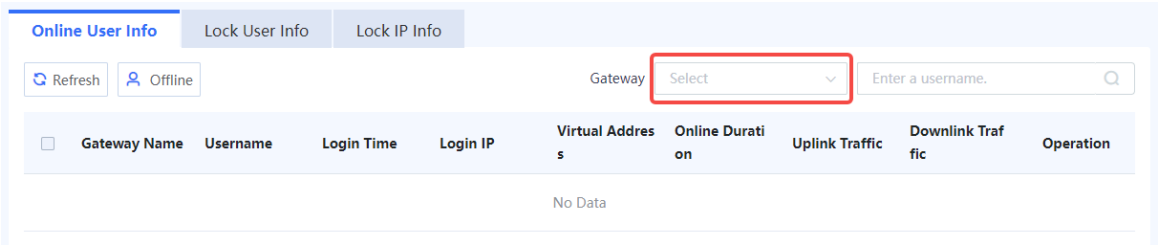
Application Scenario

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** > **VPN Mgmt** > **SSL VPN** > **Operation Monitoring**.

(2) Click the **Online User Info** tab. The online user information of all SSL VPN gateways is displayed on this tab page. Select a gateway to view only the online user information of the selected gateway.

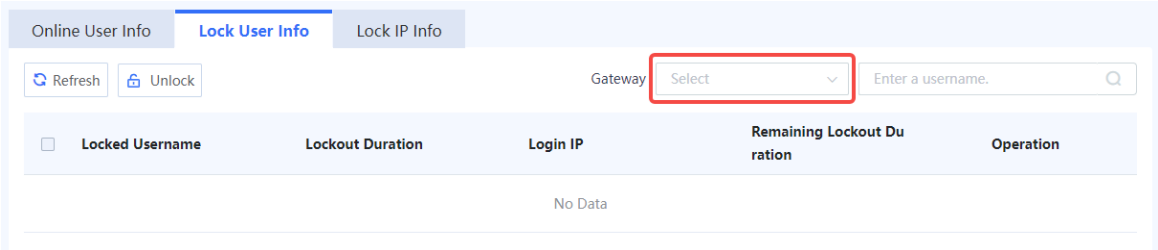


(3) To force a user to go offline, click **Offline**.

2. Viewing Locked User Information

(1) Choose **Network** > **VPN Mgmt** > **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.

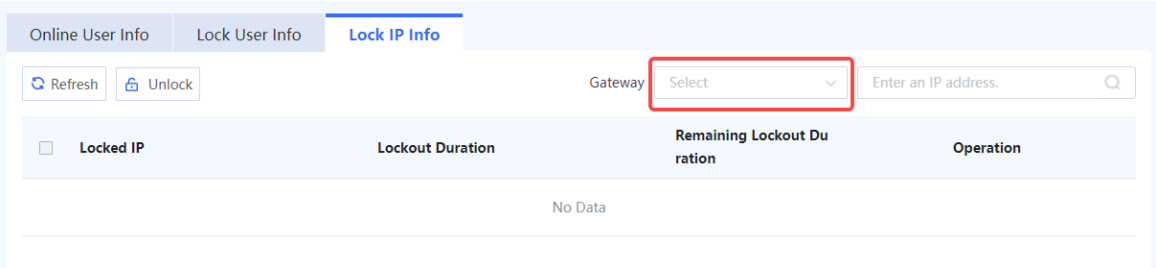


(3) To unlock a user, click **Unlock**.

3. Viewing Locked IP Information

(1) Choose **Network** > **VPN Mgmt** > **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.



(3) To unlock an IP address, click **Unlock**.

6.10 IPsec VPN

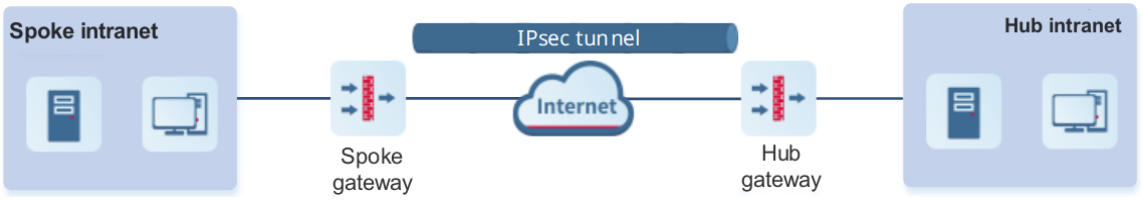
6.10.1 Overview

IPsec VPN applies Internet Protocol Security (IPsec) to establish a private channel for encrypted and secure communication on a public network. Specific algorithms are used to encrypt and authenticate data transmitted over the IPsec tunnel. IPsec VPN prevents IP packets from being intercepted, forged, or tampered with when traversing a public network, guaranteeing secure transmission of user data on the Internet.

IPsec VPN is typically used to set up secure interconnection between an enterprise hub site and spoke site. After an IPsec tunnel is established between the hub site gateway and spoke site gateway, data can be securely transferred between the hub site and spoke site, and intranet resources can be shared.

In addition, IPsec VPN supports active/standby switchover. In a hub-and-spoke scenario, an active tunnel and two standby tunnels can be established between the hub site and spoke site. When the active tunnel fails, the standby tunnel takes over traffic, thereby ensuring stable transmission.

Figure 6-10 Typical Application Scenario of IPsec VPN



6.10.2 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 IKEv1 SA.

In this phase, the two ends negotiate parameters for establishing an IKEv1 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 (IKEv1 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.

3. IKEv2 Negotiation Process

IKEv2 is an enhanced version of IKEv1. The negotiation process of IKEv2 is similar to that of IKEv1, which is divided into IKEv2 SA establishment and IPsec SA establishment. However, the negotiation process of IKEv2 is faster. To establish a pair of IPsec SAs, IKEv1 main mode requires nine messages, and IKEv1 aggressive mode

requires six messages. IKEv2 requires only four messages to establish an IKEv2 SA and a pair of IPsec SAs. In addition, IKEv2 supports the creation of multiple IPsec SAs. If more than one pair of IPsec SAs needs to be established, only two messages are required to create each additional pair of IPsec SAs. When an IKEv2 SA requires multiple IPsec SAs, child SA exchanges can be created for negotiating more than one pair of IPsec SAs.

6.10.3 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:

- **Site-to-Site (Spoke/Site)**: 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, both ends must have fixed IP addresses or domain names and can initiate an IPsec tunnel negotiation.
- **Hub-and-Spoke (Hub)**: Establish multiple IPsec tunnels between the hub site and spoke sites to enable interconnection among the sites and private networks connected to the sites. In this scenario, a peer end does not require a fixed IP address or domain name. However, only a spoke site can initiate an IPsec tunnel negotiation.

Prerequisites

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

- In a site-to-site 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.

Precautions

- Two tunnels (master and backup) can be configured between two sites, and the interesting traffic of the two tunnels can be the same. If the master tunnel fails, service data are automatically switched to the backup tunnel. The interesting traffic, authentication key, IKE parameters, and IPsec parameters of the master and backup tunnels must be the same.
- If the device establishes IPsec tunnels with multiple sites simultaneously, you must configure different interesting traffic for different sites. For example, if Site A establishes two tunnels with Site B and Site C separately, the interesting traffic of the two tunnels cannot be the same. The device creates routes based on

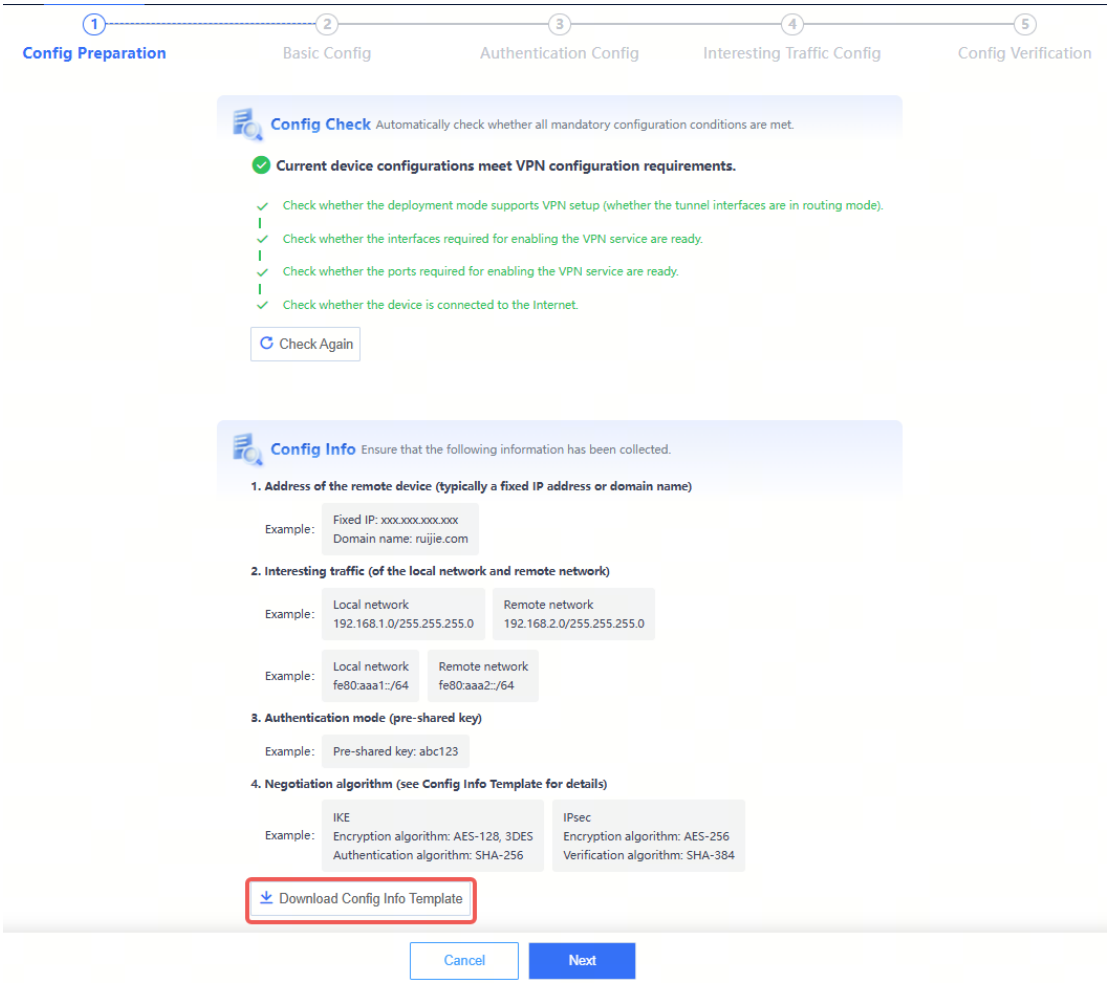
the interesting traffic. If the interesting traffic from Site A to Site B is the same as that from Site A to Site C, there are two routes to the same destination. When the device forwards packets based on the route priority, packets that should be forwarded over a tunnel may be forwarded to another tunnel, causing a service exception.

Procedure

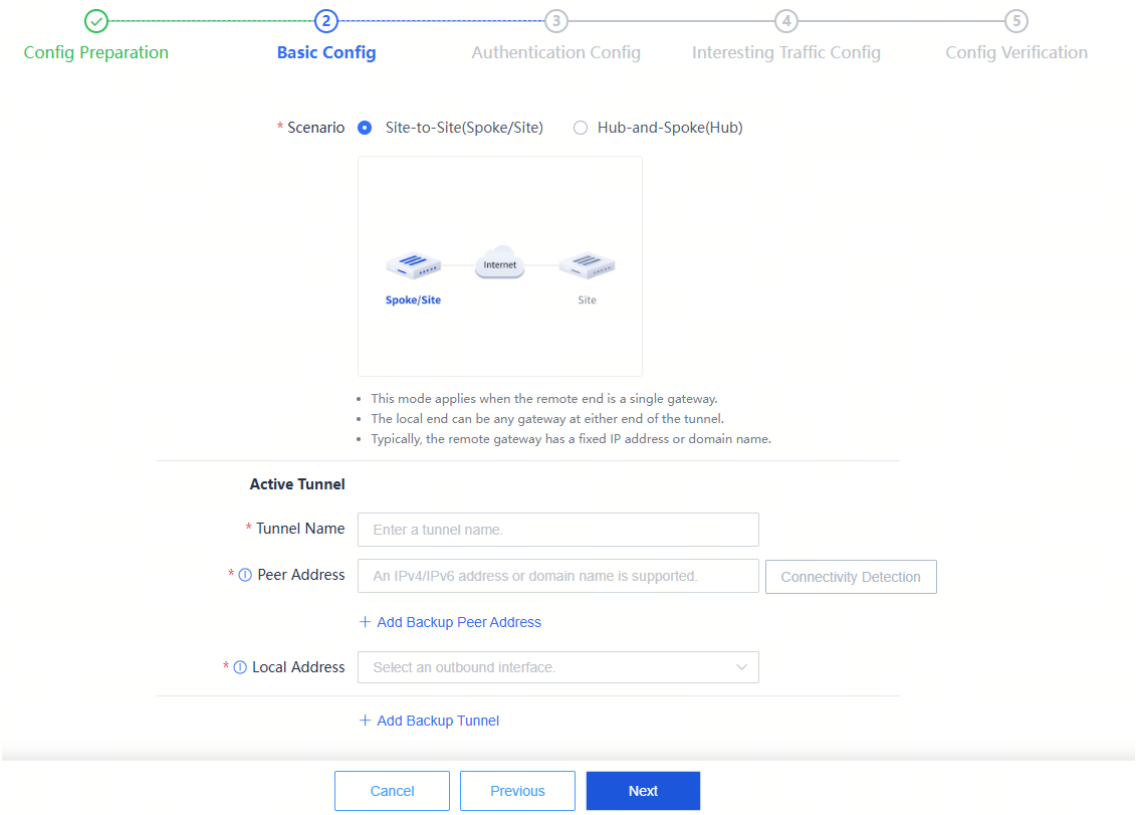
(1) Choose **Network** > **VPN Mgmt** > **IPsec VPN** > **Config Wizard**to access the Config Preparation page.

The device automatically detects whether the current configuration meets conditions for establishing an IPsec VPN tunnel and displays the detection result.

Click **Download Config Info Template** to download the configuration template locally for query and modification.



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

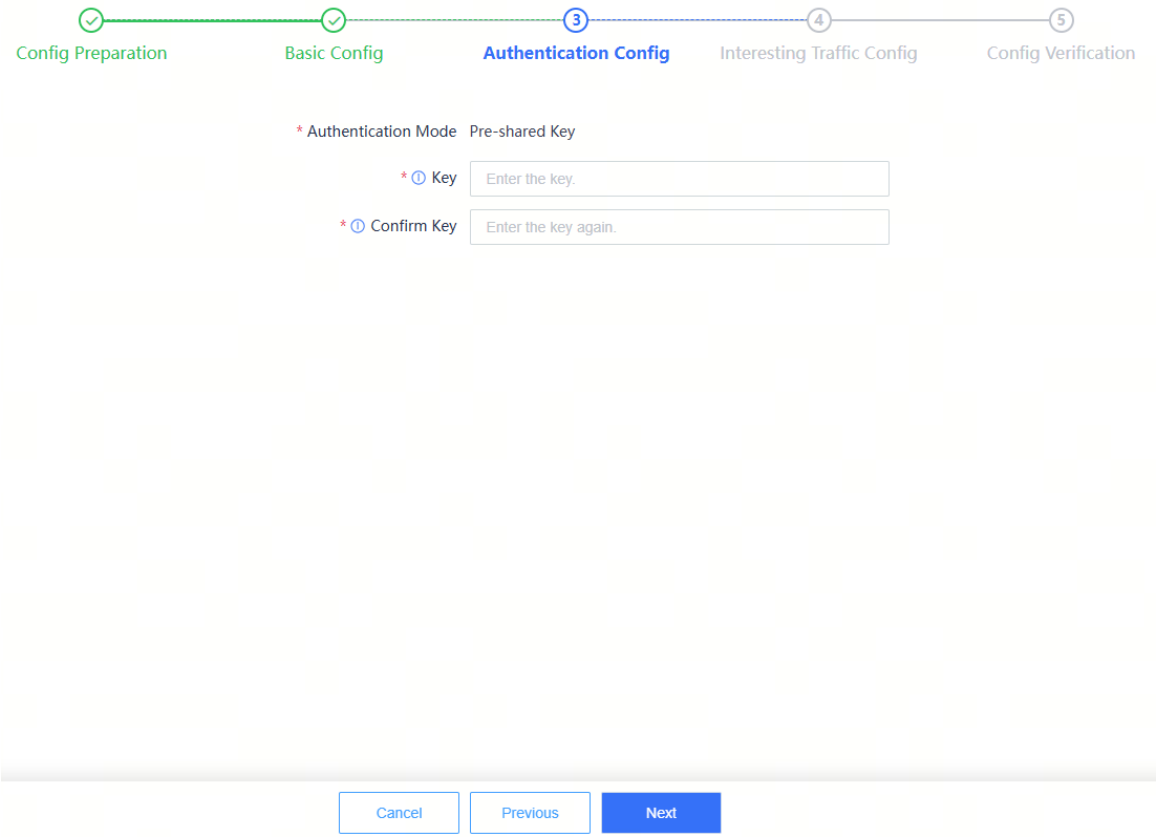


Item	Description	Remarks
Scenario	Select the IPsec tunnel type based on the deployment scenario: ● **Site-to-Site (Spoke/Site)**: applies to scenarios where the peer end has a fixed IP address or domain name, such as IPsec VPN deployment at an enterprise spoke site. ● **Hub-and-Spoke (Hub)**: applies 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.	[Example] Site-to-Site (Spoke/Site)
Scenario: Site-to-Site (Spoke/Site) In the Site-to-Site (Spoke/Site) scenario, click **Add Backup Tunnel** to configure a backup tunnel to implement link backup. You can configure one master tunnel and two backup tunnels in descending order from top down. The system preferentially uses the master tunnel to establish communication with the destination site. If the master tunnel fails, services are automatically switched to an available backup tunnel. When the master tunnel restores normal, services are automatically switched back to the master tunnel.		
Tunnel Name	IPsec tunnel name.	[Example] ipsec_1

Item	Description	Remarks
Peer Address	IP address or domain name used to establish a tunnel with the peer device.	● You need to configure this parameter for the Site-to-Site (Spoke/Site) scenario. ● Enter an IP address or domain name and click **Connectivity Detection** to check whether there is a reachable route between devices at the two ends. ● Click **Add Backup Peer Address** to add a peer address. You can configure a maximum of three peer addresses. Peer addresses have a descending order of priority from top down. ● If the master address of the peer end is unavailable (such as unreachable address, tunnel negotiation failure, and detection timeout), the system automatically switches to a backup address of the peer end for tunnel establishment. If all the peer addresses of the current tunnel are unavailable, the current tunnel is faulty. In this case, if multiple master and backup tunnels are configured, the system automatically switches to another available tunnel based on the tunnel priority. ● The peer address must be the same as the value of the **Local Address** parameter configured on the peer device. [Example 1] 40.0.0.50 [Example 2] 1234::100
Local Address	Outbound interface used to establish an IPsec tunnel with the IKE peer. The data flow protected by IPsec is forwarded to the peer end of the tunnel through this interface.	● Select a routing mode interface with an IP address. ● If the peer address is an IP address, the IP type (IPv4 or IPv6) of the local address must be the same as that of the peer address. ● The local address of the master and backup tunnels cannot be the same. [Example] Ge0/2
Scenario: Hub-and-Spoke (Hub)		
Tunnel Name	IPsec tunnel name.	[Example] ipsec_1

Item	Description	Remarks
Local Address	Outbound interface used to establish an IPsec tunnel with the IKE peer. The data flow protected by IPsec is forwarded to the peer end of the tunnel through this interface.	● Select a routing mode interface with an IP address. ● If the peer address is an IP address, the IP type (IPv4 or IPv6) of the local address must be the same as that of the peer address. [Example] Ge0/2

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



Item	Description	Remarks
Authentication Mode	Identity authentication mode of both ends of the tunnel. By default, pre-shared key authentication is used. In this mode, both ends perform hash calculation on packets using the pre-shared key. If the calculation results are the same, the authentication is successful.	N/A

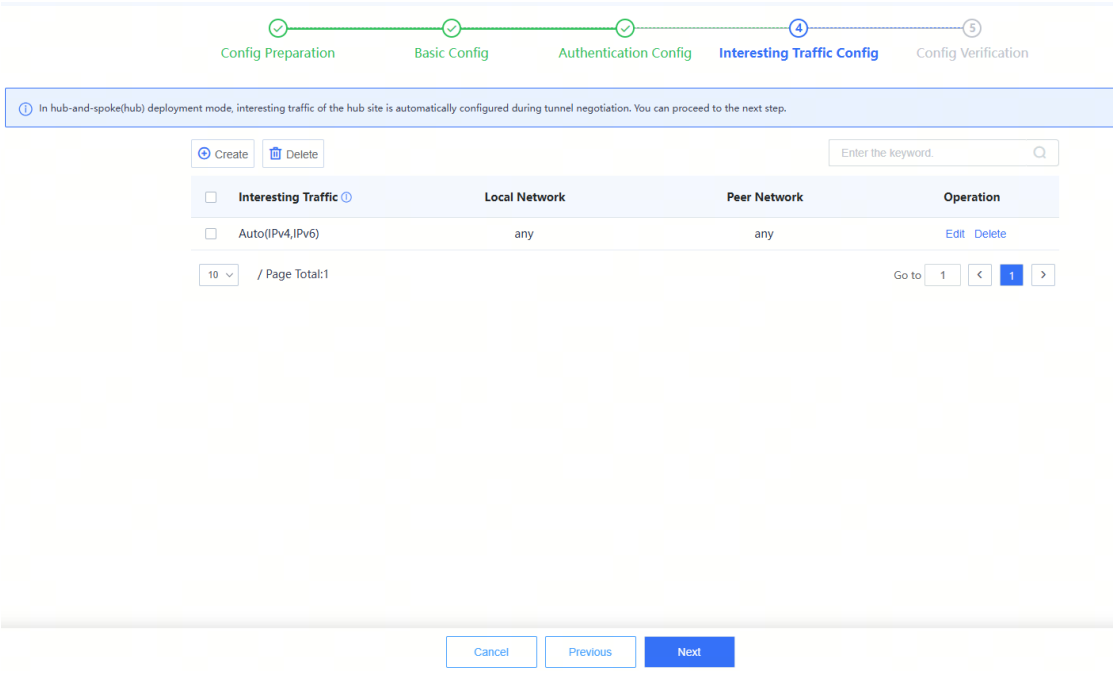
Item	Description	Remarks
Key	Key string for identity authentication in pre-shared key authentication mode.	Configure the same identity authentication mode (pre-shared key) and key for both ends. [Example] Ruijie123

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

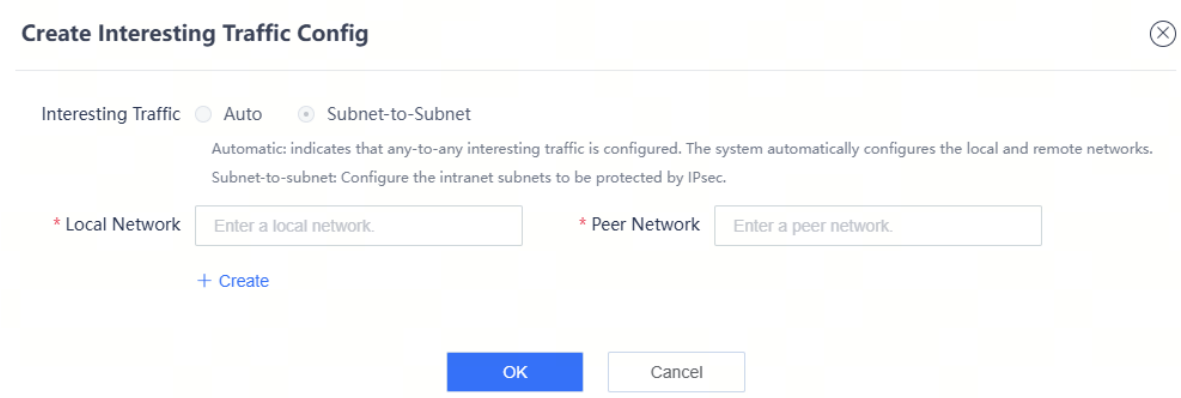
a In a site-to-site (spoke/site) deployment scenario, click **Create** to access the **Interesting Traffic Config** page.

Note

In a hub-and-spoke (hub) deployment scenario, the device automatically identifies and generates interesting traffic, and you need to check whether traffic meets actual networking requirements.



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



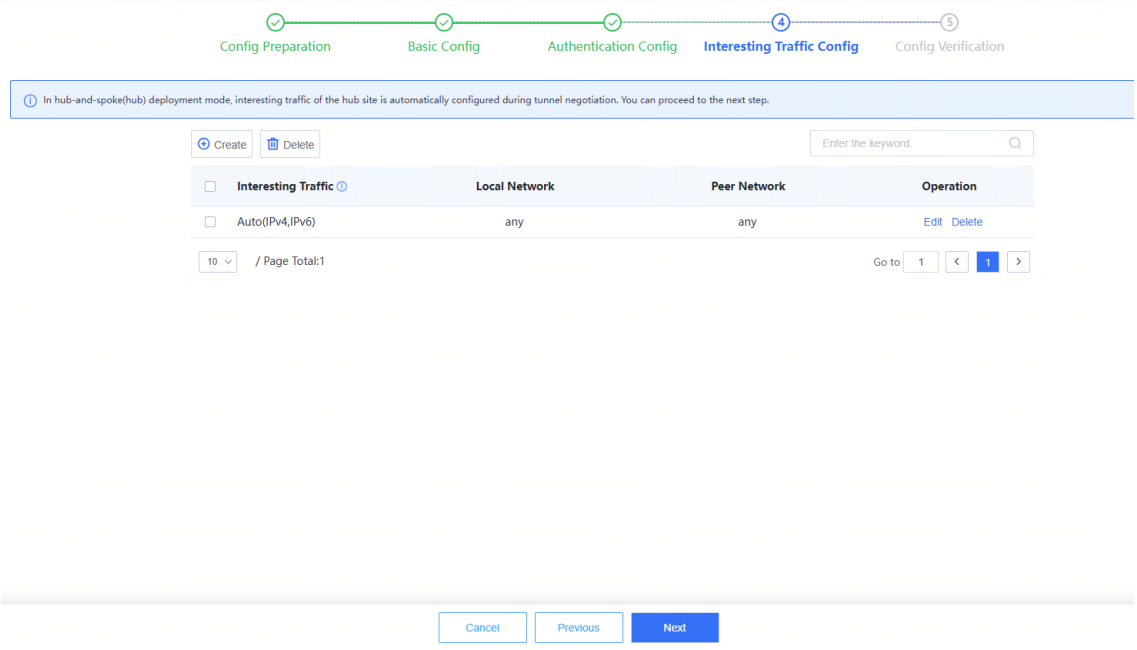
Item	Description	Remarks
Interesting Traffic	Set the proxy mode for interesting traffic based on the ranges of addresses at both ends of the tunnel that require secure mutual access: ● **Auto**: Traffic to be encrypted is automatically identified based on the interesting traffic defined at the peer end, and no configuration is performed at the local end. ● **Subnet-to-Subnet**: Data flows between two specific subnets are protected. The source and destination addresses of the data flows to be protected by IPsec must be manually configured.	● In the site-to-site (spoke/site) deployment mode, only interesting traffic of the "subnet-to-subnet" type can be configured, and the interesting traffic of the "automatic" type cannot be configured. ● The interesting traffic of IPsec tunnels to different sites cannot be the same; otherwise, VPN route conflicts will occur. The interesting traffic of active and standby IPsec tunnels to the same site can be the same. [Example] Subnet-to-Subnet
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: ● Automatic: the value is automatically set. ● Subnet-to-subnet: enter IP network segment or host address. Example: 192.168.1.0/255.255.255.0. 192.168.1.0/24 192.168.1.1 1234::100/128 1234::100

Item	Description	Remarks
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: ● Automatic: the value is automatically set. ● Subnet to subnet: enter an IP network segment or host address. Example: 192.168.1.0/255.255.255.0 192.168.1.0/24. 192.168.1.1 1234::100/128 1234::100

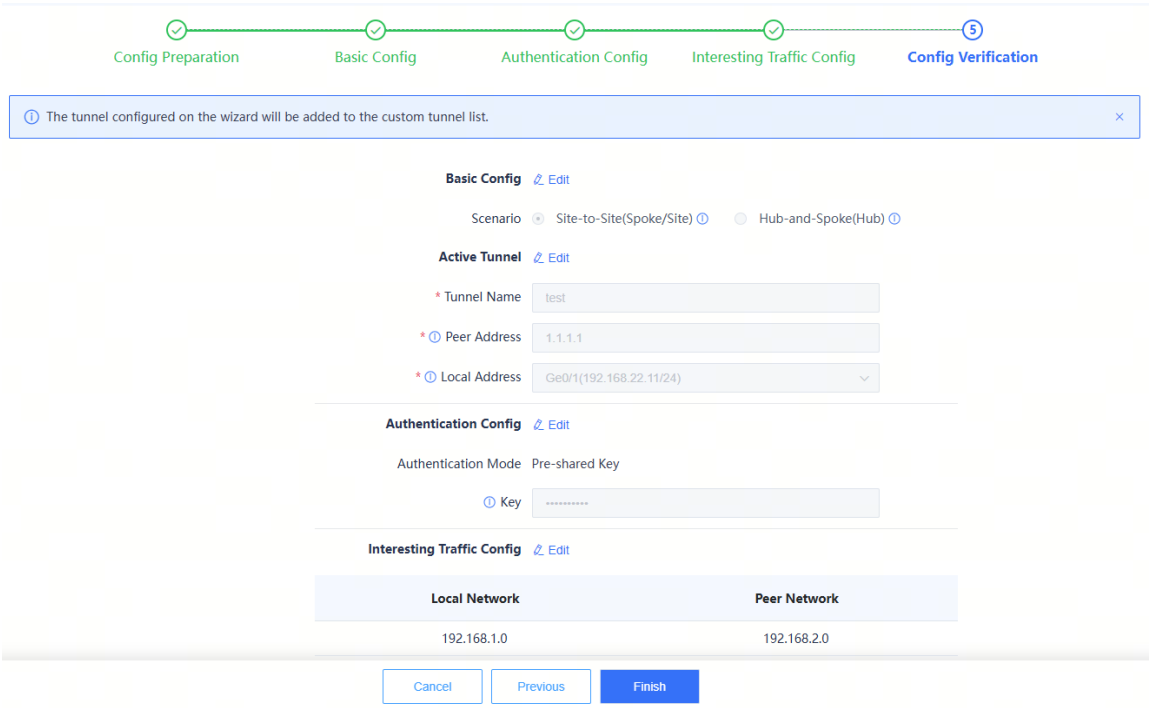
c Click **OK** to save interesting traffic configuration.

In the site-to-site (spoke/site) deployment mode, you can configure multiple interesting traffic entries of the subnet-to-subnet type. Click Add to add an interesting traffic entry.

In hub-and-spoke (hub) deployment mode, if there is interesting traffic of the automatic type, other interesting traffic does not take effect.



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

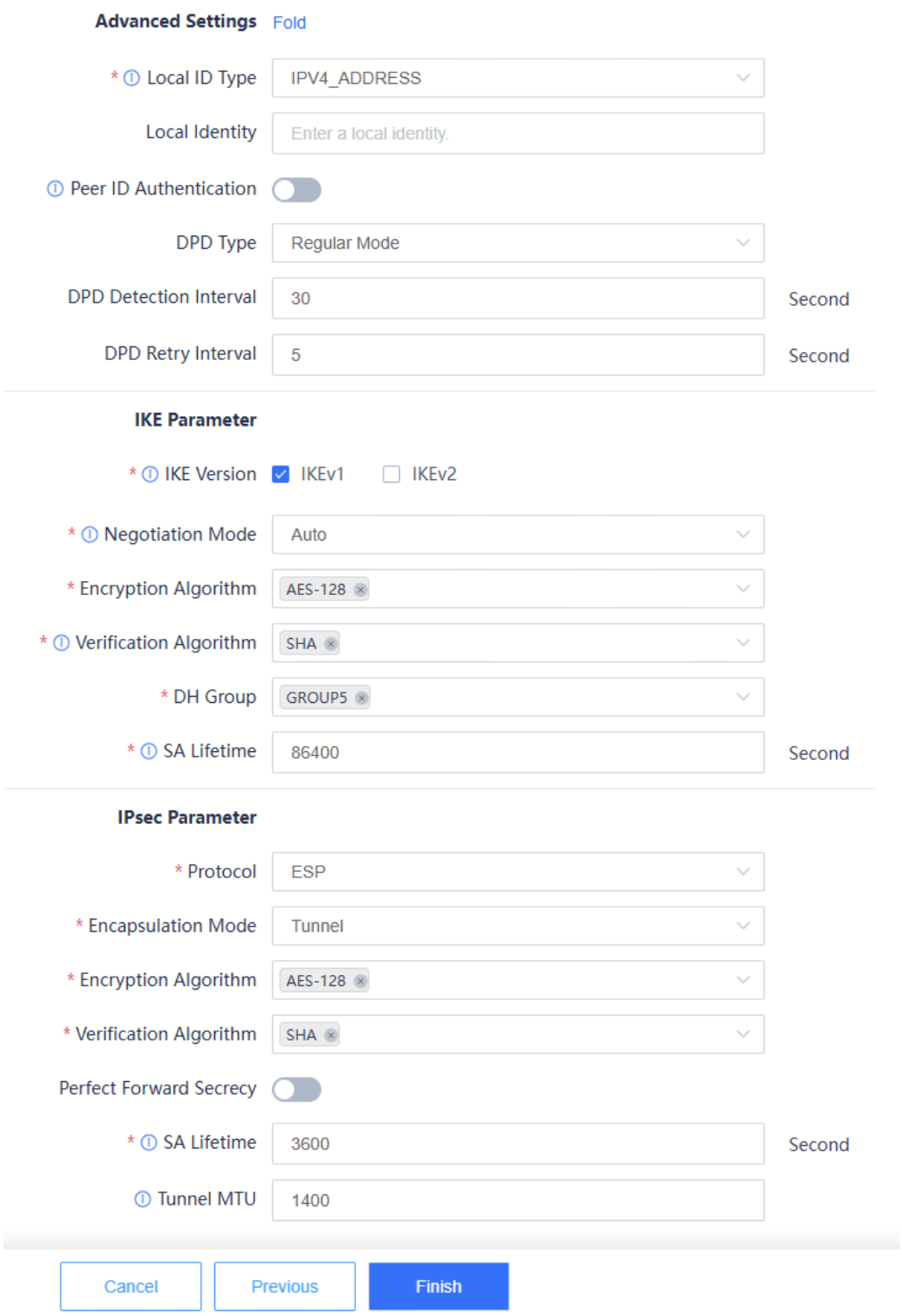


(6) (Optional) Set security parameters for IPsec tunnel negotiation in the **Advanced Settings** area.

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.



Item	Description	Remarks
Identity Authentication Parameters		

Item	Description	Remarks
Key Type	● **Single Key**: The same PSK is used for different spoke nodes to access the hub node. ● **Multiple Keys**: If the device functions as the hub node, each spoke node can use a different PSK for access, which is matched based on the ID.	In a P2MP scenario, the key type needs to be set on the hub node. [Example] Single Key
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: ● **IPV4_ADDRESS**: An IPv4 address is used as the local ID for IKE negotiation. ● **IPV6_ADDRESS**: An IPv6 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. ● **KEY_ID**: A specified key ID is used as the local ID for IKE negotiation.	● By default, the local IPv4 or IPv6 address is used as the local ID. ● When the local interface is of the PPPoE or DHCP type, you are advised to select **FQDN**, **IPV4_ADDRESS**, or **IPV6_ADDRESS**. (In this case, you cannot specify the **Local Identity** parameter.) [Example] IPV4_ADDRESS

Item	Description	Remarks

Local Identity	String that identifies the local device for identity authentication.	• 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:
		  ○ **FQDN**: Domain name of the local end. Example: **aaa.com**.
		  ○ **USER_FQDN**: User domain name of the local end in the format of *Username@Domain name*. Example: julia@aaa.com.
		  ○ **IPV4_ADDRESS**: Specifies the IPv4 address of the local end, for example, 6.6.6.2. If this parameter is not specified, the IPv4 address of the local interface is used by default. Keep this parameter empty if the local interface is of the PPPoE or DHCP type.
		  ○ **IPV6_ADDRESS**: IPv6 address of the local end. Example: 2002::2. If this parameter is not specified, the IPv6 address of the local interface is used by default. Keep this parameter empty if the local interface is of the PPPoE or DHCP type.
		  ○ **KEY_ID**: A specific string that identifies the local end, such as a vendor's private ID.

Peer ID 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
Peer ID Type	A peer ID identifies the peer device for identity authentication. The following types are supported: ● **IPV4_ADDRESS**: The peer end uses an IPv4 address as the peer ID for identity authentication. ● **IPV6_ADDRESS**: The peer end uses an IPv6 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. ● **KEY_ID**: The peer end uses a specified key ID as the peer ID for identity authentication.	● 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. [Example] IPV4_ADDRESS
Peer ID	String that identifies the peer device for identity authentication.	● 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: ○ **IPV4_ADDRESS**: IPv4 address of the peer end. Example: 10.1.1.1. ○ **IPV6_ADDRES**S: IPv6 address of the peer end. Example: 3002::2. ○ **FQDN**: Domain name of the peer end. Example: **bbb.com**. ○ **USER_FQDN**: User domain name of the peer end in the format of *Username@Domain name*. Example: **susan@bbb.com.** ○ **KEY_ID**: A specific string that identifies the peer end, such as a vendor's private ID.
Pre-shared Key	If the key type is single-key, the peer ID authentication function checks whether the peer ID is in the configured ID list. If not, the negotiation fails. If the key type is multi-key, the PSK configuration is added. The PSK is queried based on the ID.	● This parameter is available when key type is set to multi-key in hub-and-spoke (hub) deployment mode. ● In IKEv1 main mode, only the IPv4 address can be used to find the key. [Example] Test123

Item	Description	Remarks
DPD 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.		
DPD Type	Two DPD modes are supported: ● **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.	This parameter is supported in a site-to-site scenario. [Example] Idle Mode
DPD Detection Interval	In regular mode, set the interval between two DPD detections, in seconds.	The default value is 30 seconds. [Example] 30
DPD Retry Interval	Interval for retransmitting DPD messages. After sending a DPD request message, if the local end does not receive a response message within the retry interval, it retransmits the DPD request message. If the local end does not receive a response message after three retransmissions, it regards the peer end as unavailable and automatically removes the IPsec tunnel.	The default value is 5 seconds. [Example] 3
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, 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 spoke sites.		
Reverse Route Injection	Whether to enable reverse route injection.	[Example] Enable
Priority	Route priority. A larger value indicates a lower priority.	[Example] 5

Item	Description	Remarks
IKE Parameters 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. All of the following IKE parameters except **SA Lifetime** must have the same values in the IPsec VPN configuration of the peer device.		
IKE Version	IKE negotiation type.	If both IKEv1 and IKEv2 are selected, the firewall can respond to IKEv1 and IKEv2 negotiation requests, but can only initiate IKEv2 negotiation. [Example] IKEv1
Negotiation Mode	IKE negotiation mode in phase 1. The following modes are supported: ● **Auto**: The main mode or aggressive mode is used for responding to a negotiation request, and the main mode is used for initiating negotiation. ● **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
Pseudo-Random Algorithm	Set the pseudo-random function (PRF) algorithm used in IKE negotiation: ● **MD5**: MD5 algorithm that generates a 128-bit key ● **SHA**: SHA1 algorithm that generates a 160-bit key ● **SHA-256**: SHA2-256 algorithm that generates a 256-bit key ● **SHA-384**: SHA2-384 algorithm that generates a 384-bit key ● **SHA-512**: SHA2-512 algorithm that generates a 512-bit key Before exchanging keys, IKEv2 uses a PRF to encrypt keys, which enhances key exchange security. The security levels are as follows from high to low: SHA-512 > SHA-384 > SHA-256 > SHA > MD5.	● This parameter is required in IKEv2 negotiation. ● Click the input box and select one or more values from the drop-down list. ● SHA-256 is used by default. [Example] MD5

Item	Description	Remarks
Encryption Algorithm	Encryption algorithm used in IKE negotiation for establishing IPsec SAs. The following values are supported: ● **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 In order of security from high to low: AES-256 > AES-192 > AES-128 > 3DES > DES.	● 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 in IKE negotiation. The following values are supported: ● **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 A longer message digest indicates higher security and slower calculation.	● Select one or more options from the drop-down list. ● The default authentication algorithm is **SHA**. [Example] MD5
DH group	DH group used in IKE negotiation. The following values are supported: ● **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 The DH group determines the strength of the key used in IKE negotiation. A larger group number indicates higher security and slower key calculation.	● Select one or more options from the drop-down list. ● The default value is **GROUP5**. [Example] GROUP14

Item	Description	Remarks
SA Lifetime	IKE SA lifetime. When the lifetime of an IKE SA exceeds this value, the device replaces the old SA with a newly established SA. The actual IKE SA lifetime depends on the negotiation result of the two ends.	Range: 120–604800, in seconds. The default value is 86400 seconds (one day). [Example] 86400
IPsec Parameters 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. All of the following IPsec parameters except **SA Lifetime** must have the same values in the IPsec VPN configuration of the peer device.		
Protocol	Security protocol used by IPsec. Currently, only Encapsulating Security Payload (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: ● **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.	● Select one or more options from the drop-down list. ● The default encryption algorithm is **AES-128**. [Example] AES-192

Item	Description	Remarks
Authentication Algorithm	Authentication algorithm used by the IPsec tunnel. The following values are supported: ● **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 A longer message digest indicates higher security and slower calculation.	● Select one or more options from the drop-down list. ● The default authentication algorithm is **SHA**. [Example] MD5
Perfect Forward Secrecy	Whether to enable the Perfect Forward Secrecy (PFS) function. 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.	[Example] **Enable**
DH group	DH group used by PFS. The following values are supported: ● **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 A larger group number indicates higher security and slower key calculation.	● Select one or more options from the drop-down list. ● When PFS is enabled, **GROUP5** is set by default. [Example] GROUP14
SA Lifetime	IPsec SA lifetime. When the lifetime of an IPsec SA exceeds this value, the device replaces the old SA with a newly established SA. The actual IPsec SA lifetime depends on the negotiation result of the two ends.	● Range: 60–604800, in seconds. ● The default value is 3600 seconds (1 hour). [Example] 3000

Item	Description	Remarks
Tunnel MTU	Maximum number of bytes that can be transmitted over the IPsec tunnel at a time.	● The default value is 1400 bytes. ● The tunnel MTU must be smaller than the outbound interface MTU. [Example] 1480

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

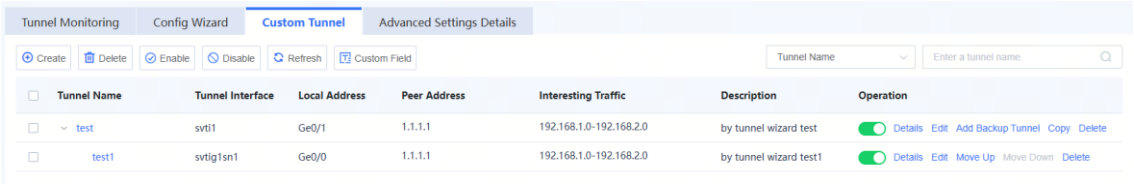
Follow-up Procedure

- If a tunnel is unreachable, you can diagnose and detect the fault cause by using IPsec VPN. For details, see 8.6.1 3. IPsec VPN Diagnosis.
- After you complete IPsec tunnel parameter configuration on the wizard, the system automatically synchronizes the following configurations to the firewall.

Item	Description
Address Object	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.
Security Zone	A security zone is added: ● **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.
VTI tunnel Interface	The IPsec tunnel interface is added: ● **Security Zone**: The value is the same as that of **Tunnel Name** set for the IPsec tunnel.
Static Routing	For a site-to-site IPsec tunnel, if the peer network address of the interesting traffic is configured with a specific IP subnet, the static route to the peer intranet is added: ● **Dest. IP Range/Mask**: Peer network address set in interesting traffic configuration. ● **Interface**: IPsec tunnel interface. ● **Priority**: 5
Intelligent Routing	For a site-to-site IPsec tunnel, if the peer network address of the interesting traffic is 0.0.0.0/0 or ::/0, the intelligent route to the peer intranet is added as follows: ● **Name**: The policy name starts with **IPsec_**. ● **Src. Address**: Local network address in the interesting traffic. ● **Dest. Address**: any ● **Egress Line**: IPsec tunnel interface.

Item	Description
Security Policy	Security policies are added to permit traffic from intranets at both ends of the tunnel in the inbound and outbound directions: ● Security policy in the inbound direction: ○ **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 (Any indicates all interfaces.) ○ **Dest. Address**: Local network address set in interesting traffic configuration. ○ **Action**: permit ● Security policy in the outbound direction: ○ **Src. Security Zone**: any (Any indicates all interfaces.) ○ **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	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. ● **Src. Security Zone**: any (Any indicates all interfaces.) ● **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 **Details** to view detailed negotiation parameters of the IPsec tunnel.
  - Click **Copy** to copy the current tunnel parameter configuration and modify it to create a tunnel.
  - Click **Edit** to modify tunnel configurations.
  - Click **Delete** to delete the IPsec tunnel policy.
  - Click **Add Backup Tunnel** to create a backup tunnel. Click the arrow in front of a tunnel name to expand the backup tunnels of the current tunnel. Tunnels in the list are sorted in descending order from top down, and the tunnel with the highest priority is the master tunnel. Click **Move Up** or **Move Down** to adjust the tunnel priority.
- To add or modify interesting traffic for a tunnel after it is created using the wizard, you need to manually add

or modify routes and security policies for the interesting traffic. Otherwise, IPsec VPN tunnel traffic may fail to be forwarded.

6.10.4 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 6.1.6 Configuring a Tunnel Interface.
- In a site-to-site 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.

Precautions

- Two tunnels (master and backup) can be configured between two sites, and the interesting traffic of the two tunnels can be the same. If the master tunnel fails, service data are automatically switched to the backup tunnel. The interesting traffic, authentication key, IKE parameters, and IPsec parameters of the master and backup tunnels must be the same.

  Note

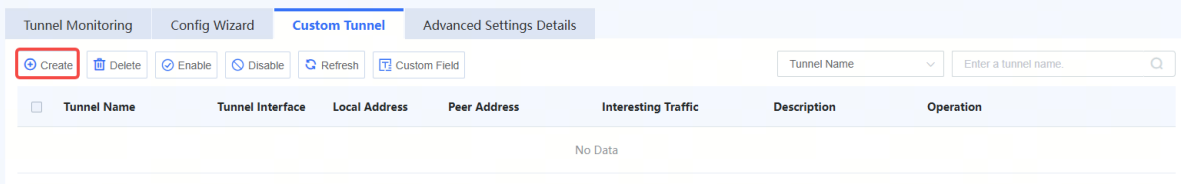
  After a tunnel is created in custom mode, you can click **Add Backup Tunnel** in the custom tunnel list to create a backup tunnel for the custom tunnel.

- If the device establishes IPsec tunnels with multiple sites simultaneously, you must configure different interesting traffic for different sites. For example, if Site A establishes two tunnels with Site B and Site C separately, the interesting traffic of the two tunnels cannot be the same. The device creates routes based on the interesting traffic. If the interesting traffic from Site A to Site B is the same as that from Site A to Site C, there are two routes to the same destination. When the device forwards packets based on the route priority,

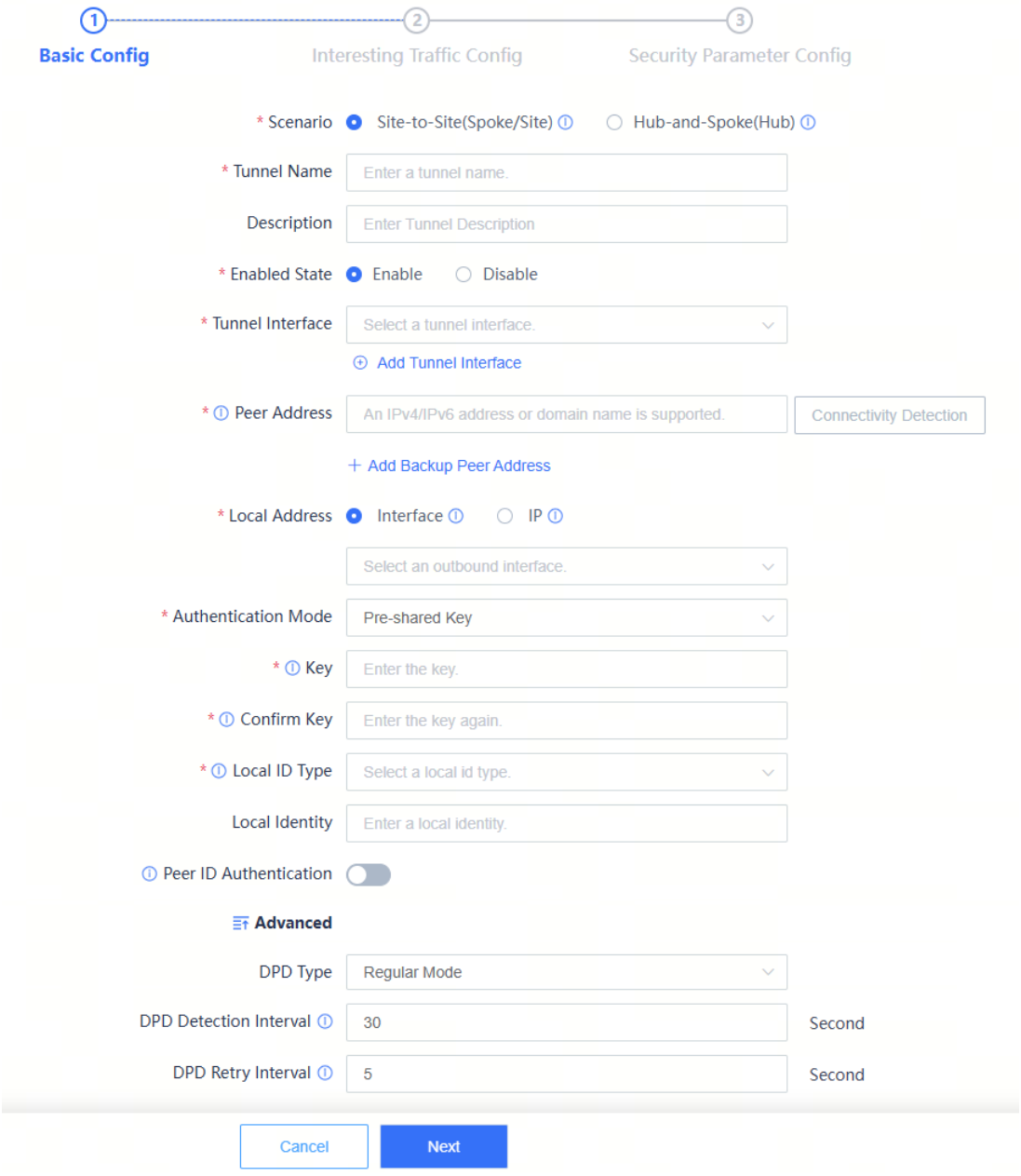
packets that should be forwarded over a tunnel may be forwarded to another tunnel, causing a service exception.

Procedure

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



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



Item	Description	Remarks
Scenario	Select the IPsec tunnel type based on the deployment scenario: ● **Site-to-Site (Spoke/Site)**: applies to scenarios where the peer end has a fixed IP address or domain name, such as IPsec VPN deployment at an enterprise spoke site. ● **Hub-and-Spoke (Hub)**: 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.	[Example] **Site-to-Site (Spoke/Site)**
Tunnel Name	IPsec tunnel name.	[Example] ipsec_1
Description	Tunnel description. Provide brief description to help the administrator understand the function of the tunnel.	[Example] Mutual access between spoke site at 11.1.1.2 and hub site at 10.1.1.2
Enabled State	Whether to enable the IPsec tunnel policy.	[Example] **Enable**
Tunnel Interface	Tunnel interface associated with the IPsec tunnel policy. IPsec data packets are encapsulated and decapsulated on this interface.	● Select a configured tunnel interface from the drop-down list. ● To add a tunnel interface, click **Add Tunnel Interface**. [Example] vti2

Item	Description	Remarks
Peer Address	IP address or domain name used by the peer device to establish the tunnel.	● You need to configure this parameter for the Site-to-Site (Spoke/Site) scenario. ● Enter an IP address or domain name and click **Connectivity Detection** to check whether there is a reachable route between devices at the two ends. ● Click **Add Backup Peer Address** to add a peer address. You can configure a maximum of three peer addresses. Peer addresses have a descending order of priority from top down. ● If the master address of the peer end is unavailable (such as unreachable address, tunnel negotiation failure, and detection timeout), the system automatically switches to a backup address of the peer end for tunnel establishment. If all the peer addresses of the current tunnel are unavailable, the current tunnel is faulty. In this case, if multiple master and backup tunnels are configured, the system automatically switches to another available tunnel based on the tunnel priority. ● The peer address must be the same as the value of the **Local Address** parameter configured on the peer device. [Example] 40.0.0.5
Local Address	Select the local interface or IP address for establishing a tunnel with the peer end.	● 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.
Authentication Mode	Identity authentication mode of both ends of the tunnel. Currently, only pre-shared key authentication is supported.	[Example] Pre-shared Key

Item	Description	Remarks
Key Type	● **Single Key**: The same PSK is used for different spoke nodes to access the hub node. ● **Multiple Keys**: If the device functions as the hub node, each spoke node can use a different PSK for access, which is matched based on the ID. If the corresponding key is not found based on the ID, the default key is used for verification.	In a P2MP scenario, the key type needs to be set on the hub node. [Example] Single Key
Key	Key string for identity authentication in pre-shared key authentication mode.	Configure the same identity authentication mode (pre-shared key) and key for both ends. [Example] Ruijie123
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: ● **IPV4_ADDRESS**: An IPv4 address is used as the local ID for IKE negotiation. ● **IPV6_ADDRESS**: An IPv6 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. ● **KEY_ID:** A specified key ID is used as the local ID for IKE negotiation.	● By default, the local IPv4 or IPv6 address is used as the local ID. ● When the local interface is of the PPPoE or DHCP type, you are advised to select **FQDN**, **IPV4_ADDRESS**, or **IPV6_ADDRESS**. (In this case, you cannot specify the **Local Identity** parameter.) [Example] IPV4_ADDRESS
Local Identity	String that identifies the local device for identity authentication.	● 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: ○ **IPV4_ADDRESS**: Specifies the IPv4 address of the local end. Example: 6.6.6.2 ○ **IPV6_ADDRESS**: IPv6 address of the local end. Example: 2002::2 ○ **FQDN**: Domain name of the local end. Example: **aaa.com** ○ **USER_FQDN**: User domain name of the local end in the format of *Username@Domain name*. Example: **julia@aaa.com** ○ **KEY_ID**: A specific string that identifies the local end, such as a vendor's private ID.

Item	Description	Remarks
Peer ID Authentication	Whether to authenticate the peer ID to verify the validity of the peer device.	• Toggle it on or off to enable or disable this function. • After enabling this function, click **Create** in the list to add identity authentication information for the peer device. • Multiple peer IDs can be added. The authentication is passed when any peer ID is matched. [Example] Enabled
Peer ID Type	A peer ID identifies the peer device for identity authentication. The following types are supported: • **IPV4_ADDRESS**: The peer end uses an IPv4 address as the peer ID for identity authentication. • **IPV6_ADDRESS**: The peer end uses an IPv6 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. • **KEY_ID**: The peer end uses a specified key ID as the peer ID for identity authentication.	• In the **Create Peer Identity** dialog box, select the ID type from the drop-down list. • 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. [Example] IPV4_ADDRESS

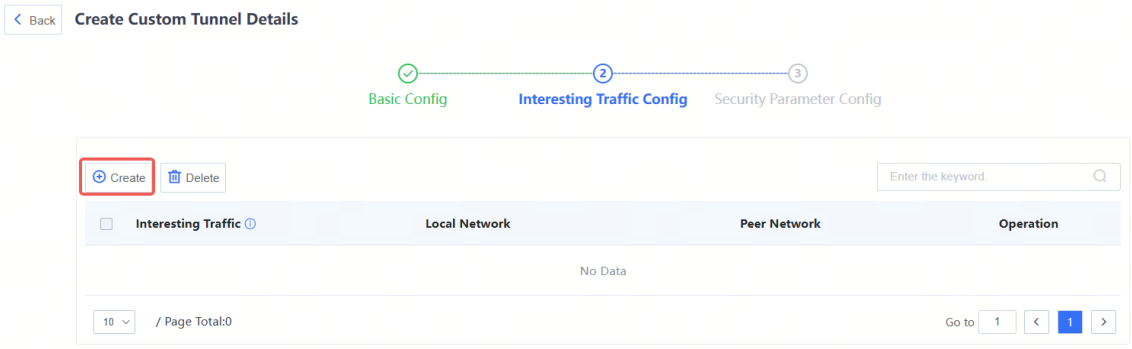
Peer ID	String that identifies the peer device for identity authentication.	• The value must be the same as that of **Local ID** configured for the peer device. Obtain the value from the administrator of the peer device.
		• In the **Create Peer Identity** dialog box, select the ID type, and enter the ID in the correct format.
		  ○ **IPV4_ADDRESS**: IPv4 address of the peer end. Example: 10.1.1.1.
		  ○ **IPV6_ADDRESS**: IPv6 address of the peer end. Example: 3002::1.
		  ○ **FQDN**: Domain name of the peer end. Example: **bbb.com**.
		  ○ **USER_FQDN**: User domain name of the peer end in the format of *Username@Domain name*. Example: **susan@bbb.com**.
		  ○ **KEY_ID**: A specific string that identifies the peer end, such as a vendor's private ID.

Item	Description	Remarks
Pre-shared Key	If the key type is single-key, the peer ID authentication function checks whether the peer ID is in the configured ID list. If not, the negotiation fails. If the key type is multi-key, the PSK configuration is added. The PSK is queried based on the ID.	This parameter is available when the key type is multi-key in hub-and-spoke (hub) deployment mode. In IKEv1 main mode, only the IPv4 address can be used to find the key. [Example] Test123
Advanced Click to expand advanced settings.		
DPD Type	DPD is used to detect peer status of an IPsec tunnel and remove abnormal tunnels in a timely manner. Two DPD modes are supported: ● **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.	This parameter is supported in a site-to-site scenario. [Example] Idle Mode
DPD Detection Interval	In regular mode, set the interval between two DPD detections, in seconds.	The default value is 30 seconds. [Example] 30
DPD Retry Interval	Interval for retransmitting DPD messages. After sending a DPD request message, if the local end does not receive a response message within the retry interval, it retransmits the DPD request message. If the local end does not receive a response message after three retransmissions, it regards the peer end as unavailable and automatically removes the IPsec tunnel.	The default value is 5 seconds. [Example] 3
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 hub-and-spoke scenario. [Example] Enable

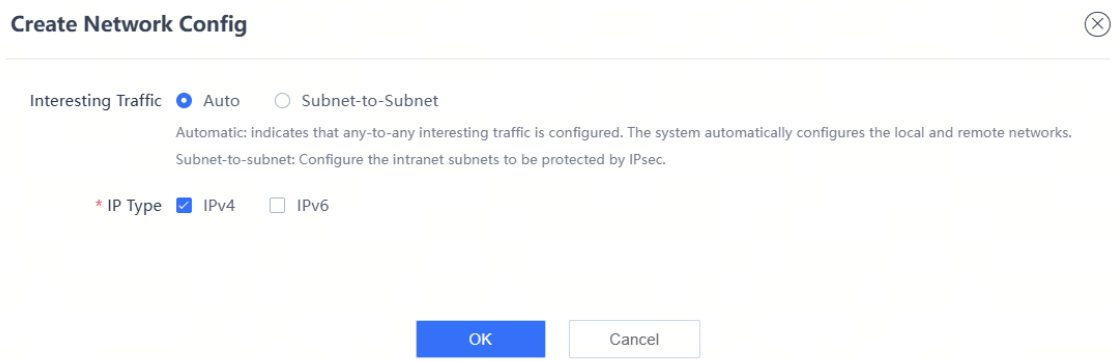
Item	Description	Remarks
Priority	Route priority.	This parameter takes effect only when reverse route injection is enabled. [Example] 5

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

a Click **Create** to access the **Create Network 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.

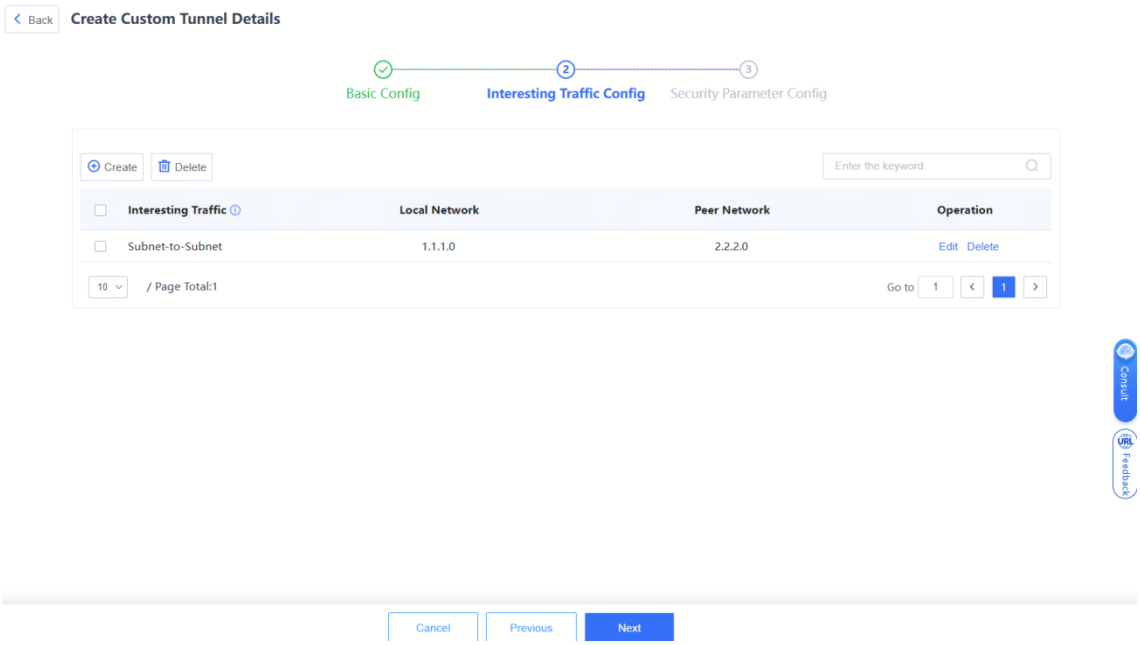


Item	Description	Remarks
Interesting Traffic	Set the proxy mode for interesting traffic based on the ranges of addresses at both ends of the tunnel that require secure mutual access: ● **Auto**: Traffic to be encrypted is automatically identified based on the interesting traffic defined at the peer end, and no configuration is performed at the local end. ● **Subnet-to-Subnet:** Data flows between two specific subnets are protected. The source and destination addresses of the data flows to be protected by IPsec must be manually configured.	[Example] Subnet-to-Subnet
Interesting Traffic: Auto		
IP Type	Set the IP address type of data flows to be protected.	[Example] IPv4,IPv6
Interesting Traffic: Subnet-to-Subnet		
Local Network	Source address of interesting traffic. Typically, a network segment or specific host address to be protected on the local intranet is set.	[Example] ● 192.168.1.0/255.255.255.0 ● 192.168.1.0/24 ● 192.168.1.1 ● 1234::100 ● 1234::100/128
Peer Network	Destination address of interesting traffic. Typically, a network segment or specific host address to be protected on the peer intranet is set.	[Example] ● 192.168.1.0/255.255.255.0 ● 192.168.1.0/24 ● 192.168.1.1 ● 1234::100 ● 1234::100/128

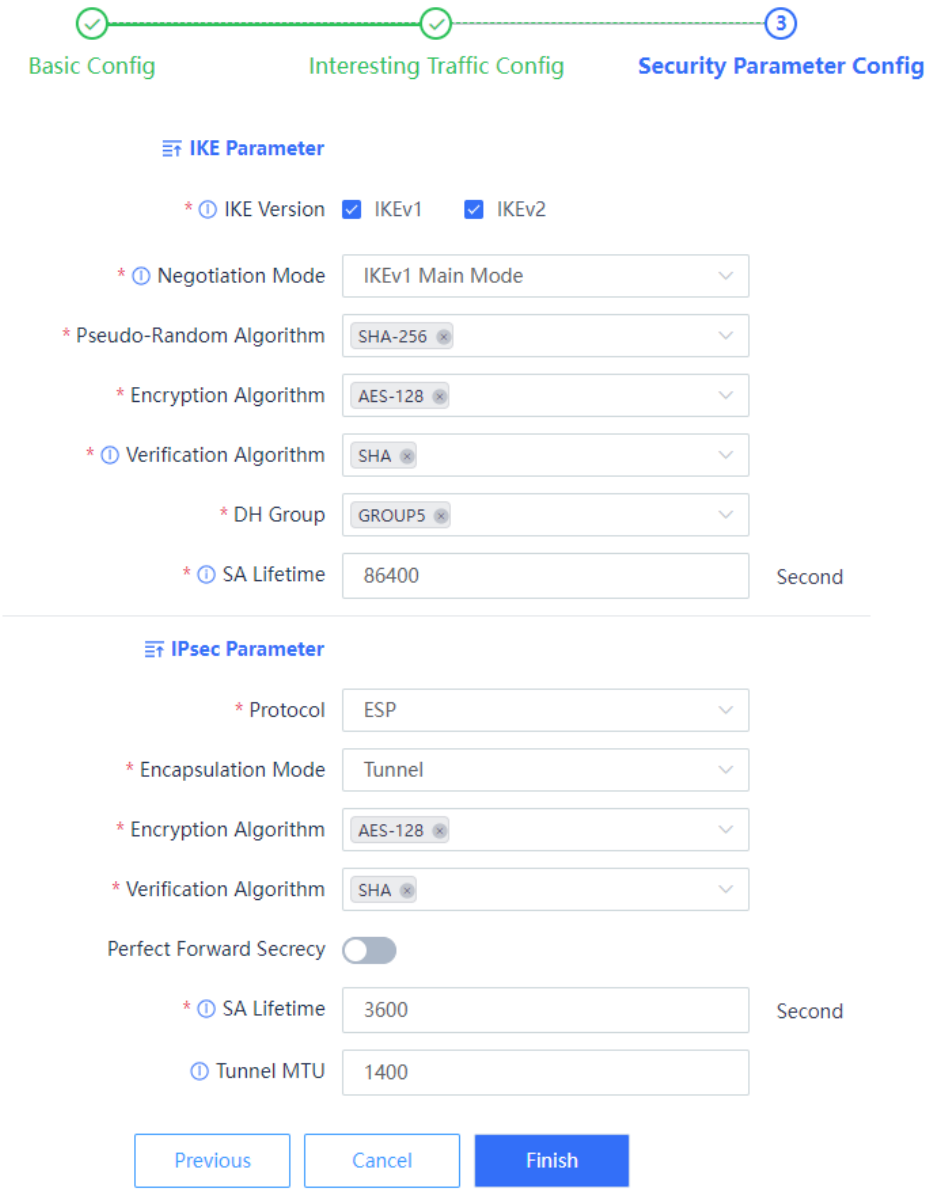
c Click **OK** to save interesting traffic configuration.

You can configure multiple interesting traffic entries of the subnet-to-subnet type. Click Create to add an entry.

If an interesting traffic entry of the automatic type exists, interesting traffic entries of the subnet-to-subnet type do not take effect.



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



Item	Description	Remarks
IKE Parameters 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. All of the following IKE parameters except **SA Lifetime** must have the same values in the IPsec VPN configuration of the peer device.		

Item	Description	Remarks
IKE Version	IKE negotiation type.	If both IKEv1 and IKEv2 are selected, the firewall can respond to IKEv1 and IKEv2 negotiation requests, but can only initiate IKEv2 negotiation. [Example] IKEv1
Negotiation Mode	IKE negotiation mode in phase 1. The following modes are supported: ● **Auto**: The main mode or aggressive mode is used for responding to a negotiation request, and the main mode is used for initiating negotiation. ● **IKEv1 Main Mode**: In this mode, identity information is encrypted and protected for higher security. ● I**KEv1 Aggressive Mode**: In this mode, the negotiation speed is faster, but identity information is not encrypted or protected.	[Example] IKEv1 Main Mode
Pseudo-Random Algorithm	Set the PRF algorithm used in IKE negotiation: ● **MD5**: MD5 algorithm that generates a 128-bit key ● **SHA**: SHA1 algorithm that generates a 160-bit key ● **SHA-256**: SHA2-256 algorithm that generates a 256-bit key ● **SHA-384**: SHA2-384 algorithm that generates a 384-bit key ● **SHA-512**: SHA2-512 algorithm that generates a 512-bit key Before exchanging keys, IKEv2 uses a PRF to encrypt keys, which enhances key exchange security. The security levels are as follows from high to low: SHA-512 > SHA-384 > SHA-256 > SHA > MD5.	● This parameter is required in IKEv2 negotiation. ● Click the input box and select one or more items from the drop-down list. ● SHA-256 is used by default. [Example] MD5

Item	Description	Remarks
Encryption Algorithm	Encryption algorithm used in IKE negotiation for establishing IPsec SAs. The following values are supported: ● **DES**: DES algorithm using 56-bit **keys** ● 3DES: 3DES algorithm using 168-bit keys ● **AES-128**: AES algorithm using 128-bit keys ● **AES-19**2: AES algorithm using 192-bit keys ● **AES-256**: AES algorithm using 256-bit keys In order of security from high to low: AES-256 > AES-192 > AES-128 > 3DES > DES.	● 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 in IKE negotiation. The following values are supported: ● **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 A longer message digest indicates higher security and slower calculation.	● Select one or more options from the drop-down list. ● The default authentication algorithm is **SHA**. [Example] MD5
DH group	DH group used in IKE negotiation. The following values are supported: ● **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 The DH group determines the strength of the key used in IKE negotiation. A larger group number indicates higher security and slower key calculation.	● Select one or more options from the drop-down list. ● The default value is **GROUP5**. [Example] GROUP14

Item	Description	Remarks
SA Lifetime	IKE SA lifetime. The actual IKE SA lifetime depends on the negotiation result of the two ends.	● Range: 120–604800, in seconds. ● The default value is 86400 seconds (one day). [Example] 86400
IPsec Parameters 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. All of the following IPsec parameters except **SA Lifetime** must have the same values in the IPsec VPN configuration of the peer device.		
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: ● **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.	● Select one or more options from the drop-down list. ● The default encryption algorithm is **AES-128**. [Example] AES-192

Item	Description	Remarks
Authentication Algorithm	Authentication algorithm used by the IPsec tunnel. The following values are supported: ● **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 A longer message digest indicates higher security and slower calculation.	● Select one or more options from the drop-down list. ● The default authentication algorithm is **SHA**. [Example] MD5
Perfect Forward Secrecy	Whether to enable the PFS function. 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.	[Example] **Enable**
DH group	DH group used by PFS. The following values are supported: ● **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 A larger group number indicates higher security and slower key calculation.	● Select one or more options from the drop-down list. ● When PFS is enabled, **GROUP5** is set by default. [Example] GROUP14
SA Lifetime	IPsec SA lifetime. When the lifetime of an IPsec SA exceeds this value, the device replaces the old SA with a newly established SA. The actual IPsec SA lifetime depends on the negotiation result of the two ends.	● Range: 60–604800, in seconds. ● The default value is 3600 seconds (1 hour). [Example] 3000

Item	Description	Remarks
Tunnel MTU	Maximum number of bytes that can be transmitted over the IPsec tunnel at a time.	The default value is 1400 bytes. The tunnel MTU must be smaller than the outbound interface MTU. [Example] 1480

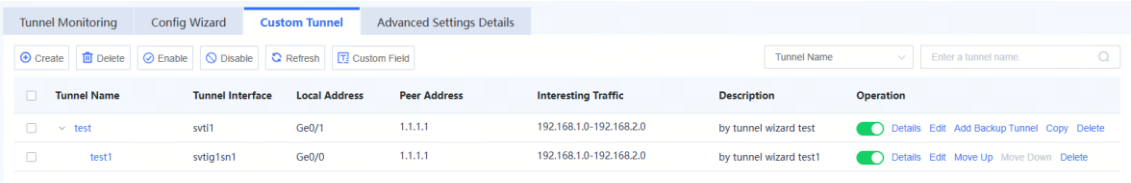
(5) After verifying the configurations, click **Finish** to save the configurations. To modify the configurations, click **Previous**.

Follow-up Procedure

- If a tunnel is unreachable, you can diagnose and detect the fault cause by using IPsec VPN. For details, see 8.6.1 3. IPsec VPN Diagnosis.
- 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.	● **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:	● Security policy in the inbound direction: ○ **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: ○ **Src. Security Zone**: any (Any indicates all interfaces.) ○ **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 **Details** to view detailed negotiation parameters of the IPsec tunnel.
- Click **Copy** to copy the current tunnel parameter configuration and modify it to create a tunnel.
- Click **Edit** to modify tunnel configurations.
- Click **Delete** to delete the IPsec tunnel policy.
- Click **Add Backup Tunnel** to create a backup tunnel. Click the arrow in front of a tunnel name to expand the backup tunnels of the current tunnel. Tunnels in the list are sorted in descending order from top down, and the tunnel with the highest priority is the master tunnel. Click **Move Up** or **Move Down** to adjust the tunnel priority.

Caution

The tunnel interface and local address of a backup tunnel cannot be the same as those of an existing tunnel.

6.10.5 Advanced Settings

Application Scenario

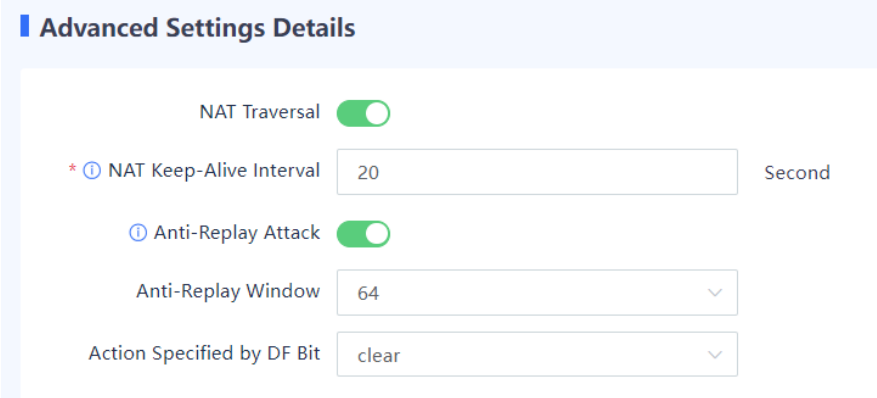
You can configure advanced settings for IPsec VPN to meet VPN function requirements in different scenarios.

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** > **VPN Mgmt** > **IPsec VPN** > **Advanced Settings Details**.

(2) Modify the advanced settings of IPsec VPN.



Item	Description	Remarks
NAT Traversal	Whether to enable NAT traversal. When this function is enabled, the device adds a standard UDP header between the new IP header and ESP header of 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.	● This parameter takes effect only when **NAT Traversal** is enabled. ● The default NAT keep-alive interval is 20 seconds. [Example] 20 seconds
Anti-Replay Attack	Whether to enable the anti-replay attack function. A replay attack occurs when an attacker obtains and sends packets that have been received by the target host to deceive the host. When this function is enabled, IPsec detects replay packets through the anti-replay window mechanism and discards these packets before decapsulating them. 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.	Enabled by default. [Example] Enable

Item	Description	Remarks
Anti-Replay Window	Anti-replay window size. The following values are supported: 64, 128, 256, and 1024. 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.	● 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. [Example] 64
Action Specified by DF Bit	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: ● **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.	● 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. [Example] clear

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

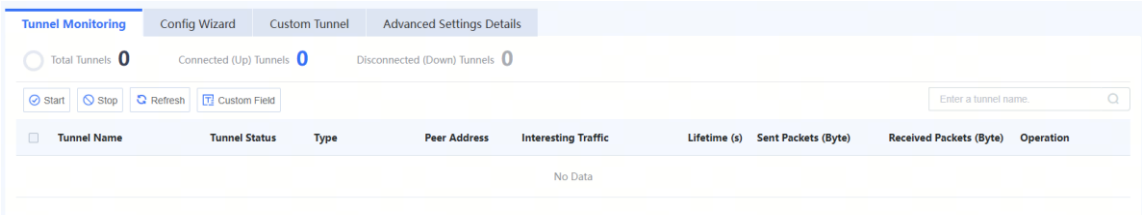
6.10.6 Tunnel Monitoring

Application Scenario

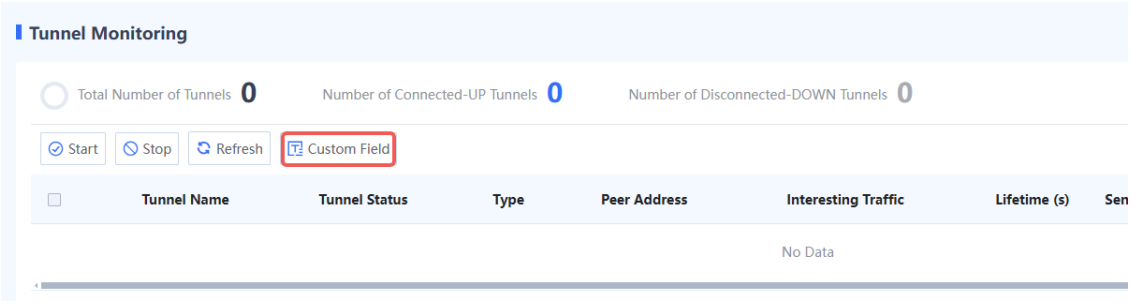
By using this function, the administrator can view configuration and status information about all IPsec tunnels to check whether IPsec VPN is working properly. In addition, the IPsec tunnels can be enabled or disabled.

Procedure

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



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



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

Item	Description
Tunnel Name	IPsec tunnel name.
Tunnel Status	Tunnel status, indicating whether IPsec tunnel negotiation is completed and whether the tunnel is successfully established.
Type	Tunnel type.
Peer Address	Peer IP address of the tunnel.
Interesting Traffic	Source and destination addresses of the data flows to be encrypted and transmitted over the tunnel.
Lifetime (s)	Remaining lifetime of the current IPsec SA. After the IPsec SA lifetime expires, the device replaces the old SA with a newly negotiated SA and updates the tunnel connection.
Sent Packets (Byte)	Total number of bytes that the local end sends to the IPsec tunnel.
Received Packets (Byte)	Total number of bytes that the local end receives from 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 hub-and-spoke 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 spoke sites simultaneously. The administrator can view the running status and connection information of the data transmission channels established between the device and spoke 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**.
- Click **Diagnose** in the **Operation** column of a tunnel to access the diagnosis center page for tunnel fault diagnosis. For details, see 8.6.1 3. IPsec VPN Diagnosis.

6.10.7 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 8.3.2 8. Querying IPsec VPN Logs.

6.11 DNS

6.11.1 Configuring DNS Server

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.

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.

You can configure IPv4 and IPv6 DNS servers on the device.

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.

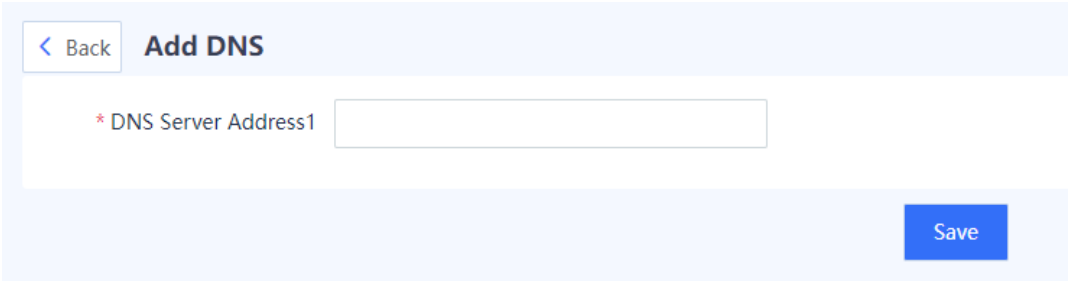
Procedure

(1) Choose **Network** > **DNS** > **DNS** and click the **DNS Config** tab.

(2) Set the IP address of DNS server 1.

a Click **Create**.

The **Add DNS** page is displayed.



b Set **DNS Server Address1** to the IPv4 or IPv6 address of the first DNS server.

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.

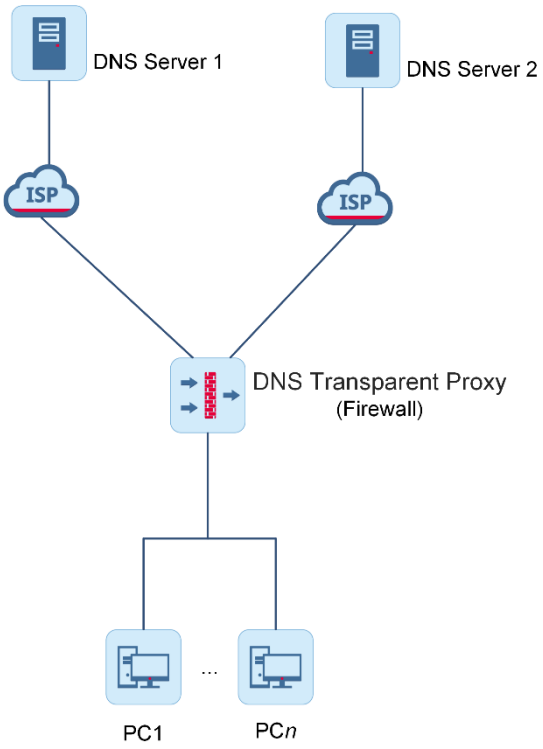
6.11.2 Configuring DNS Transparent Proxy

1. Overview

Typically, a DNS transparent proxy is deployed between DNS servers and user PCs to process DNS requests from users. For DNS request packets that hit the DNS transparent proxy policy, the device modifies the destination address (DNS server address) in a DNS request packet based on the outbound interface selected according to the packet. In this way, the DNS request packets can be forwarded to different DNS servers for resolution, and Internet access traffic can be forwarded over different links, fully leveraging link resources.

DNS transparent proxy is typically used in scenarios where the egress line includes services from multiple ISPs.

If both DNS forward proxy and DNS proxy are enabled on the device, DNS forward proxy takes precedence over DNS proxy.



The data processing process of DNS transparent proxy is as follows:

(1) When receiving a DNS request packet, the device checks whether DNS proxy is enabled. If not, the device does not perform DNS transparent proxy. If so, the device matches the DNS request packet against the proxy policy.

(2) The device checks whether the packet matches the DNS transparent proxy policy. If not, DNS transparent proxy is not performed. If so, the device proceeds to step (3).

(3) The device selects an available outbound interface for the DNS request packet.

If multiple routing configurations exist, the priorities in descending order are as follows: domain name-based routing (intelligent routing), excluded domain name, static route, ISP address library-based routing, and default route.

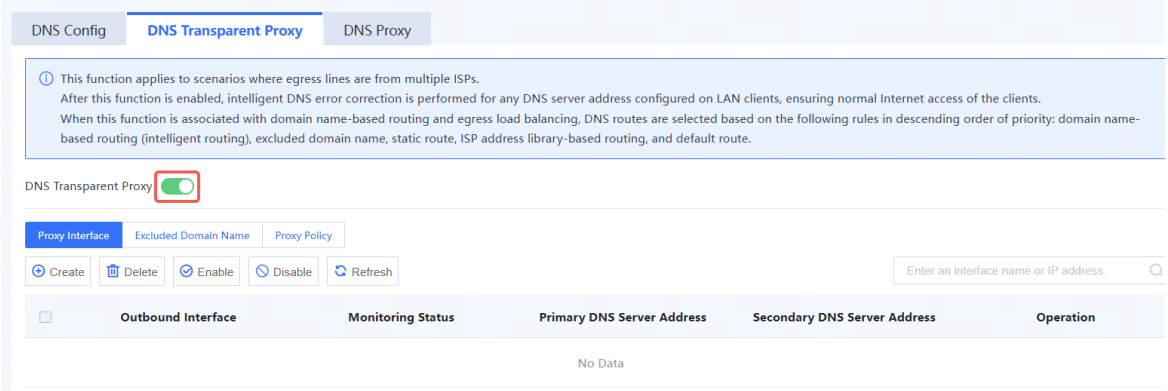
(4) On the device, each outbound interface can be bound to two DNS servers (primary DNS server and secondary DNS server). The DNS transparent proxy function preferentially uses the address of the primary DNS server as the destination address in a DNS request packet. When the primary DNS server is unavailable, the address of the secondary DNS server is used. The device performs DNS transparent proxy only when the outbound interface is bound to an available DNS server and a proxy flag exists in the DNS request packet.

2. Creating a DNS Transparent Proxy

Procedure

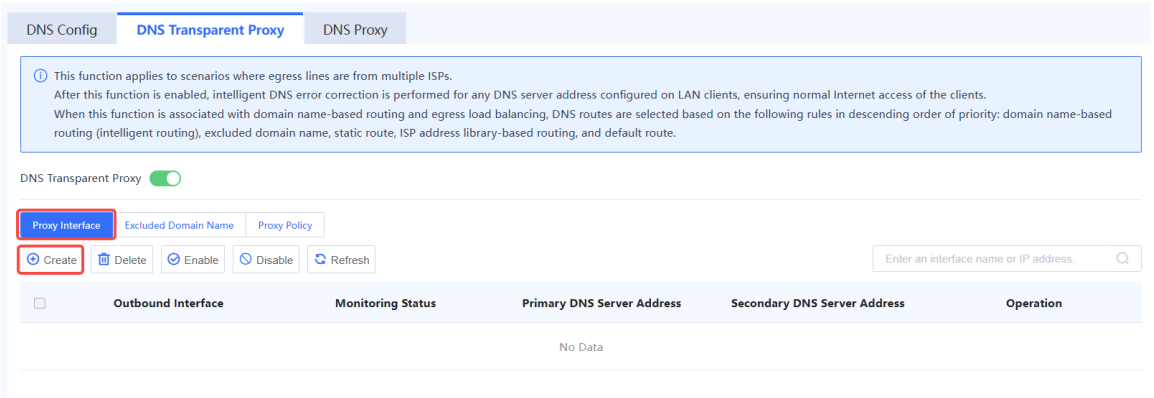
(1) Choose **Network** > **DNS** > **DNS** and click the **DNS Transparent Proxy** tab.

(2) Toggle on the switch to enable DNS transparent proxy.

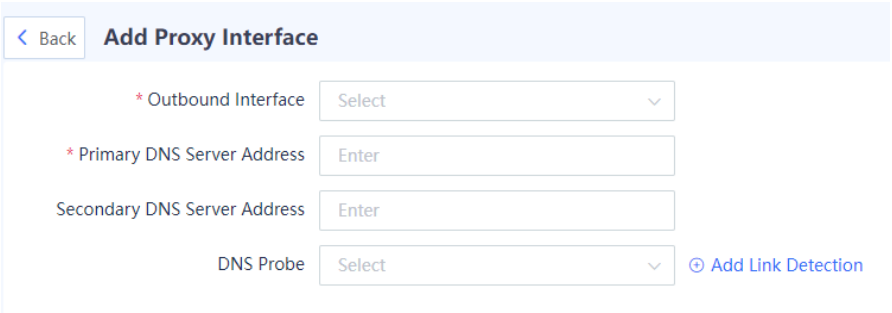


(3) Configure a proxy interface.

a Click **Create**.



b Create a DNS proxy interface.



Item	Description	Remarks
Outbound Interface	Outbound interface of DNS request packets.	[Example] Ge0/7
Primary DNS Server Address	Address of the primary DNS server bound to the outbound interface.	If the interface connection type is DHCP or PPPoE, the DNS server address with the highest priority on the device is automatically set after the outbound interface is configured. You can also manually enter or modify the DNS server address. If the interface connection type is static address, you need to manually configure the DNS server address.
Secondary DNS Server Address	Address of the secondary DNS server bound to the outbound interface. The secondary DNS server address is used only when the primary DNS server is unreachable.	If the interface connection type is DHCP or PPPoE, the DNS server address with the priority value 2 on the device is automatically set after the outbound interface is configured. You can also manually enter or modify the DNS server address. If the interface connection type is static address, you need to manually configure the DNS server address.
DNS Probe	Select or create DNS link detection. The detection result is displayed in the lower part of the page. For link detection, the minimum number of survivability nodes needs to be configured. In primary/secondary DNS link detection, if the minimum number of survivability nodes is 1, the detection result is normal when at least one node is available. After DNS proxy is associated with link detection, the secondary DNS server is used when the primary DNS server is unreachable.	For details about link detection, see 6.14 Link Detection.

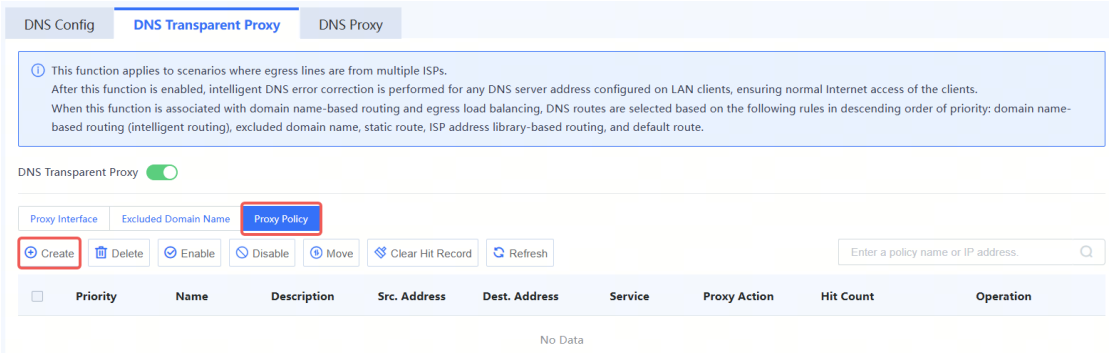
Note

If the address type of the outbound interface is different from that of the DNS server configured in the system (for example, only an IPv4 address is configured for the outbound interface, but an IPv6 DNS server address is configured in the system), the system does not automatically fill in the DNS server address.

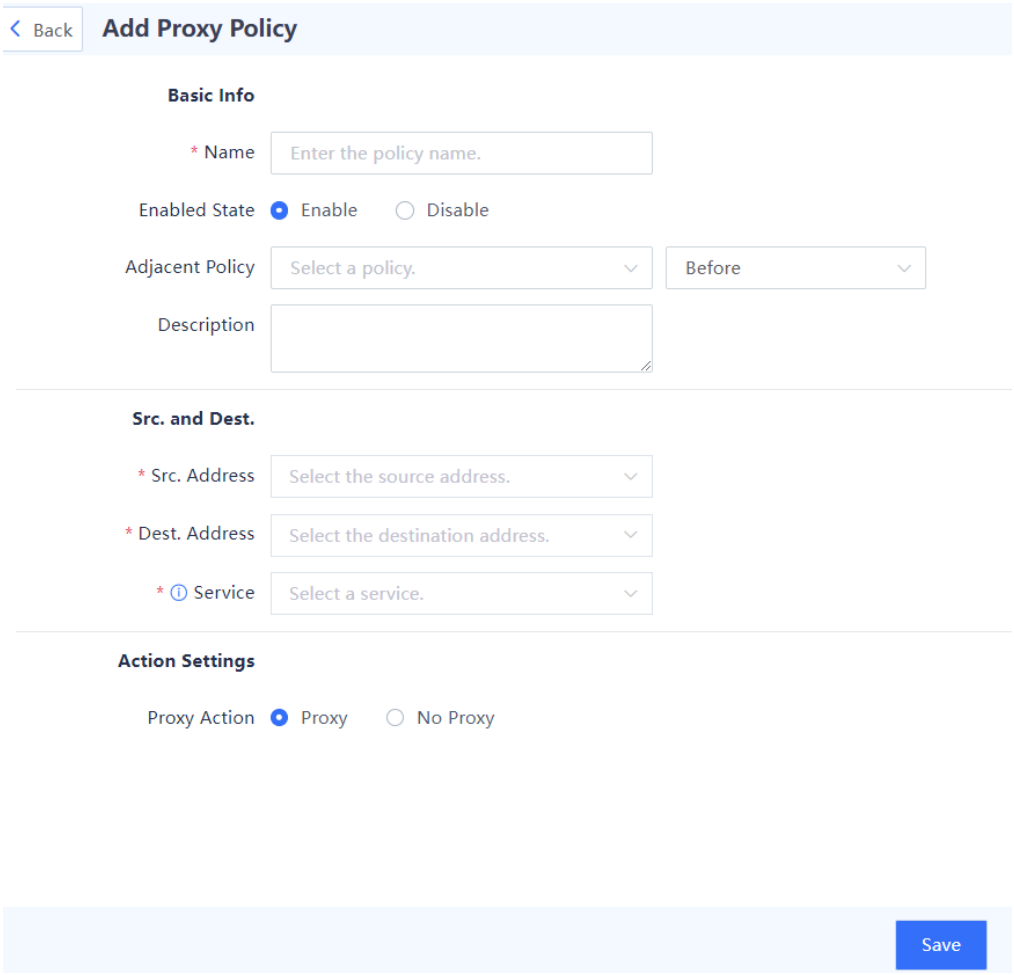
c Click **Save**.

(4) Configure a proxy policy.

a Click **Create**.



b Configure a proxy policy.



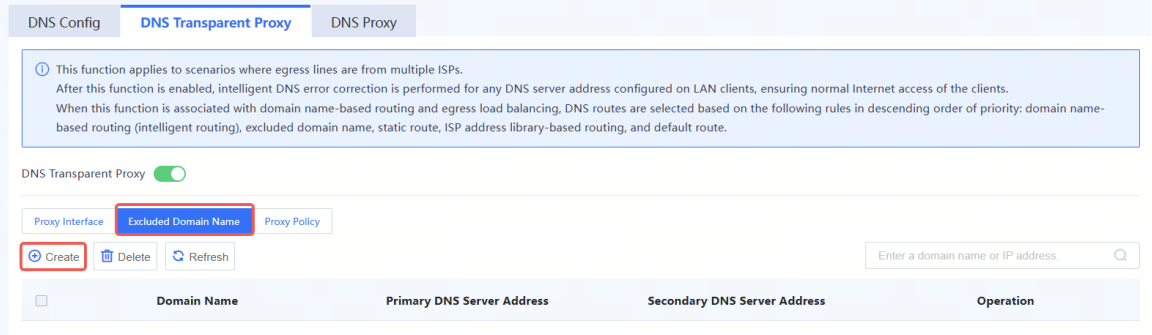
Item	Description	Remarks
Basic Info		
Name	Name of the DNS proxy policy.	[Example] DNS_Proxy
Enabled State	Whether to enable the DNS proxy policy.	[Example] Enable
Adjacent Policy	Move the new policy before or after the specified policy. The closer a policy is to the front, the higher its priority in matching.	Select a value from the drop-down list.
Description	Description of the proxy policy.	[Example] Proxy policy
Src. and Dest.		

Item	Description	Remarks
Src. Address	Source address of a DNS request packet.	● 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. ● Click **Add Address** or **Add Address Group** to add a source address. [Example] any
Dest. Address	Destination address of a DNS request packet.	● 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. ● Click **Add Address** or **Add Address Group** to add a destination address. [Example] any
Service	Service type of a DNS request packet.	● Click the drop-down list, and select a service in the **To-be-selected** area. The selected service is automatically added to the **Selected** area. ● Click **Add Service** or **Add Service Group** to add a service. [Example] dns-t
Action Settings		
Proxy Action	Whether to enable DNS transparent proxy for DNS request packets.	[Example] Proxy

c Click **Save**.

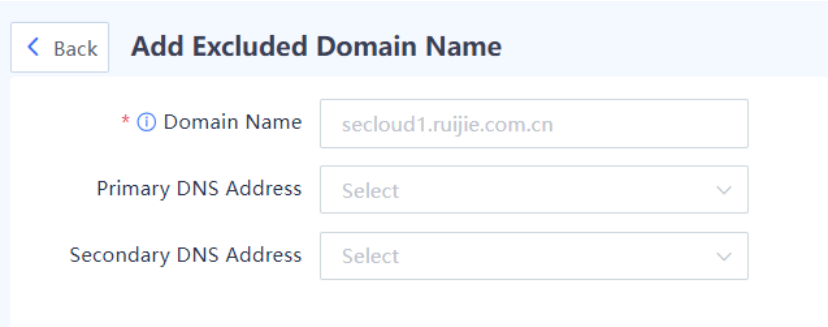
(5) Configure excluded domain names.

a Click **Create**.



b Add an excluded domain name.

In some scenarios, after the DNS transparent proxy function is enabled, special processing on specific domain names is required for network resource utilization or security reasons. For example, traffic needs to be forwarded to an ISP link with better network quality, or traffic does not require DNS proxy (with no DNS server address configured). In this case, you can add excluded domain names so that packets with the specific domain names can be processed accordingly when the proxy function is enabled.



Item	Description	Remarks
Domain Name	DNS domain name exclusion provides three matching modes: ● Exact match: Enter the complete domain name, such as www.ruijie.com. ● Prefix match: Enter an incomplete domain name ended with an asterisk (*), for example, www.ruijie.*. ● Suffix match: Enter an incomplete domain name started with an asterisk (*), for example, *.ruijie.com. The matching priorities in descending order are as follows: exact match, suffix match, and prefix match. Fuzzy match in other formats is not supported.	[Example] www.test.com
Primary DNS Address	Address of the primary DNS server specified for the domain name to be excluded. If the DNS server for resolving the domain name is modified, the device changes the destination address of corresponding DNS request packets to the specified DNS server address.	Select a DNS server address configured for the proxy interface from the drop-down list.
Secondary DNS Address	Address of the secondary DNS server specified for the domain name to be excluded.	Select a DNS server address configured for the proxy interface from the drop-down list.

c Click **Save**.

Follow-up Procedure

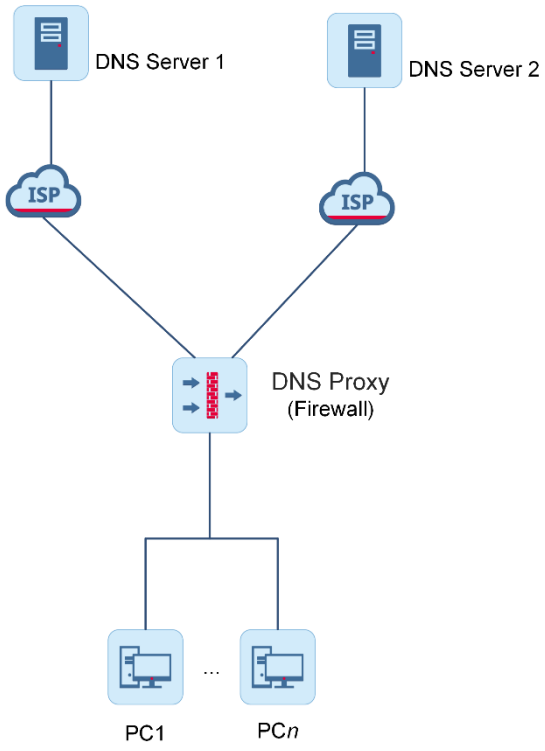
- Click **Create** to add more proxy interfaces, excluded domain names, or proxy policies.
- Click **Delete** to delete a specified proxy interface, excluded domain name, or proxy policy.
- Click **Enable** to enable a proxy interface or proxy policy. Click **Disable** to disable a proxy interface or proxy policy.
- Click **Move** to change the location of a specified proxy policy. The closer a policy is to the front, the higher its priority in matching.
- Select a policy and click **Clear Hit Record** to clear the hit statistics for the policy.
- Click **Refresh** to obtain the latest configuration of proxy interfaces, excluded domain names, and proxy policies.

6.11.3 Configuring DNS Proxy

1. Overview

A DNS proxy is typically deployed between a DNS server and a PC to process domain name resolution requests from the PC. Intranet users need to set the DNS server address to the IP address of the proxy interface. When receiving a DNS request from a user host, the device searches for the static domain name binding record, queries DNS cache records on the device, and then queries the DNS server if no record is found. The device returns the query result to the user host. If no DNS server address is specified, the device uses the statically configured or dynamically obtained DNS server address by default.

If both DNS forward proxy and DNS proxy are enabled on the device, DNS forward proxy takes precedence over DNS proxy.

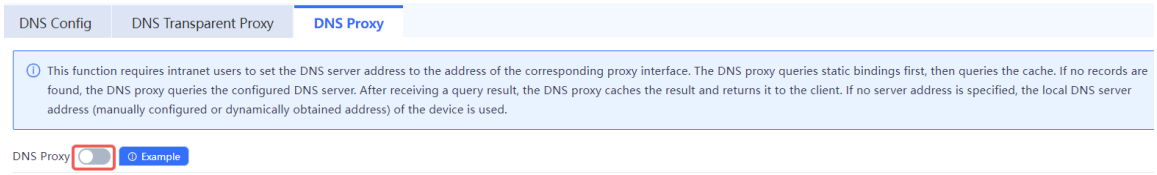


2. Creating a DNS Proxy

Procedure

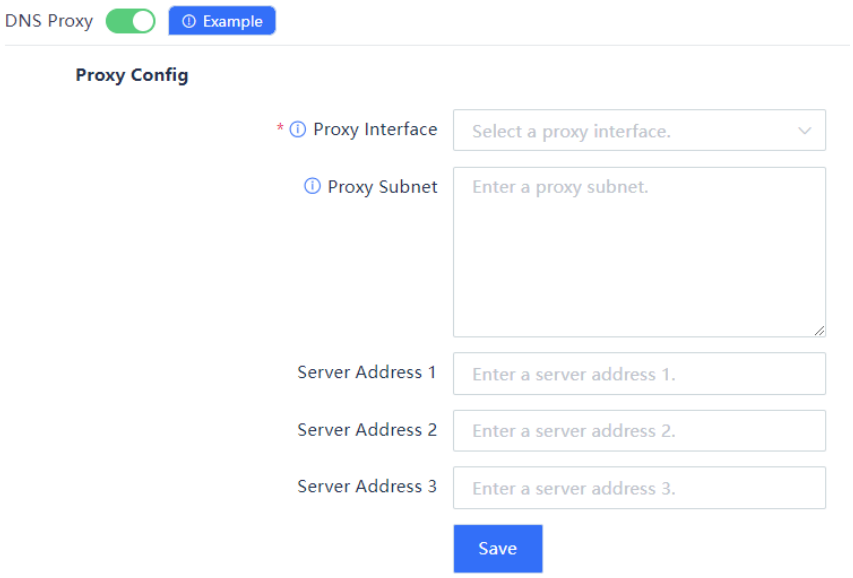
(1) Choose **Network** > **DNS** > **DNS** and click the **DNS Proxy** tab.

(2) Click  to enable DNS proxy.



(3) Configure the DNS proxy.

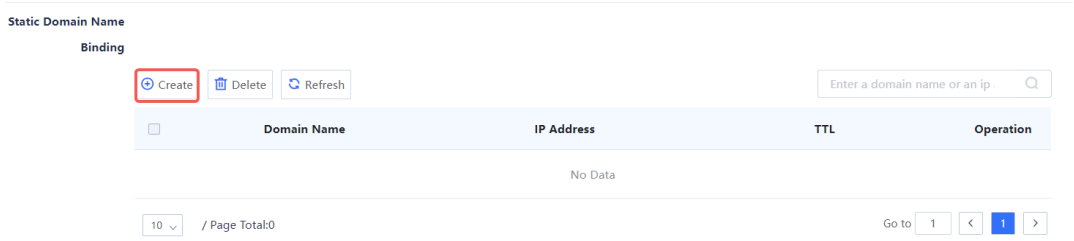
- Perform the proxy configuration.



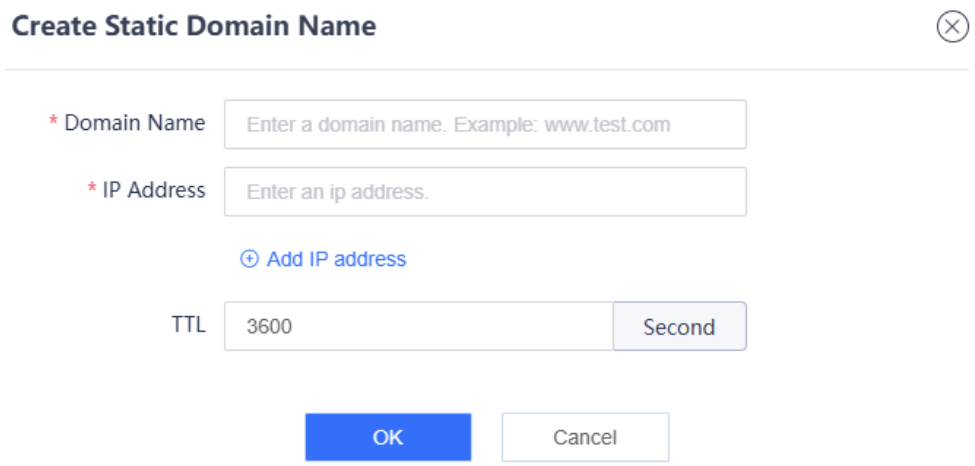
Item	Description	Remarks
Proxy Interface	Receives DNS requests from users. Intranet users need to set the DNS server address to the IP address of the proxy interface.	Select one or more items from the drop-down list box.
Proxy Subnet	Network segment where the proxy user resides. After a proxy network segment is configured, the DNS proxy interface receives requests only from users on the proxy network segment. If no proxy network segment is configured, the DNS proxy interface receives requests from users on any network segment.	Enter an IP address or network segment. [Example1] 192.168.1.1 or 192.168.1.0/24 [Example2] 1234::/64

Item	Description	Remarks
Server Address	DNS server address. A maximum of three server addresses in descending order of priority can be configured.	Enter an IP address. [Example1] 192.168.1.1 [Example2] 1234::100

- Configure static domain name binding.
  a Click **Create**.



  b Add static domain name binding.



Item	Description	Remarks
Domain Name	Domain name resolved by the DNS request.	[Example] www.test.com
IP Address	IP address corresponding to the domain name resolved by the DNS request.	Enter an IP address. [Example1] 192.168.1.1 [Example2] 1234::100

Item	Description	Remarks
TTL	Aging time of domain name cache records of a user PC.	[Example] The default interval is 3600 seconds.

c Click **OK**.

Follow-up Procedure

- Click **Create** to add a static domain name binding.
- Click **Delete** to delete the specified static domain name binding.
- Click **Refresh** to obtain the latest static domain name binding configuration.

6.11.4 Configuring DDNS

1. Overview

The Domain Name System (DNS) only provides static mappings between domain names and IP addresses. If a DNS client IP address is updated, the DNS server cannot update the mappings between domain names and IP addresses. In this case, if the original domain name is used to access the DNS client, the IP address obtained through domain name resolution is incorrect, causing an access failure.

The Dynamic DNS (DDNS) service is used to dynamically update the mappings between domain names and IP addresses on the DNS server. The DDNS server synchronizes the updated mappings between domain names and IP addresses to other DNS Servers. If the IP address of a DDNS client changes, users can still access the DDNS client using the same domain name.

DDNS applies to the scenario where the firewall acts as an intranet border device and connects to the external network by obtaining a public IP address through dial-up or DHCP. In this scenario, the IP address of the outbound interface of the firewall changes dynamically. When the firewall provides IPsec VPN, SSL VPN, or other services to external users through the outbound interface, you need to configure a DDNS policy to dynamically update the mappings between domain names and IP addresses.

2. Configuring a DDNS Policy

Application Scenario

Configure a DDNS policy on the outbound interface of the firewall so that the firewall can act as a DDNS client. If the IP address of the device interface is updated, the firewall sends a request to the DDNS server to update the mapping between the domain name and IP address.

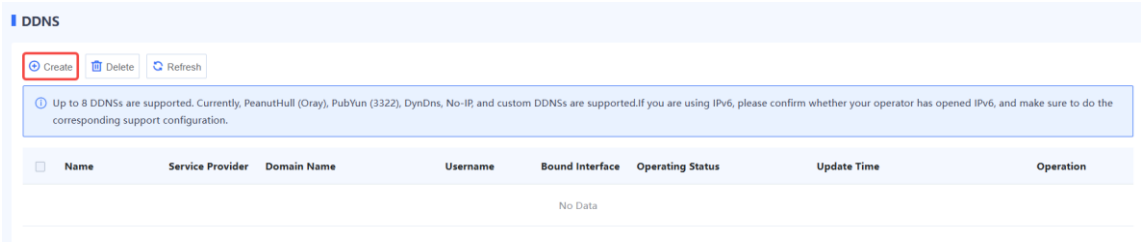
Prerequisites

- The firewall functions as the egress gateway and can obtain a public IP address (If the outbound interface uses a private network address, the DDNS function may not take effect.).
- You have registered an account and domain name with a third-party DDNS service provider. To configure IPv6 DDNS to implement mapping between a domain name and an interface IPv6 address, ensure that the DDNS service provider supports IPv6 resolution.
- The device can access the Internet and communicate with the DDNS server.

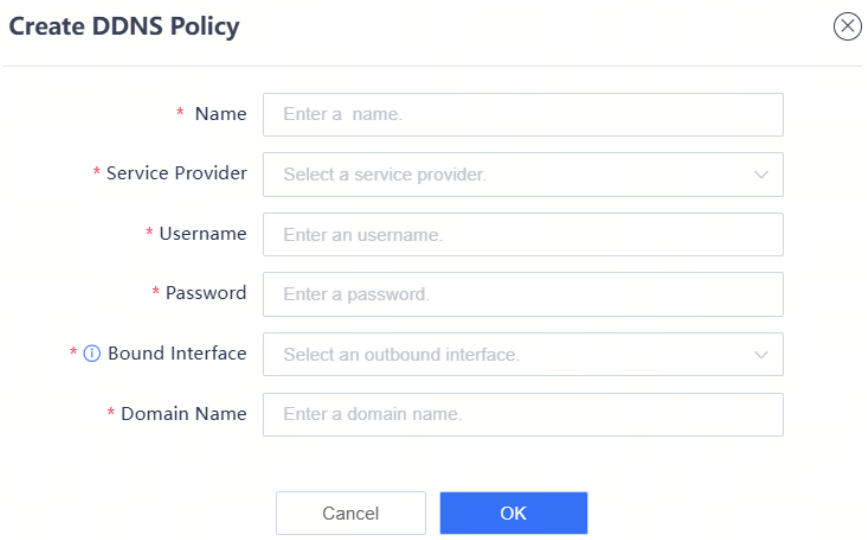
Procedure

(1) Choose **Network** > **DNS** > **DDNS**.

(2) Click **Create**.



(3) Configure a DDNS policy.



Item	Description	Remarks
Name	Name of the DDNS policy.	[Example] DDNS_1
Service Provider	Name of the third-party DDNS service provider.	[Example] No-IP
Username/Password	Enter the username and password of the account registered on the official website of the DDNS service provider.	N/A
Bound Interface	Select the interface to be bound with the DDNS policy. After an interface is configured, if the IP address of the interface is updated, the firewall sends a request to the DDNS server to update the mapping between the domain name and IP address.	● A physical interface, sub-interface, bridge interface, or aggregate interface can be set. ● The DDNS policy takes effect only when the interface is configured with an IP address. [Example] Ge0/7

Item	Description	Remarks
Domain Name	Domain name that corresponds to the IP address of the bound interface. One account can be bound with multiple domain names. Specify at least one domain name for the interface IP address. The specified domain names are resolved to the interface IP address.	[Example] www.abc.com

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

Follow-up Procedure

- On the **DDNS** page, check the operating status and update time of DDNS policies.
- Click **Edit** in the **Operation** column to modify policy configurations.
- Click **Delete** in the **Operation** column to delete the DDNS policy. After deletion, the DDNS server does not update the mappings between the domain names and interface IP addresses specified in the policy.

6.12 DHCP Management

6.12.1 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 CF series firewall can be configured as a DHCP server to allocate IP addresses to intranet users.

  The CF series firewall can also function as the DHCP relay agent to connect a DHCP client and a DHCP server on different network segments. In this way, the client can obtain the network configuration such as the IP address from the DHCP server on different network segment.

6.12.2 Configuring a DHCP Server

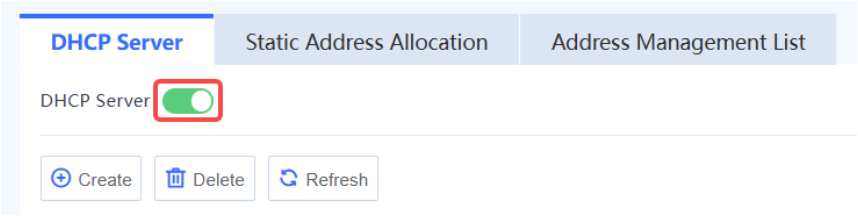
1. Application Scenario

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** > **DHCP Server**.

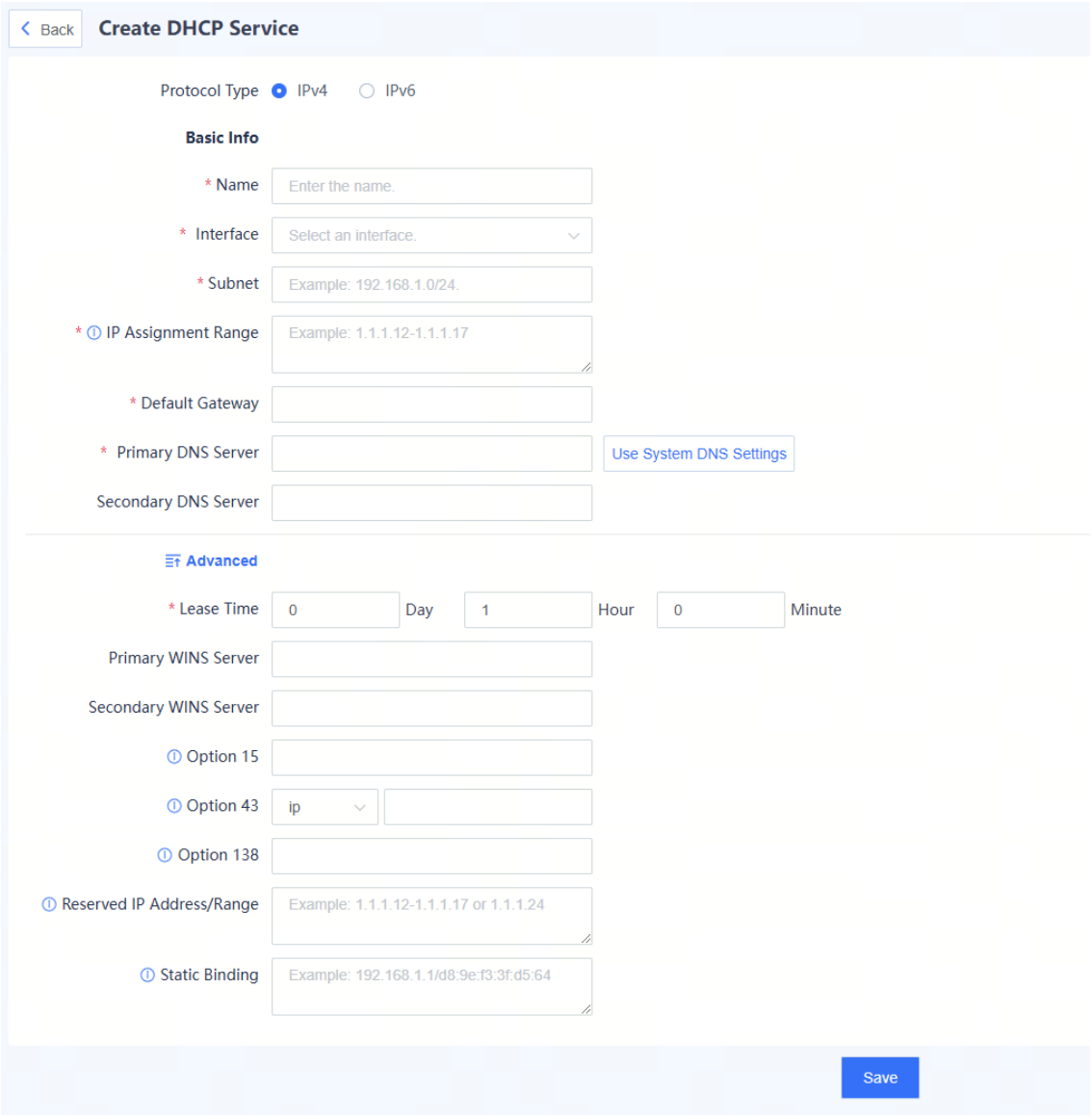
(2) Toggle on  to enable the DHCP server function.



(3) Configure the DHCP server information.

a Click **Create**.

The **Create DHCP Service** page is displayed. Set **IPv4**.



b Set parameters of the DHCP server.

Item	Description	Remarks
Name	Name of a DHCPv4 address pool.	[Example] DHCP Server 1
Interface	Interface where the DHCPv4 service is configured. After the DHCPv4 service is enabled, the interface can allocate IPv4 addresses.	The DHCP server and relay functions cannot be configured on an interface simultaneously. [Example] Ge0/1
IP Assignment Range	Range of IP addresses allocated by the DHCP server.	● Enter an IP address range per line. ● Connect the start IP address and end IP address with a hyphen (-). [Example] 192.168.1.1-192.168.1.10
Subnet	Subnet where the IP addresses are located.	Enter the subnet address/ mask bits. [Example] 192.168.1.0/24
Default Gateway	Default gateway that provides network access 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		

Item	Description	Remarks
Lease Time	Address lease period. In general, terminal devices automatically renews the lease in connected state to keep the IP address unchanged. If the lease is not renewed due to disconnection or network instability, the IP addresses are reclaimed after the lease expires. When the terminal devices recover connectivity, they will request the addresses again.	● The lease period ranges from 3 minutes to 365 days. ● The default lease period is 1 hour. [Example] 1 hour
Primary WINS Server	Windows Internet Naming Service (WINS) is used to register host names of network basic input/output system (NetBIOS) and resolve IP addresses based on host names.	This parameter is optional. The value is empty by default. [Example] 10.1.1.4
Option 15	Option 15 carried in DHCP packets. This option is used to specify the domain name suffix used by the client for host name parsing in the domain name system.	[Example] example.com
Option 43	Option 43 carried in DHCP packets. Option 43 is typically used in wireless network management scenarios to notify APs of the IP address of the wireless access controller (AC) so that the APs can register with the AC. When the AC and APs are on different LANs, the APs cannot discover the AC in broadcast mode. In this case, Option 43 needs to be configured for DHCP response packets on the DHCP server.	● The supported option types vary with AP models. Select Option 43 or Option 138 based on the supported option types of managed APs. ● Two formats are supported: o IP address: Enter the IP address of the AC. Typically, the loopback address of the AC is configured. o ASCII code: Set Option 43 to a hexadecimal number in ASCII format.
Option 138	Option 138 in DHCP packets. Option 138 is similar to Option 43. When the AC and APs are on different LANs, you can configure Option 138 to enable the AP to obtain the IP address of the AC.	Enter the IP address of the AC. Typically, the loopback address of the AC is configured. The supported option types vary with AP models. Select Option 43 or Option 138 based on the supported option types of managed APs.

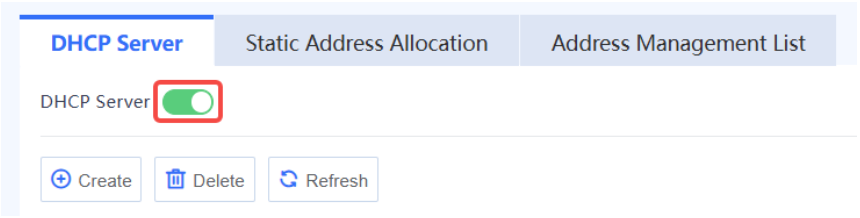
Item	Description	Remarks
Secondary WINS Server	Secondary WINS server address assigned to a DHCP client. If the DHCP client fails to resolve the host name through the primary WINS server, the DHCP client requests the secondary WINS server to resolve the host name.	This parameter is optional. The value is empty by default. [Example] 10.1.1.5
Reserved IP Address/Range	Reserved IP addresses in the **IP Assignment Range**.	[Example] 192.168.1.2 or 1.1.1.12-1.1.1.17
Static Binding	Static bindings between the pre-assigned IP addresses specified by **IP Assignment Range** and the MAC addresses of the clients. When receiving a request for an IP address from a client with a matching MAC address, the DHCP server allocates the pre-assigned IP address that is bound to the MAC address only to this client.	● The value is in the format of IP address/MAC address, where the IP address should be a pre-assigned address in the **IP Assignment Range**. ● Enter one binding entry per line. ● The configured static IP-MAC binding entries can be viewed on the **Static Address Allocation** page. [Example] 192.168.10.1/d8:9e:f3:3f:d5:64

c Click **Save**.

3. Configuring a DHCPv6 Server

(1) Choose **Network** > **DHCP** > **DHCP Server** > **DHCP Server**.

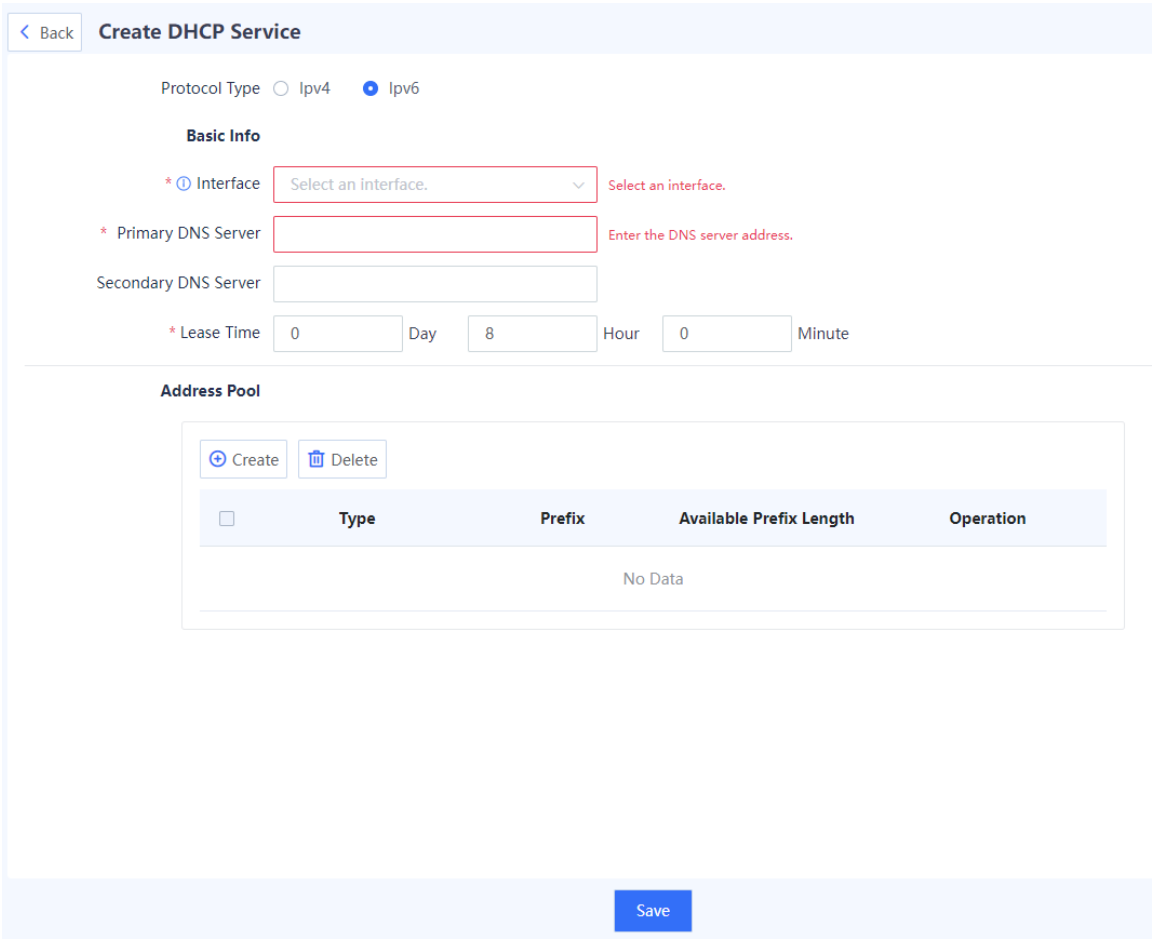
(2) Toggle on to enable the DHCP server function.



(3) Configure the DHCP server information.

a Click **Create**.

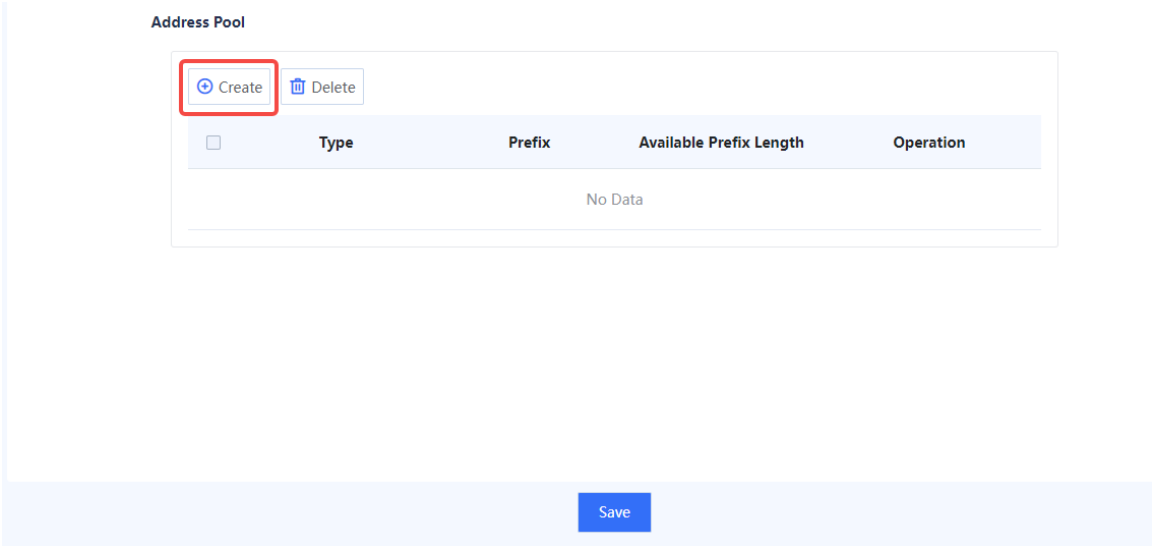
The **Create DHCP Service** page is displayed. Set **IPv6**.



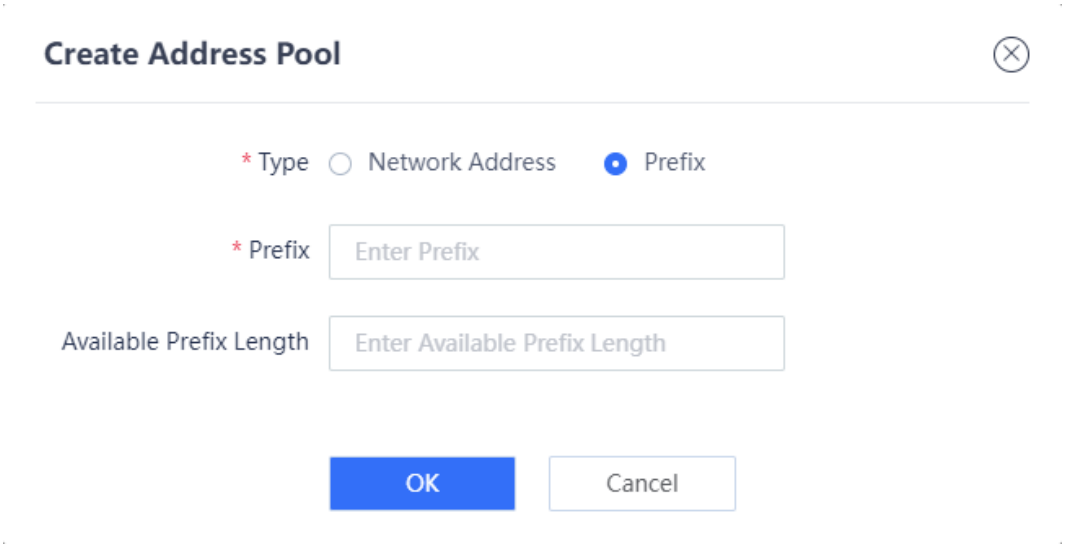
b Set parameters of the DHCP server.

Item	Description	Remarks
Interface	Interface where the DHCPv6 server is configured. After the DHCPv6 function is enabled, the interface can allocate IPv6 addresses.	[Example] Ge0/4
Primary DNS Server	Preferred DNS server used by the DHCP service.	[Example] 2001::1
Secondary DNS Server	Alternative DNS server used by the DHCP service.	[Example] 2001::2
Lease Time	Address lease period. In general, terminal devices automatically renews the lease in connected state to keep the IP address unchanged. If the lease is not renewed due to disconnection or network instability, the IP addresses are reclaimed after the lease expires. When the terminal devices recover connectivity, they will request the addresses again.	[Example] 1 hour

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



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

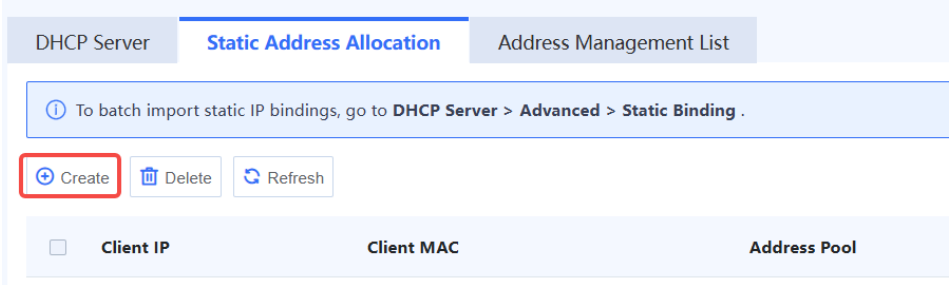


e Click **Save**.

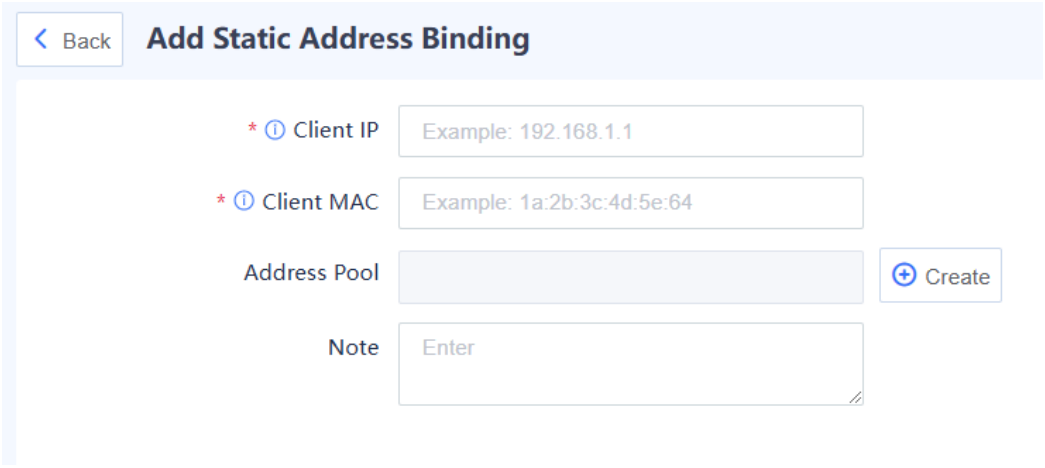
4. Configuring Static Address Allocation

(1) Choose **Network** > **DHCP** > **DHCP Server** > **Static Address Allocation**.

(2) Click **Create**.



(3) Enter the MAC address of a client and the IP address to be allocated to the client.



Item	Description	Remarks
Client IP	IP address allocated to a DHCP client. The IP address must be from an existing address pool.	[Example] 192.168.1.1
Client MAC	MAC address of a client.	[Example] 1a:2b:3c:4d:5e:64
Address Pool	Address pool to which the IP address allocated to a client belongs. After you set **Client IP**, the system automatically identifies the address pool and fills in its name.	-
Note	Description of a static address binding.	-

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

5. 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.
- Choose **Network** > **DHCP** > **Address Management List** to view the assignment of IP addresses in each address pool.

6.12.3 Configuring a DHCP Relay Agent

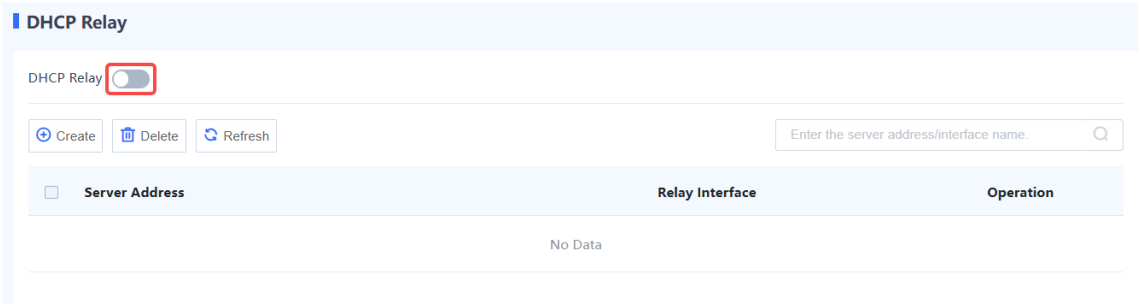
Application Scenario

After the DHCP relay function is enabled on a firewall, the firewall functions as a DHCP relay agent to transmit DHCP messages between different network segments. In this way, clients can obtain IP addresses and other network configurations from the DHCP server on different network segment, implementing automatic configuration of clients' addresses and simplifying network management.

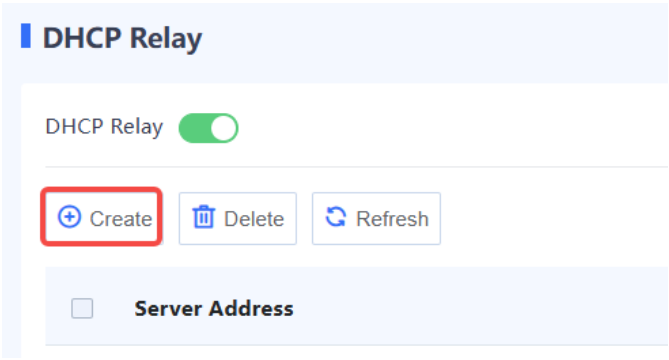
Procedure

(1) Choose **Network** > **DHCP** > **DHCP Relay**.

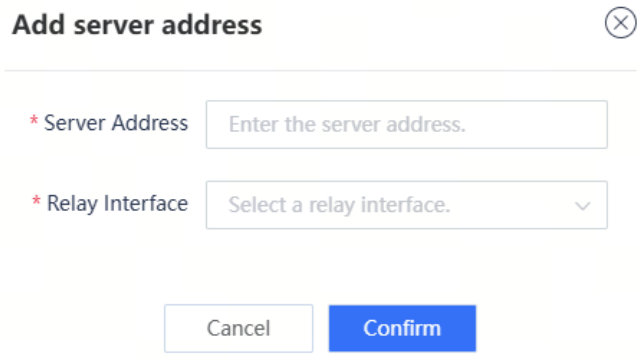
(2) Click to enable the DHCP relay function.



(3) Click **Create**.



(1) Configure the DHCP relay.

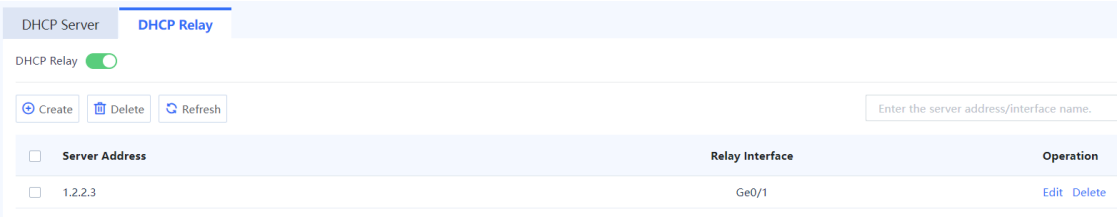


Item	Description	Remarks
Server Address	DHCP server address.	Only IPv4 addresses are supported. [Example] 192.168.1.2

Item	Description	Remarks
Relay Interface	Configure the DHCP relay on an interface. After the DHCP relay function is enabled on an interface, the interface can forward DHCP messages.	● The DHCP server and relay functions cannot be configured on an interface simultaneously. ● If the interface address is on the same network segment as the server address, the interface cannot be configured as a relay interface. ● Only a LAN interface can be configured as a relay interface. ● Select one or more items from the drop-down list. [Example] Ge0/1

(2) Click **Confirm**.

Follow-up Procedure



- Select one or more entries and click **Delete** to batch delete relay service entries.
- Click **Delete** in the **Operation** column to delete the DHCP relay service entry. Click **Edit** in the **Operation** column to modify the DHCP relay service entry.

6.12.4 Address Management List

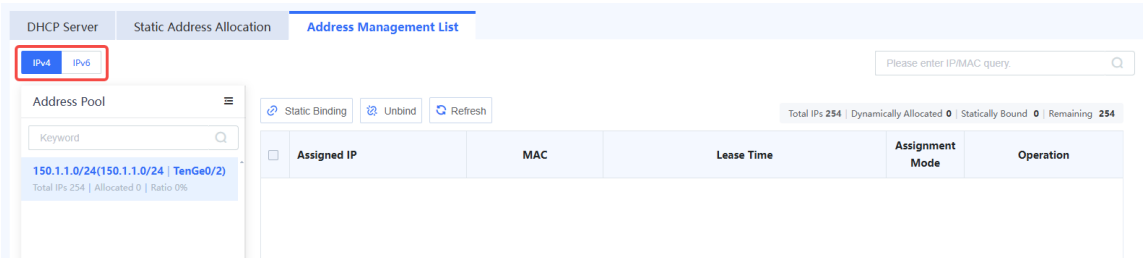
Application Scenario

This operation allows you to check the IP addresses allocated by the DHCP server and the IP address allocation status of the specified address pool.

Procedure

(1) Choose **Network** > **DHCP** > **DHCP Server** > **Address Management List**.

(2) Click **IPv4** or **IPv6** in the upper-left corner to view assigned IPv4 or IPv6 addresses.



(3) In the address pool list on the left, click a specified address pool to view the IP address allocation status of the address pool, including the total number of allocated IP addresses, the number of dynamically allocated IP addresses, the number of statically bound IP addresses, and the number of remaining IP addresses.



(4) 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. After you remove a static binding entry, the corresponding entry on the **Static Address Allocation** tab page will be removed automatically.

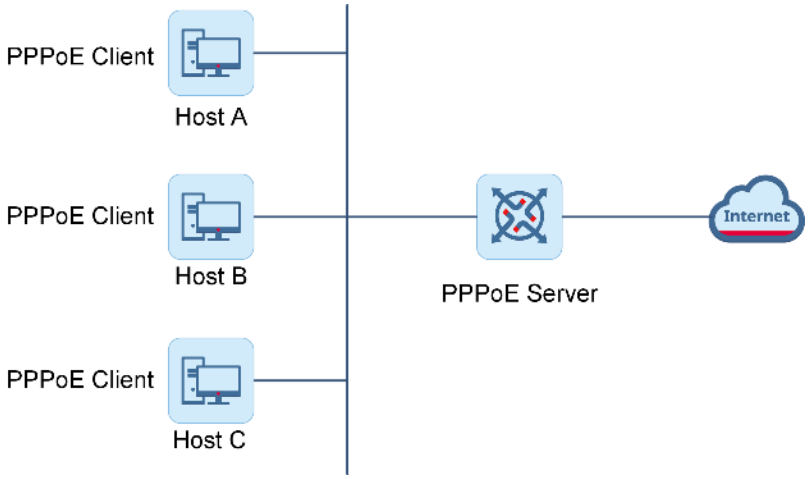
6.13 PPPoE Server

6.13.1 Overview

Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol that packages PPP frames in Ethernet frames so that PPP can run in multi-access networks such as Ethernet to implement point-to-point communication in the Ethernet environment. PPPoE networking uses the client/server (C/S) structure. A PPPoE client initiates a connection request to establish a PPPoE session with a PPPoE server.

The device can function as a PPPoE server to provide dial-up access services for clients in the local area network (LAN) and implement external network access. When the device serves as a PPPoE server, it can implement user authentication, dynamic IP address allocation, access control, and traffic statistics collection.

Figure 6-11 Topology of the Device Working as a PPPoE Server



6.13.2 PPPoE Server Configuration

Application Scenario

This section describes how to configure the device as a PPPoE server to provide access control and authentication functions for LAN users.

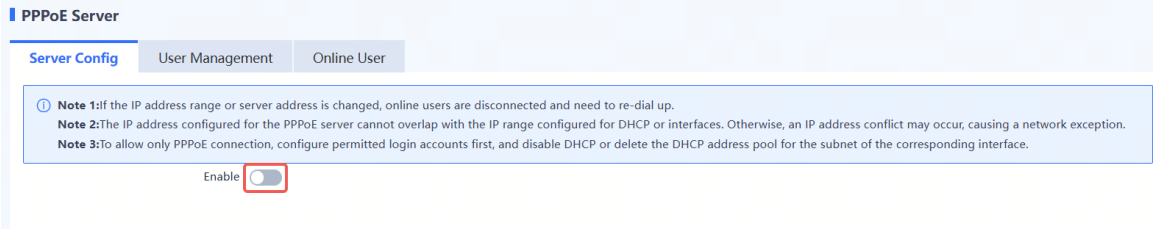
Prerequisites

- Before enabling the PPPoE server function, create at least one PPPoE user by choosing **Network** > **PPPoE Server** > **User Management**. For configuration details, see 6.13.3 PPPoE User Management.
- If you want to allow only PPPoE dial-up access on the interface, configure a PPPoE user account that can be used for login, and disable the DHCP service on the interface or delete the DHCP address pool on the network segment of the corresponding interface.

Procedure

(1) Choose **Network** > **PPPoE Server** > **Server Config**.

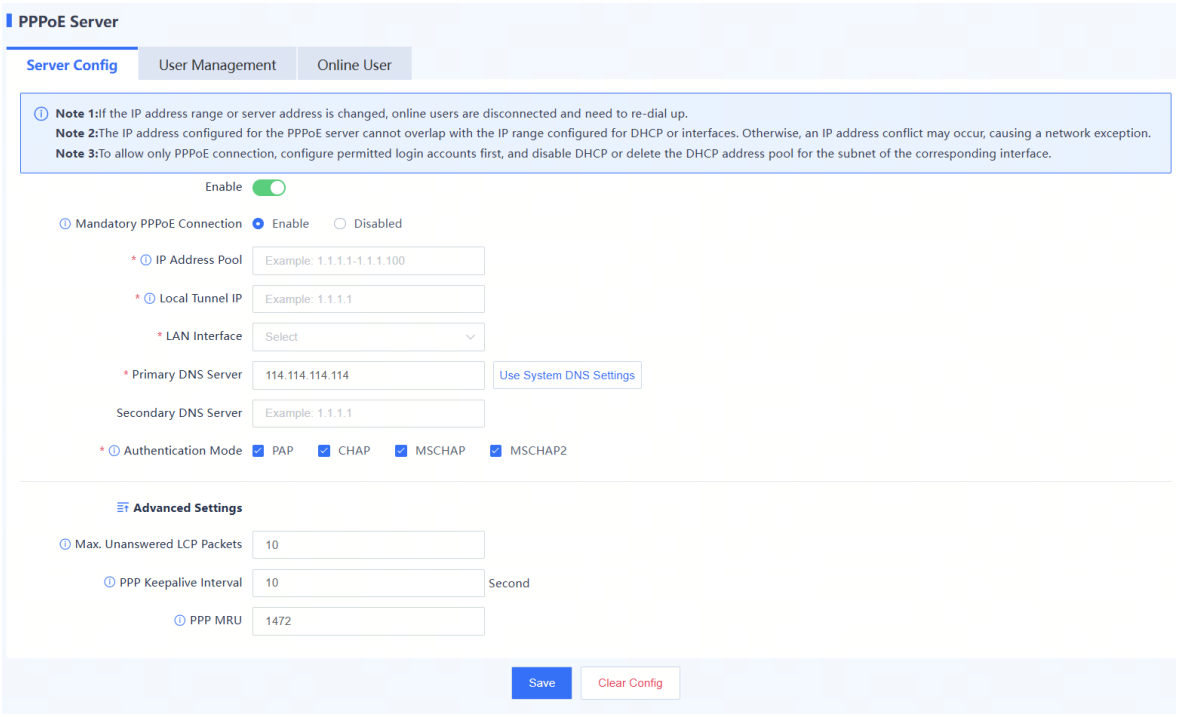
(2) Toggle on **Enable**.



(3) Set configuration items related to the PPPoE server.

Caution

Changing the IP address pool range of the PPPoE server or the local tunnel IP address causes online users to go offline and requires them to re-dial up.



Item	Description	Remarks
Enable	Whether the PPPoE server function is enabled globally.	By default, this function is disabled. [Example] Enabled

Item	Description	Remarks
Mandatory PPPoE Connection	After forcible PPPoE dialup is enabled, only PPPoE traffic is permitted to pass through the LAN interface with the PPPoE server function enabled. That is, LAN users on the interface can only obtain IP addresses through the device through PPPoE dialup to access the network. After forcible PPPoE dialup is enabled on an internal network interface, users cannot log in to the device using the IP address of the internal network interface with PPPoE dialup enabled. To access and manage the device through the internal network interface, you can disable this configuration, or perform the following steps: (1) Before enabling the PPPoE server function, configure a PPPoE user account dedicated for device management on the PPPoE server. (2) Enable the PPPoE server function on the device. (3) A user uses the preceding account to dial up on a downstream device connected to the LAN interface of the device, accesses the local tunnel IP address configured on the PPPoE server, and manages the device.	[Example] Enabled
IP Address Pool	Specifies the IP address range that can be allocated by the PPPoE server to access users. Note that this address pool cannot overlap the DHCP address pool or the IP address of the device interface. Otherwise, an IP address conflict may occur, resulting in network exceptions.	Enter the IP address range. Use an en dash (–) to separate the start IP address and end IP address. Format: start IP address–end IP address. [Example] 10.20.1.1–10.20.1.254
Local Tunnel IP	IP address used by the device (PPPoE server) to establish a connection with a PPPoE client. PPPoE dial-up user can access the PPPoE server through this IP address. The IP address of the local tunnel cannot overlap with the IP address of the DHCP address pool or the interface of the device. Otherwise, an IP address conflict may occur.	● By default, the first IP address in an IP address pool is used as the local tunnel address of the server. ● IP addresses in the same range as the IP address pool need to be configured. [Example] 10.20.1.1

Item	Description	Remarks
LAN Interface	Specifies the LAN interface on which the PPPoE server function is to be enabled.	● Select an interface for which ARP check needs to be enabled from the drop-down list. Multiple interfaces can be selected. ● Only LAN interfaces in routing mode can be selected. [Example] Ge0/1, Ge0/2
Primary DNS Server	Peimary server address assigned to a PPPoE client.	Click **Use System Dns Settings**, and the DNS server configuration of the device is automatically entered. [Example] 114.114.114.114
Secondary DNS Server	Secondary DNS server address assigned to a PPPoE client.	[Example] 8.8.8.8
Authentication Mode	Specifies the PPPoE authentication mode.	● Multiple choices are supported. ● The authentication mode of the PPPoE client must match that of the PPPoE server. To be compatible with different types of clients, you are advised to enable multiple authentication modes. [Example] PAP, CHAP
Advanced settings Configure PPPoE keepalive parameters. If the PPPoE server does not receive any response from the PPPoE client within the timeout period, the PPPoE server automatically closes the session. PPPoE connection timeout period = Maximum unanswered LCP packets x PPP keepalive interval		
Max. Unanswered LCP Packets	The value of this parameter increases by 1 if the PPPoE server does not receive any reply packet from the client within the specified period after sending an LCP packet. If the number of consecutive unanswered LCP packets exceeds the configured threshold, the PPPoE server considers that the PPPoE client has been disconnected and automatically closes the session.	The default value is 10, indicating that the device automatically terminates the connection if it does not receive any response from the client for 10 consecutive LCP packets. [Example] 10

Item	Description	Remarks
PPP Keepalive Interval	Specifies an interval at which a device sends PPP link maintenance detection packets (LCP Echo-Request packets). After a PPPoE connection is established, the device periodically sends PPP link maintenance detection packets to detect the PPP link state and ensure the normal running of the PPPoE connection.	The default value is 10, indicating that the device sends PPP Hello packets every 10 seconds. [Example] The default value is 10 seconds.
PPP MRU	The PPP maximum receive unit (MRU) is used to limit the maximum PPP frame length (in bytes) of the local device (PPoE server) to prevent packet loss or performance deterioration caused by excessively large frames.	[Example] 1472

(4) Click **Save**. A message prompting you to configure a security policy is displayed. You can click **Configure** to redirect to the security policy configuration page, where you can configure a security policy to permit packets whose source IP addresses belong to the address pool.

Follow-up Procedure

- You can **Clear Config** to clear the current PPPoE server configuration and restore the server to the unconfigured state.
- After setting the network connection type of the PPPoE client to PPPoE and entering the username and password, you can perform PPPoE dial-up.

6.13.3 PPPoE User Management

Application Scenario

You can configure a PPPoE user account as the access credential for the PPPoE client. When a PPPoE client initiates a connection request to the PPPoE server, it must provide a valid identity credential (username and password) for authentication. Only authenticated clients can establish PPPoE sessions and access the network. You can configure and manage PPPoE users to ensure network security and prevent unauthorized access.

Procedure

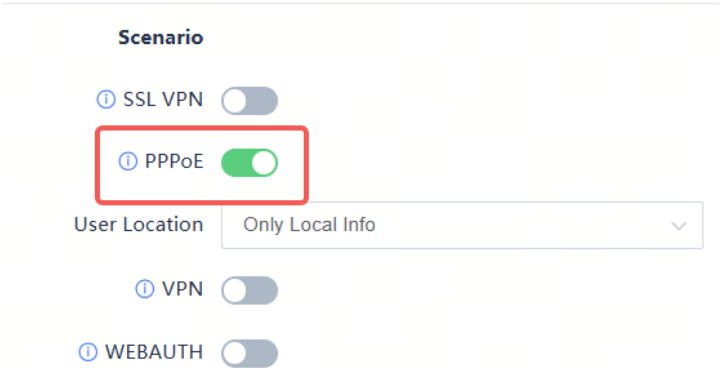
(1) Choose **Network** > **PPPoE Server** > **User Management**.

(2) (Optional) Configure an authentication domain for the PPPoE server.

By default, the PPPoE server uses the PPPoE authentication domain to authenticate PPPoE access users. To change the authentication domain used by the PPPoE server, click **Switch authentication domain**.

Caution

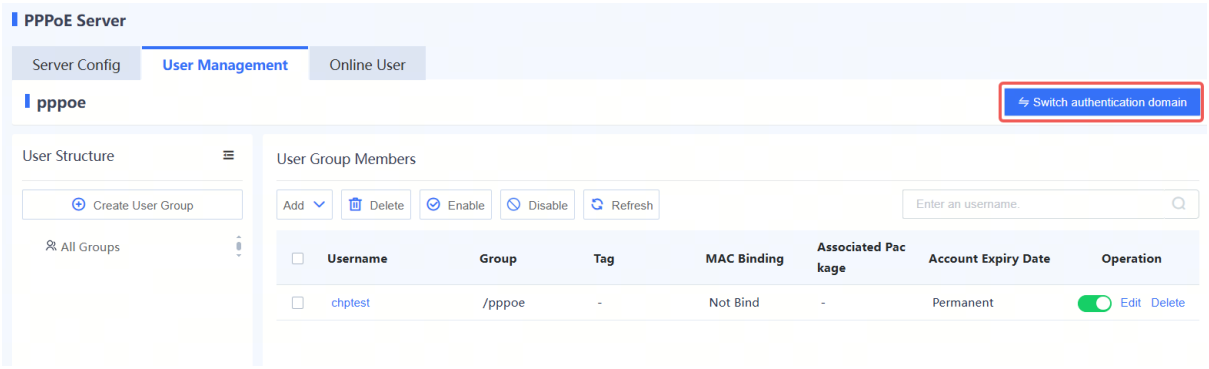
- The PPPoE scenario function must be enabled for the authentication domain used by the PPPoE server. Otherwise, users cannot go online.



- Changing the authentication domain of the PPPoE server will cause all users to go offline. Therefore, exercise caution when performing this operation.

Note

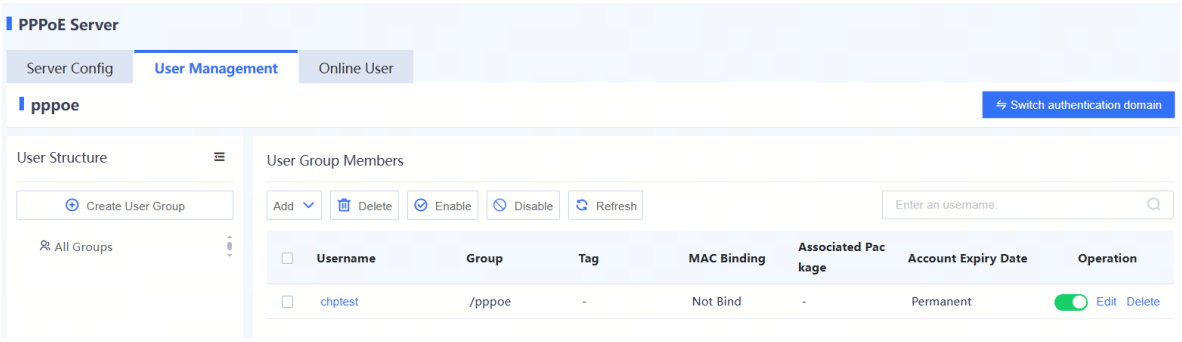
- By default, the authentication domain named pppoe uses only local user information for PPPoE access authentication, that is, PPPoE user information needs to be configured and managed on the local device. If PPPoE user information is stored on an external server, you can set **Only Info on Server** and configure the authentication server.
- To add an authentication domain or modify the authentication domain configuration, choose **Object** > **User Authentication** > **Authentication Domain**. For more information about authentication domains, see 5.8.7 Authentication Domain Management.



(3) Configure a PPPoE user.

The overall operation logic of the PPPoE client management page is similar to that of the authenticated client management page. You can configure user groups, add a single user, add users in batches, and export user information. For details about user management operations, see 5.8.2 User Management.

Follow-up Procedure



- Click **Edit** in the **Operation** column to modify user information. Modifying the IP/MAC binding configuration, for example, changing from no binding to automatic MAC address binding, may cause authenticated users to go offline.
- Toggle on the switch in the **Operation** column to enable or disable the user account.
- Select multiple users and click **Delete** to delete user information in batches. After deletion, authenticated users go offline and cannot pass authentication again.
- Select multiple users and click **Disable** to disable users in batches. Authenticated users will go offline and cannot pass authentication again.
- Select multiple users and click **Enable** to enable users in batches.

6.13.4 Viewing Online Users

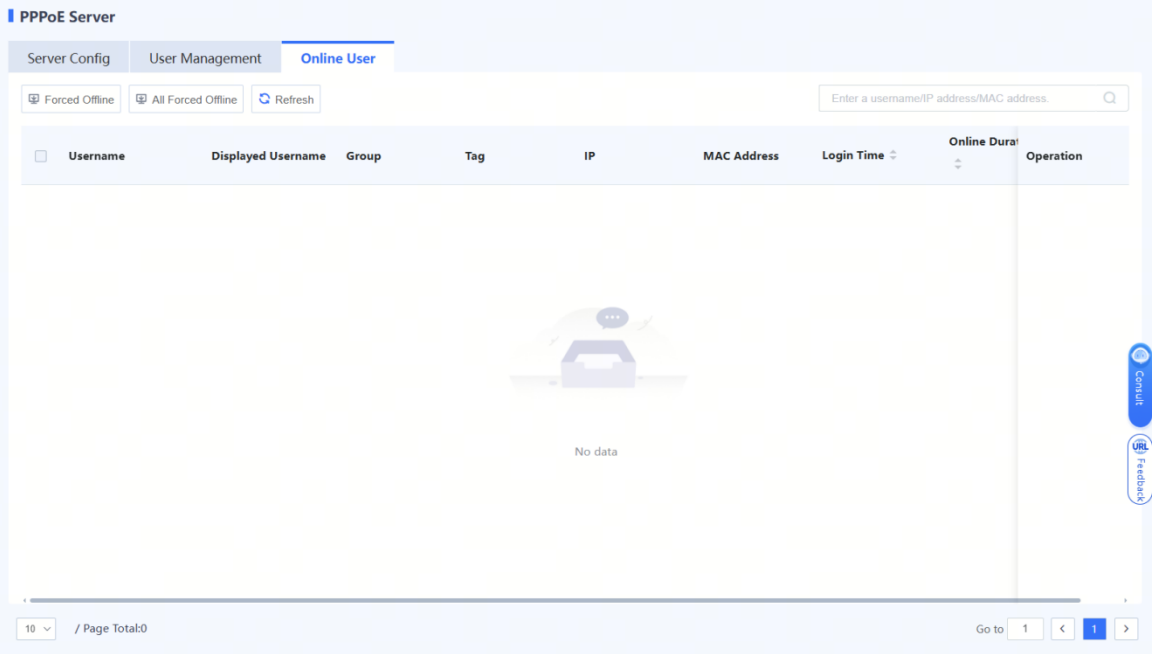
Application Scenario

The **Online User** tab page displays information about users who access the device (PPPoE server) through PPPoE dial-up. You can forcibly log out a user and disconnect a user from the PPPoE server.

Procedure

(1) Choose **Network** > **PPPoE Server** > **Online User.**

(2) The page displays details about the online PPPoE users, including the IP address, terminal MAC address, login time, and uptime. Click **Refresh** to view the latest data.



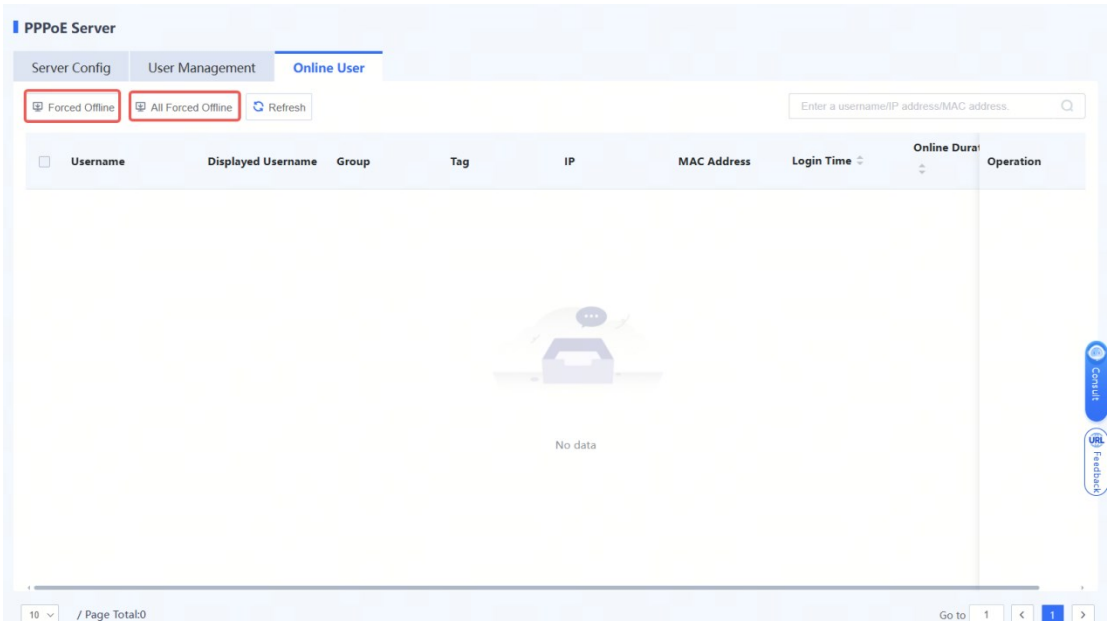
(3) (Optional) Disconnect users.

- Disconnect a single user: In the **Operation** column, click **Offline**.

Note

A single PPPoE user account may be used by different clients. Therefore, differentiate login devices by MAC address.

- Logging out users in batches: Select the target users and click **Forced Offline** at the top of the page. To force all online users offline, click **Force All Offline**.



6.14 Link Detection

6.14.1 Link Quality Detection

1. Detection Configuration

Application Scenario

Link quality detection checks the connectivity of network links. After this function is enabled, the device periodically detects the link status. If other modules are associated with the detection policy, detection results are used for processing.

After configuring link detection, associate the link detection object with a module. Otherwise, detection results are only displayed but are not used for processing. On the device, link detection is supported on the following modules:

- Physical interface
- Sub-interface
- Aggregate interface
- Static routing
- Intelligent routing
- DNS transparent proxy
- High availability

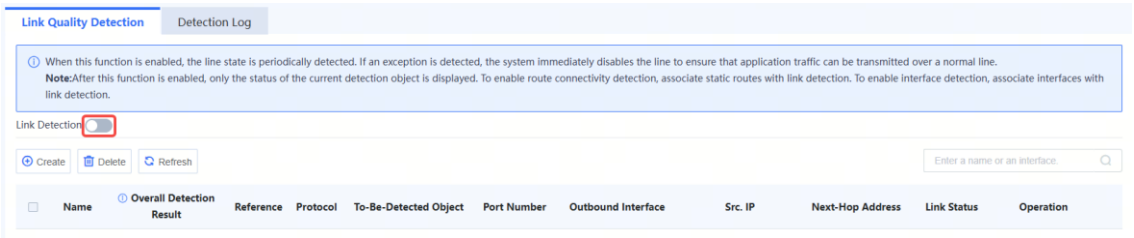
Procedure

(1) Choose **Network** > **Link Detection** > **Link Quality Detection** > **Link Quality Detection**.

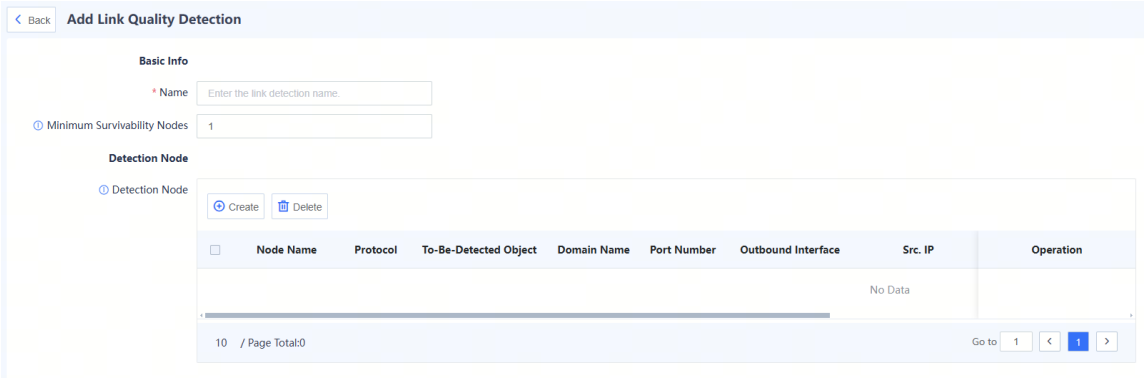
(2) Toggle on to enable link detection.

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 Quality Detection** page. Set the detection parameters.



Item	Description	Remarks
Basic Info		
Name	Name of a link detection object.	[Example] Test
Minimum Survivability Nodes	Minimum number of detection survivability instances. Range: smaller than or equal to the number of detection nodes.	[Example] 1
Detection Node You can configure multiple detection nodes for a link detection object. When the number of survivability nodes of a link detection object is smaller than the minimum number of survivability nodes, the link detection fails. Click **Create** to add a detection node.		
Node Name	Name of the detection node.	[Example] Test_node
Protocol	Detection protocol type.	[Example] ICMP
To-Be-Detected Dest. IP	IP address of the detection node when the protocol type is ICMP or TCP.	You can enter an IPv4 or IPv6 address. The destination IP address to be detected must be of the same type as the source IP address. [Example] 192.168.2.2

Item	Description	Remarks
To-Be-Detected DNS Server	IP address of the DNS server to be detected when the protocol type is DNS.	You can enter an IPv4 or IPv6 address. The DNS server address to be detected must be of the same type as the source IP address. [Example] 192.168.2.2
Domain Name	Domain name to be detected when the protocol type is DNS.	[Example] www.test.com
Port	Port to be detected when the protocol type is DNS or TCP.	[Example] 53
To-Be-Detected URL	URL to be detected when the protocol type is HTTP or HTTPS.	● Only exact match is supported. ● You can enter a port number at the end of the URL. [Example] http://www.ruijie.com:53
Outbound Interface	Outbound interface for node detection.	The outbound interface must be a WAN interface in routing mode. [Example] Ge0/2
Src. IP	Source IP address for node detection.	The destination IP address to be detected must be of the same type as the source IP address. [Example] 192.168.2.1
Next-Hop Address	Next-hop IP address of the route destined for the detection node.	This parameter is available when the protocol type is ICMP, DNS, or TCP. [Example] 192.168.2.1
Detection Frequency	Frequency of node detection or node recovery detection.	[Example] 6000 ms

Item	Description	Remarks
Retries	Number of periods for node detection, which takes effect in real time. For example, if the detection frequency is 6 seconds and the number of retries is 4, the interface sends a detection packet every 6 seconds. If no response is received for four consecutive times, the interface considers that an exception occurs and the detection result is Down.	[Example] 4
Recovery Times	Number of periods for node recovery detection, which takes effect in real time. For example, if the detection frequency is 6 seconds and the number of recovery times is 3, the interface goes Up again after it sends a detection packet every 6 seconds and the response packet is received successfully for three consecutive times.	[Example] 3
Operation	● Toggle on or off the switch to specify whether to detect this node. ● Click **Edit** or **Delete** to edit or delete the node.	-

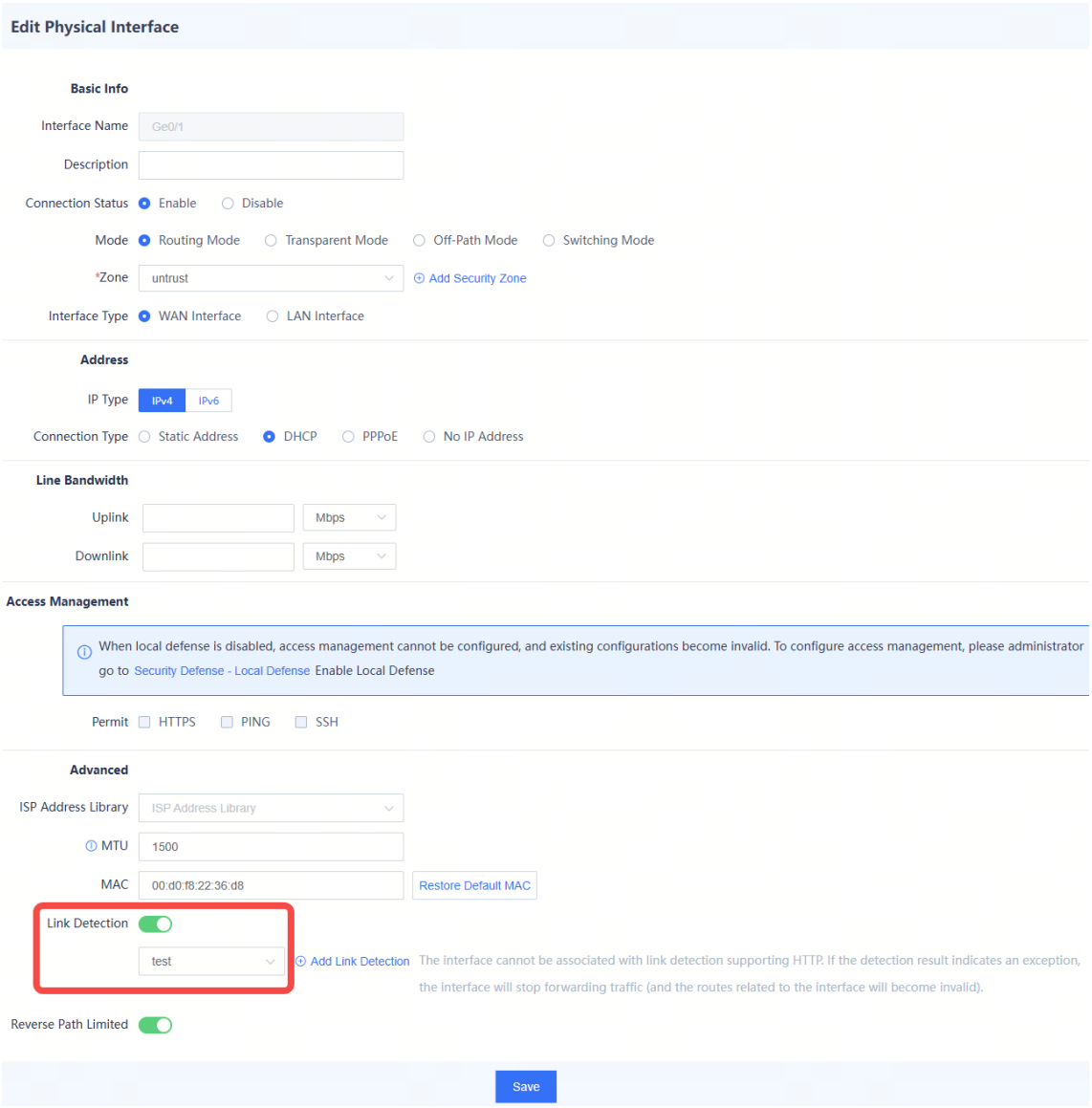
(4) Click **Save**.

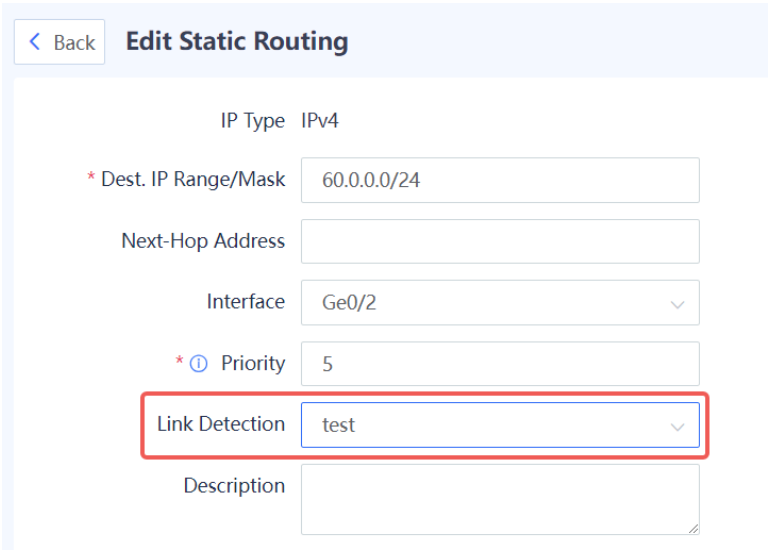
Follow-up Procedure

- After configuring link detection, associate the link detection object with a routing rule or interface. Otherwise, link detection does not take effect. For example, if outbound interface Ge0/2 is configured for link detection object test, you need to associate link detection object test with Ge0/2 or a routing rule.

Note

- When you associate an interface or route with a link detection object, the device verifies the IP address type of the detected node. IPv4 addresses or routes can only be associated with link detection objects configured with IPv4 detection nodes. IPv6 addresses or routes can only be associated with link detection objects configured with IPv6 detection nodes.
- If the detection fails, the route on Ge0/2 is deleted and Ge0/2 does not participate in routing. If the detection result changes to Up again, the route on Ge0/2 is restored and Ge0/2 participates in routing again. Therefore, you are advised to use this feature in a multi-egress scenario and reserve at least one interface not associated with any link detection object as a bypass line.
- If the detection fails, the associated routes become invalid and are deleted from the routing table. If the detection result changes to normal again, the routes are restored and added back to the routing table.


Edit Physical Interface
Basic Info
Interface Name
Ge0/1
Description
Connection Status
Enable
Disable
Mode
Routing Mode
Transparent Mode
Off-Path Mode
Switching Mode
*Zone
untrust
Add Security Zone
Interface Type
WAN Interface
LAN Interface
Address
IP Type
IPv4
IPv6
Connection Type
Static Address
DHCP
PPPoE
No IP Address
Line Bandwidth
Uplink
Mbps
Downlink
Mbps
Access Management
When local defense is disabled, access management cannot be configured, and existing configurations become invalid. To configure access management, please administrator go to Security Defense - Local Defense Enable Local Defense
Permit
HTTPS
PING
SSH
Advanced
ISP Address Library
ISP Address Library
MTU
1500
MAC
00:d0:f8:22:36:d8
Restore Default MAC
Link Detection
test
Add Link Detection
The interface cannot be associated with link detection supporting HTTP. If the detection result indicates an exception, the interface will stop forwarding traffic (and the routes related to the interface will become invalid).
Reverse Path Limited
Save


Back
Edit Static Routing
IP Type
IPv4
* Dest. IP Range/Mask
60.0.0.0/24
Next-Hop Address
Interface
Ge0/2
* Priority
5
Link Detection
test
Description

2. Detection Log

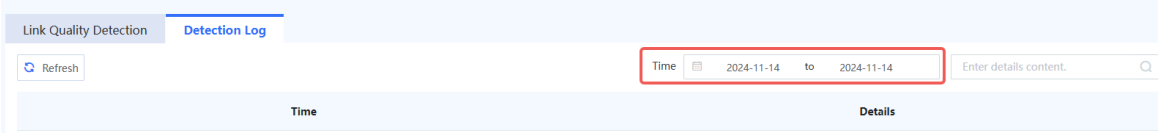
Application Scenario

View historical detection logs on the **Detection Log** tab page.

Procedure

(1) Choose **Network** > **Link Detection** > **Link Quality Detection** > **Detection Log**.

(2) Select the query period and view the detection logs generated within the specified period.



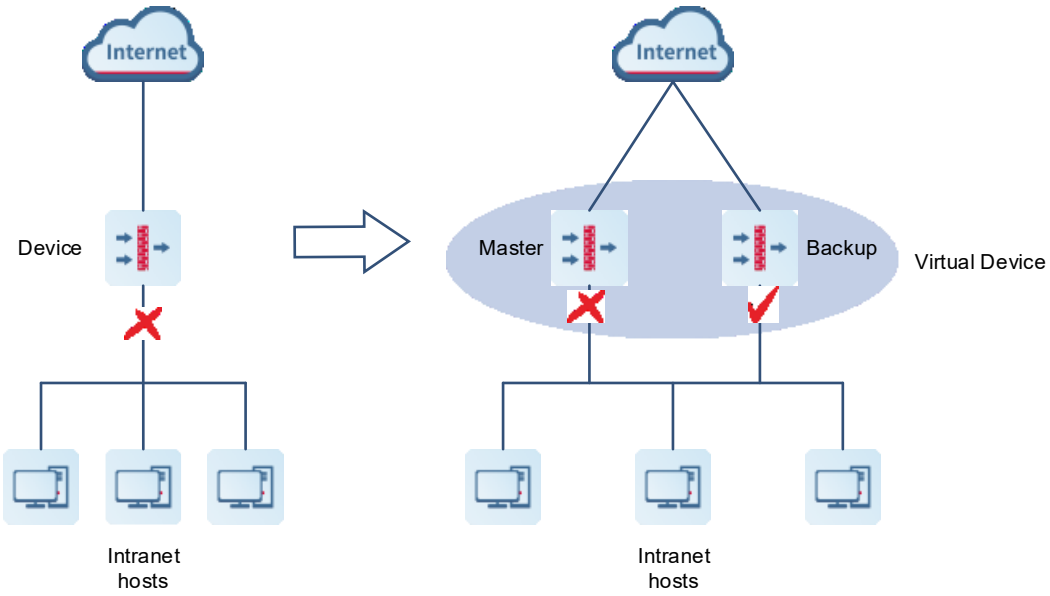
6.15 VRRP

6.15.1 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 external network 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.
- VRRP and high availability cannot be enabled simultaneously.

6.15.2 Working Process

After VRRP is configured, its working process is as follows:

(1) In a VRRP group, a master device is elected among devices based on priorities, while the remaining devices become backup devices. The master device sends gratuitous ARP messages to inform other devices and hosts of its virtual MAC address and is responsible for forwarding packets.

(2) The master device periodically sends VRRP messages to advertise its VRRP state, priority, and other information.

(3) If the master device fails, such as due to an uplink interface failure, a new master device is elected from the backup devices in the VRRP group based on priorities.

(4) Currently, VRRP supports only the preemption mode: When receiving a VRRP message, a backup device compares its priority with that of the master device in the VRRP message. If the backup device 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.)

(5) When the master role is taken by a new device, the new master device sends a gratuitous ARP message containing the MAC address and virtual IP address of the virtual device to notify other hosts and devices to update their ARP information. The new master device is responsible for forwarding packets. Hosts and devices on the network are unaware of the master device switchover.

For enhanced security, VRRP provides plain text authentication. The master device adds an authentication text in the VRRP message and sends it to the backup devices. Upon receiving the VRRP message, the backup device compares the authentication text with its locally configured text. If the authentication texts match, the received VRRP message is considered valid. Otherwise, the backup device regards the VRRP message as an invalid message and discards it.

6.15.3 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.

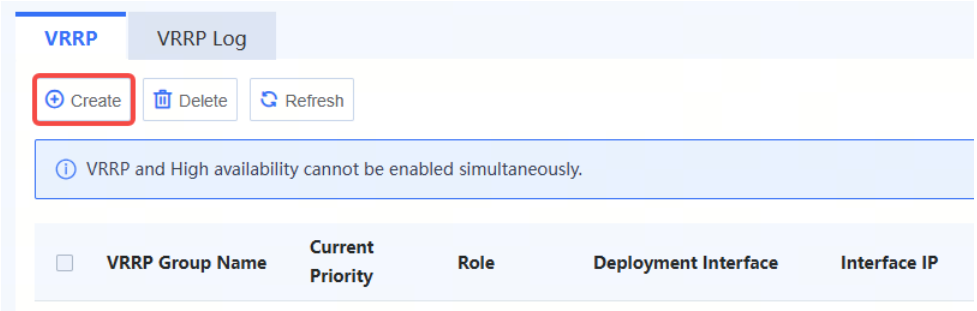
Precautions

To associate a VRRP group with a monitoring interface and link detection, choose **Network** > **Link Detection** > **Link Quality Detection** > **Link Quality Detection** and toggle on **Link Detection**. Otherwise, the detection will not be performed. For details, see 6.14 Link Detection.

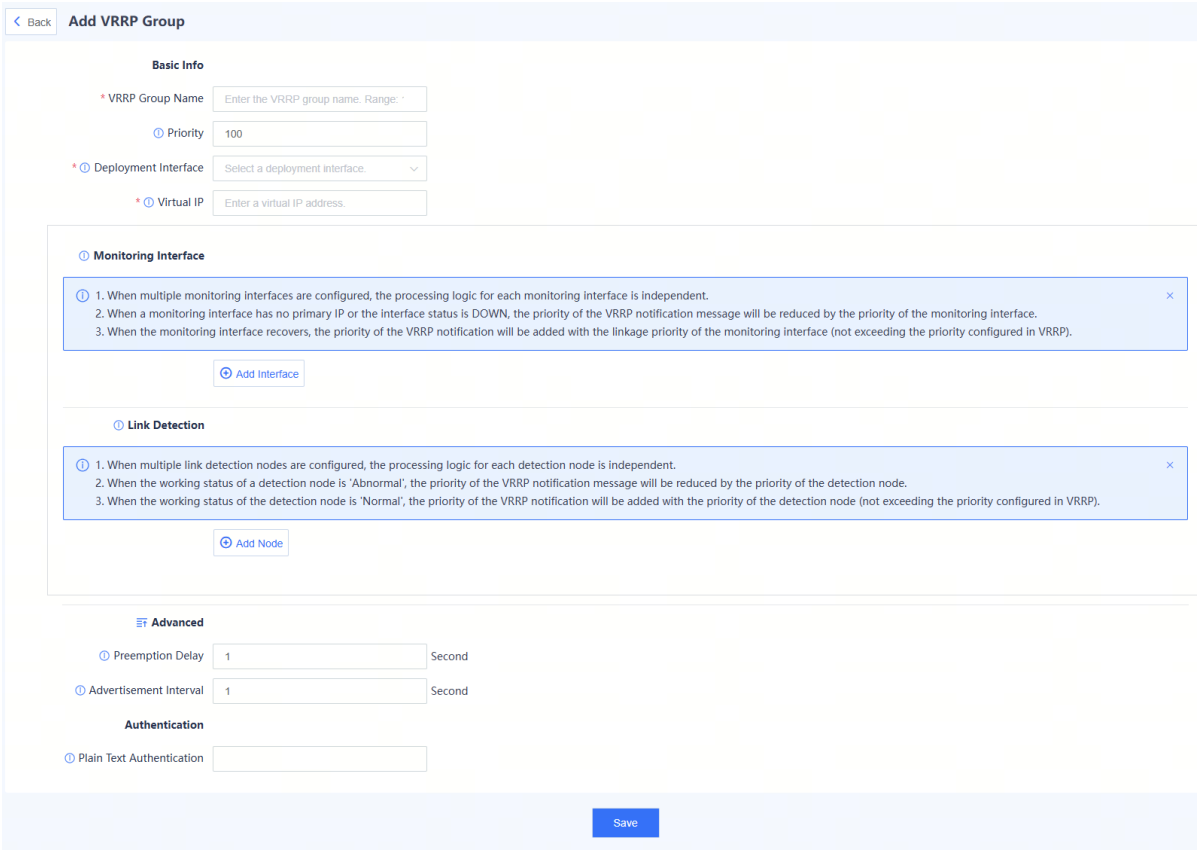
Procedure

(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.



Item	Description	Remarks
Basic Info		
VRRP Group Name	Number of the VRRP group. A group of devices with the same VRRP group name forms a virtual device.	[Example] 1
Priority	The priority of the VRRP group. A larger value indicates a higher priority. In a VRRP group, the device with the highest priority is elected as the master device.	[Example] 254

Item	Description	Remarks
Deployment Interface	Interface on which the VRRP function is enabled. You can specify only a physical interface or logical sub-interface in routing mode configured with an IPv4 address. The deployment interface and monitoring interface cannot be the same.	[Example] Ge0/4
Virtual IP	IP address of the virtual device, which is different from the IP address of the deployment interface but must be on the same network segment as the deployment interface.	[Example] 192.168.1.1
Monitoring Interface The device monitors the Layer 3 interface status and the status of the interfaces associated with the VRRP group on the network for master election. You only need to configure this parameter on the master device. Click **Add Interface** to add a monitoring interface and set its association priority.		
Monitoring Interface	Interface under monitoring and associated with service interface status of the local device. You can only select a physical interface or logical sub-interface configured with an IPv4 address and in the routing mode, which cannot be the same as the interface used for deployment.	[Example] Ge0/2
Association Priority	VRRP priority value changed for the local device when the status of the monitoring interface changes. If the monitoring interface does not have a master IP address or is Down, the priority of the local device in the VRRP group is decreased by the specified value. In this case, another device with a higher priority is elected as the new master of the VRRP group. After the monitoring interface restores normal, the priority of the local device in the VRRP group is increased by the specified value (not greater than the originally configured priority).	[Example] 10
Link Detection The device monitors the link status and the status of the links associated with the VRRP group on the network for master election. You only need to configure this parameter on the master device. Click **Add Node** to add a link detection object.		

Item	Description	Remarks
Association Priority	VRRP priority value changed for the local device when the working status of the link detection node changes. If the working status of the detection node is **Exception**, the priority of the local device in the VRRP group is decreased by the specified value. In this case, another device with a higher priority is elected as the new master of the VRRP group. After the working status of the detection node restores normal, the priority of the local device in the VRRP group is increased by the specified value (not greater than the originally configured priority).	[Example] 10
Protocol	Detection protocol type.	[Example] ICMP
To-Be-Detected Dest. IP	IP address of the detection node when the protocol type is ICMP or TCP.	[Example] 192.168.2.2
To-Be-Detected DNS Server	IP address of the DNS server to be detected when the protocol type is DNS.	[Example] 192.168.2.2
Domain Name	Domain name to be detected when the protocol type is DNS.	[Example] www.test.com
Port	Port to be detected when the protocol type is DNS or TCP.	[Example] 53
To-Be-Detected URL	URL to be detected when the protocol type is HTTP or HTTPS.	● Only exact match is supported. ● You can enter a port number at the end of the URL. [Example] http://www.ruijie.com:53
Outbound Interface	Outbound interface for node detection.	[Example] Ge0/2
Src. IP	Source IP address for node detection.	[Example] 192.168.2.1

Item	Description	Remarks
Next-Hop Address	Next-hop IP address of the route destined for the detection node.	This parameter is available when the protocol type is ICMP, DNS, or TCP. [Example] 192.168.2.1
Detection Frequency	Interval for sending detection packets.	[Example] 10000 ms
Retries	Number of retries for detection failure. If the number of consecutive detection failures reaches the specified value, the device considers that the node is abnormal and changes the detection status to Down. For example, if the detection frequency is 10 seconds and the number of retries is 5, the interface sends a detection packet every 10 seconds. If no response is received for five consecutive times, the interface considers that an exception occurs and the detection result is Down.	[Example] 5
Recovery Times	Number of times for node recovery detection. If the number of consecutive detection successes reaches the specified value, the device considers that the node restores normal. For example, if the detection frequency is 10 seconds and the number of recovery times is 3, the interface sends a detection packet every 10 seconds. If the response packet is received successfully for three consecutive times, the device considers that the link restores normal and the detection status changes to Up.	[Example] 3
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

Item	Description	Remarks
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

(4) Confirm the configuration and click **Save**.

Follow-up Procedure

- Choose **Policy** > **Security Defense** > **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.
- Check the configuration information and monitoring status (including the monitoring interface and detected links) in the VRRP list after configuring a VRRP group.

6.15.4 Viewing VRRP Logs

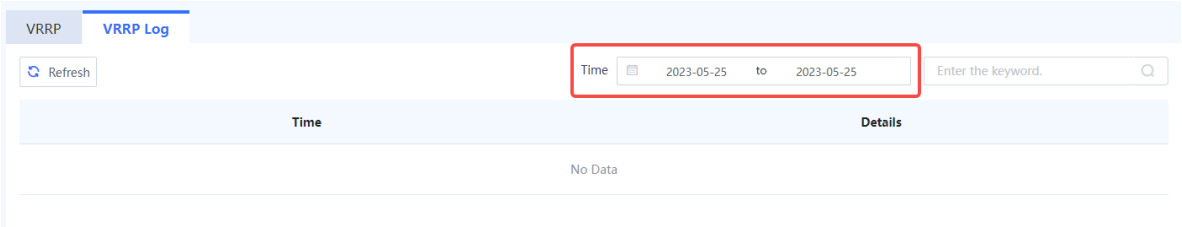
Application Scenario

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

(1) Choose **Network** > **VRRP**. Click the **VRRP Log**.

(2) Select a query period and the **VRRP Log** tab page displays the logs generated within the specified period.



6.16 Neighbor Status

6.16.1 ARP Entries

Application Scenario

ARP entries can be classified into dynamic ARP entries and static ARP entries. The difference between them is as follows:

- Dynamic ARP entries are automatically learned, generated, and updated by the ARP protocol based on ARP message exchange. These entries can be aged out and overwritten by new dynamic ARP entries.
- Static ARP entries are manually configured and maintained by the network administrator. These entries

cannot be aged out or overwritten by dynamic ARP entries.

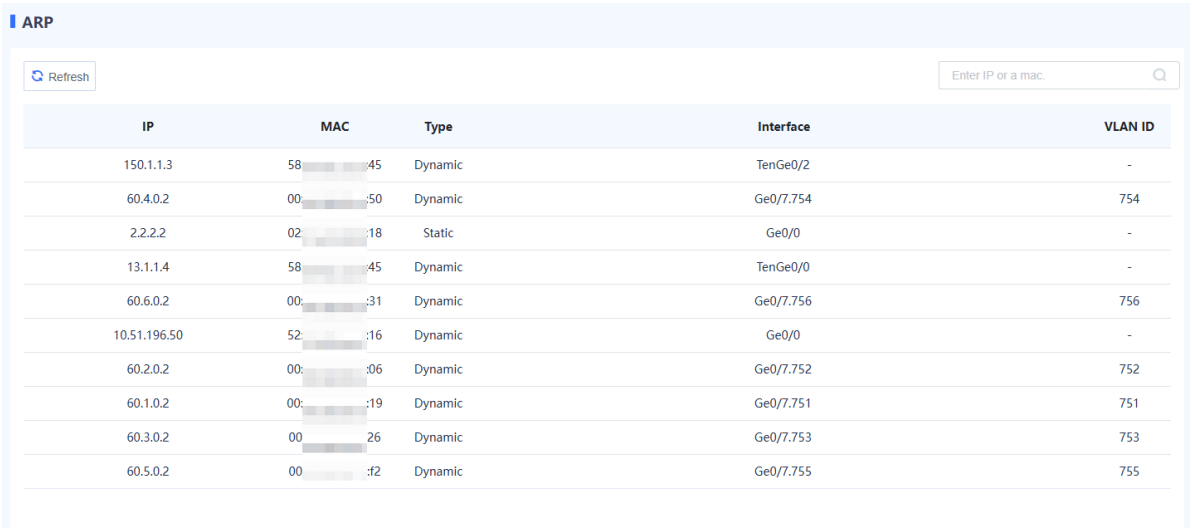
This page displays all ARP entries. For details about static ARP entries, see 4.7.7 IP-MAC Binding.

Procedure

Choose **Network** > **Neighbor Status** > **ARP** to view ARP entries.

Note

To bind the IP address and MAC address in an ARP entry, choose **Policy** > **Security Defense** > **IP-MAC Binding**. For details about IP-MAC binding, see 4.7.7 IP-MAC Binding.



6.16.2 ND Entries

Application Scenario

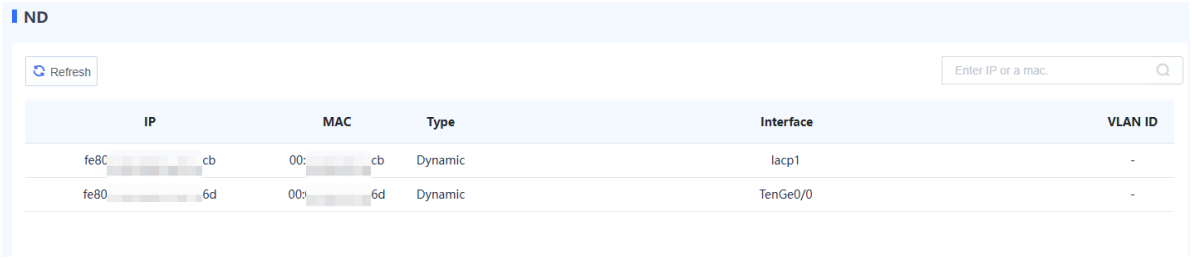
ND entries can be classified into dynamic ND entries and static ND entries. The difference between them is as follows:

- Dynamic ND entries are automatically learned, generated, and updated by the ND protocol based on ND message exchange. These entries can be aged out and overwritten by new dynamic ND entries.
- Static ND entries are manually configured and maintained by the network administrator. These entries cannot be aged out or overwritten by dynamic ND entries.

The following describes dynamic ND entries. For details about static ND entries, see 4.7.7 IP-MAC Binding.

Procedure

Choose **Network** > **Neighbor Status** > **ND** to view dynamic ND entries.



6.16.3 LLDP

1. Enabling LLDP

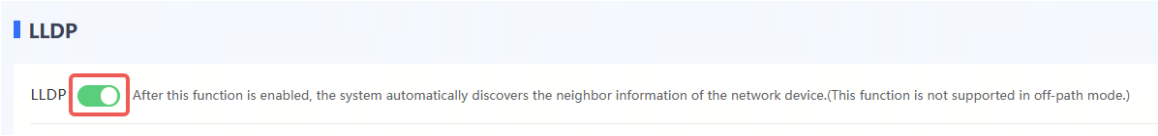
Application Scenario

After the Link Layer Discovery Protocol (LLDP) function is enabled, the device can automatically discover neighbors on the network. LLDP helps the network administrator quickly obtain the network topology and changes in the topology.

Procedure

(1) Choose **Network** > **Neighbor Status** > **LLDP**.

(2) Enable LLDP globally.



Follow-up Procedure

When LLDP is enabled, you can toggle off the LLDP switch to disable this function. After LLDP is disabled, the device will stop discovering neighbors of network devices and the discovered neighbor information will be hidden.

2. Viewing the Neighbor Device Information

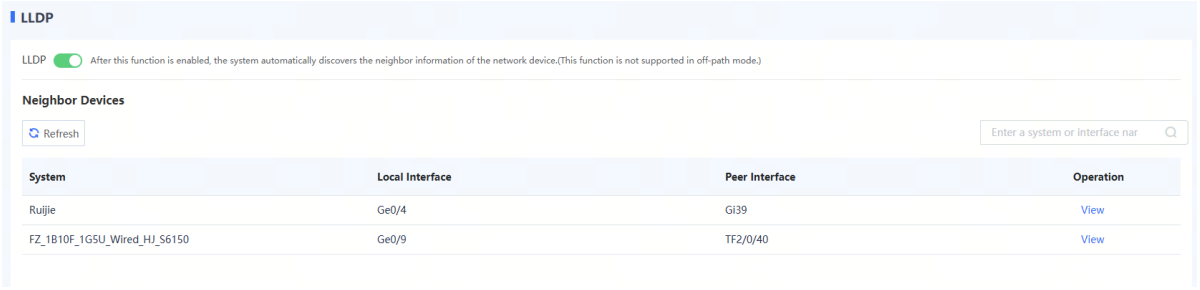
Application Scenario

After the LLDP function is enabled, the administrator can view the LLDP neighbor information of device interfaces on the page.

Procedure

(1) Choose **Network** > **Neighbor Status** > **LLDP**.

(2) Information about the discovered neighboring devices is displayed on the page.



(3) Click **View** to view the detailed information.

7 System Management

7.1 Administrators

7.1.1 Overview

The CF 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 7-1.

Table 7-1 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	● No permission on **Admin** menus under **System** ● Read-write permissions on other menus	securityadmin
Auditor	● Read permission on **Home** menus ● Read permission on **O&M** menus (except for **Fault Diagnosis**) ● No permissions on other menus	auditadmin
User Admin	● Read permission on **Home** menus ● Read-write permissions on **Admin** menus under **System** ● No permissions on other menus	useradmin

7.1.2 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.

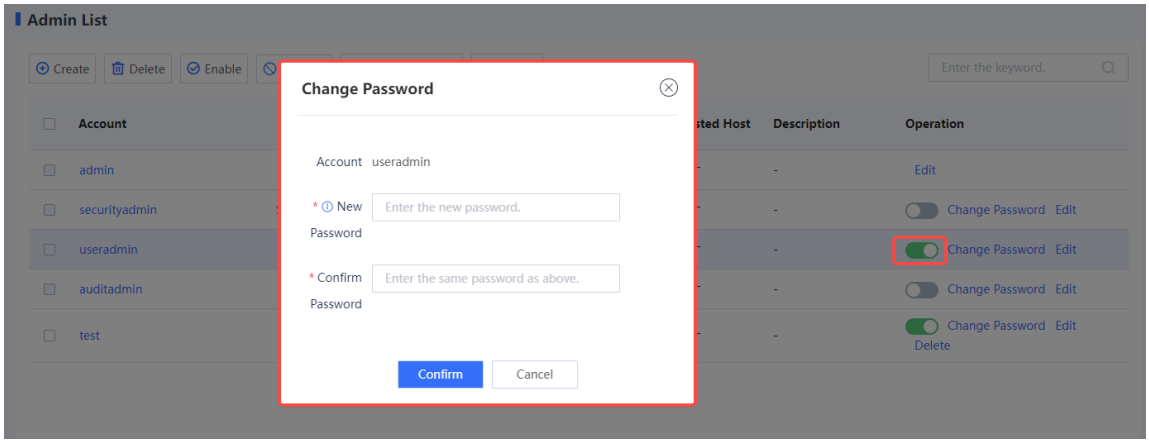
Procedure

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

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.

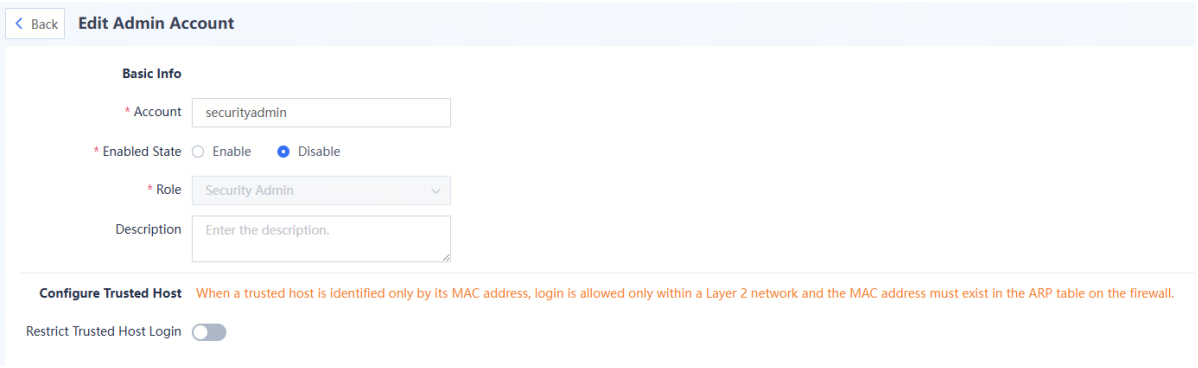
A valid password should meet the following format requirements:

- 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.

(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.



- The default administrator account cannot be deleted.

7.1.3 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 7-2 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.

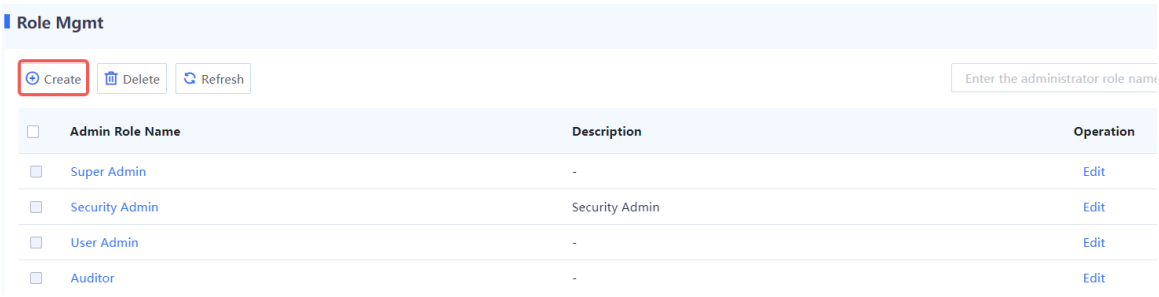
When creating an administrator, you can assign the default role to the administrator. You can also create new roles as required.

Procedure

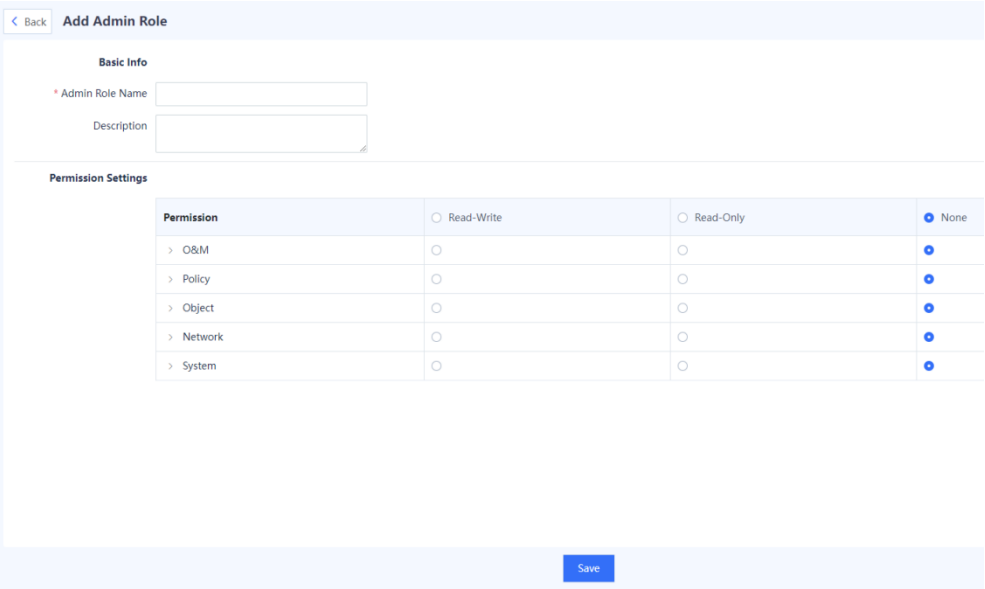
(1) Access the **Add Admin Role** page.

a Choose **System** > **Admin** > **Role Mgmt**.

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.	-
Permission Type	Permission types of the new administrator role, including: ● **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.

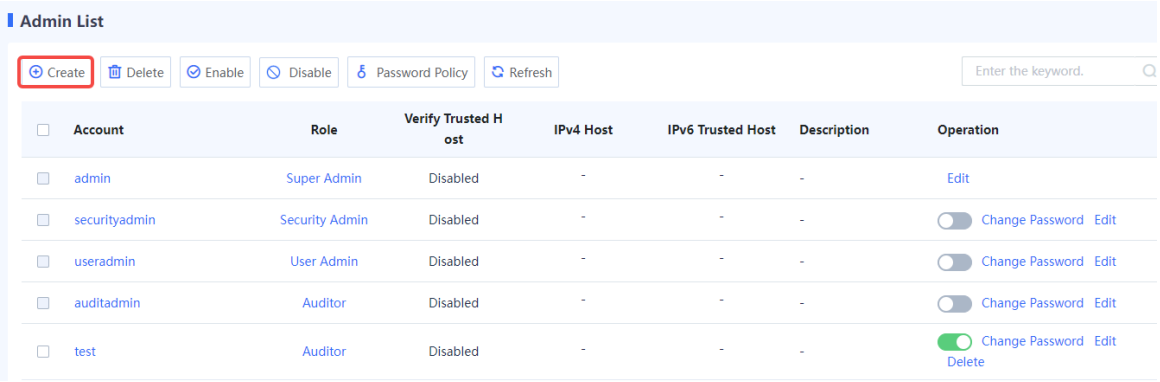
Both the super administrator and user administrator have the permission to create an administrator account.

Procedure

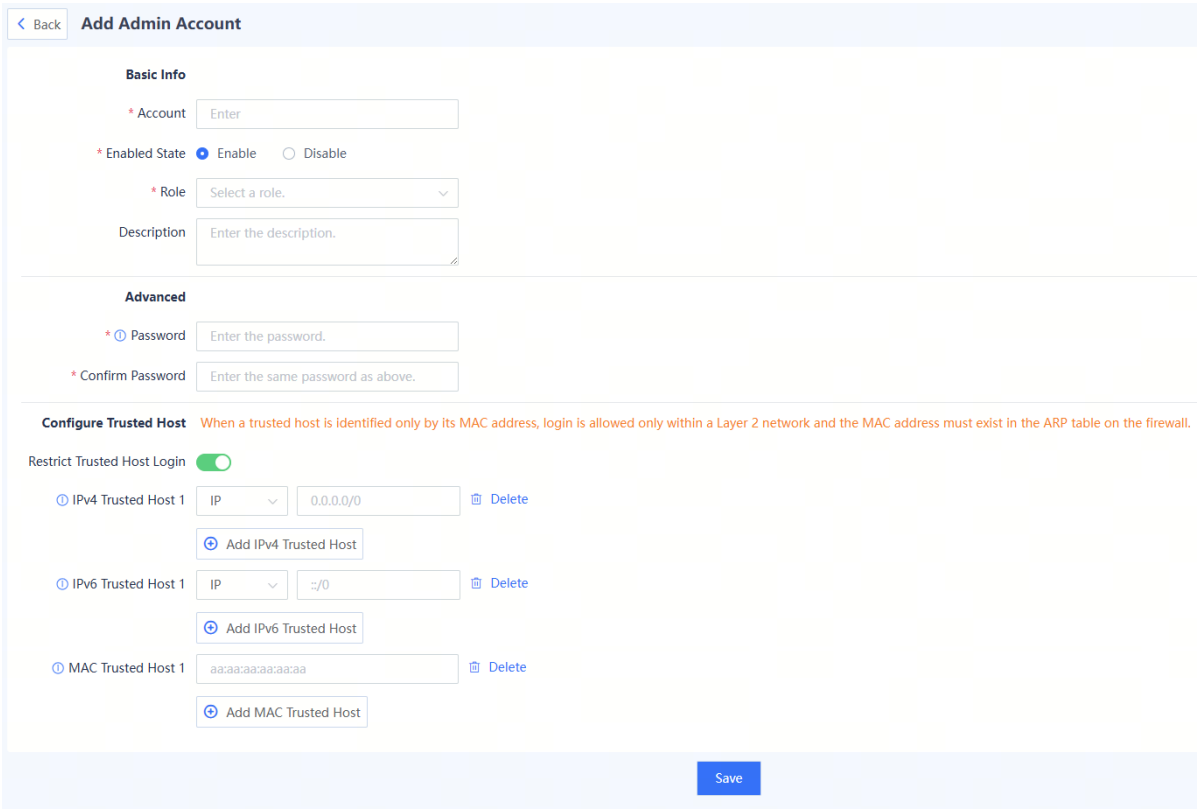
(1) Access the **Add Admin Account** page.

a Choose **System** > **Admin** > **Account Mgmt**.

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



(2) Set parameters for the new administrator.



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

Item	Description	Remarks
Password	Password used by the new administrator to log in to the web UI.	● 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 Note: If a trusted host is configured with only a MAC address, you can log in to the device only over a Layer 2 network, and the MAC address must exist in the ARP table of the device. Otherwise, the login will fail. For details about ARP entries, see 6.16.1 ARP Entries.		
Restrict Trusted Host Login	If this function is enabled, the account can only log in to the firewall using a specified IP address or MAC address (trusted host).	[Example] Enable
IPv4 Trusted Host	IPv4 address or IPv4 address plus MAC address of a trusted host.	[Example] 192.168.1.1
IPv6 Trusted Host	IPv6 address or IPv6 address plus MAC address of a trusted host.	[Example] 333:444:0:1::1
MAC Trusted Host	MAC address of a trusted host.	[Example] aa:aa:bb:aa:bb:bb

(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.

7.1.4 Modifying the Administrator Password Security Policy

Application Scenario

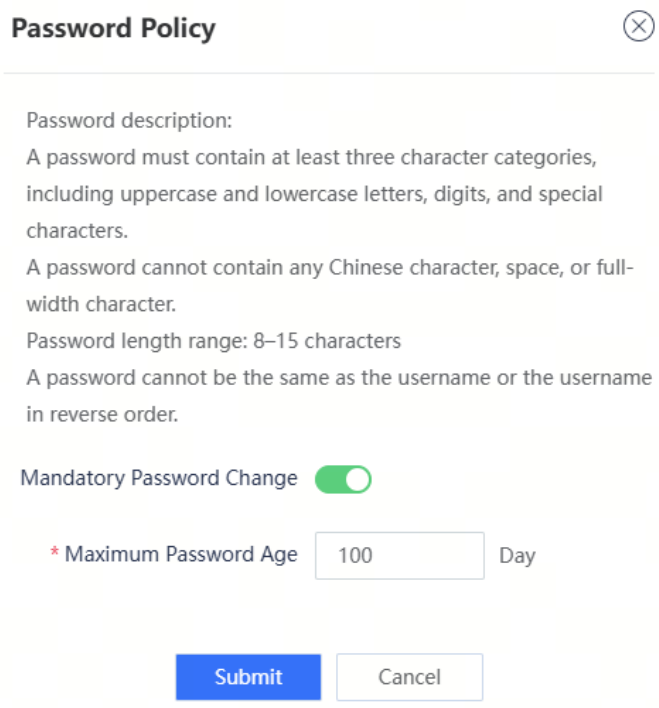
To ensure the security of an administrator password, the account and password must be modified periodically. You can set a validity period for a password. After a password expires, the system forces the user to change the password.

Procedure

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

a Choose **System** > **Admin** > **Account Mgmt**.

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



(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.

7.1.5 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.

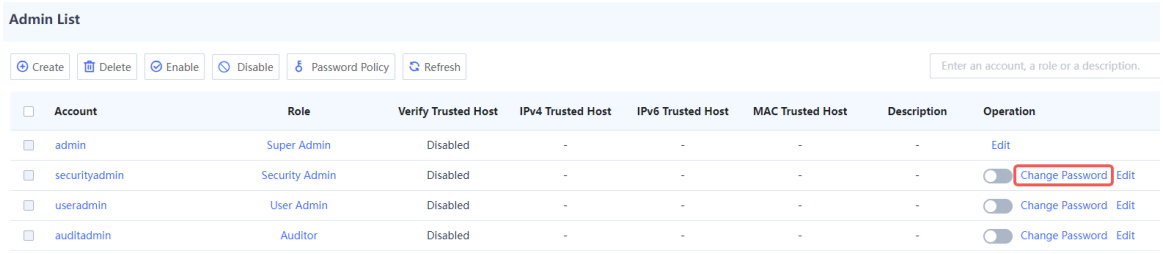
- The **admin** account can be used to modify the login passwords of other administrators.
- The **useradmin** account can be used to modify the login passwords of other administrators except for the **admin** account.

Procedure

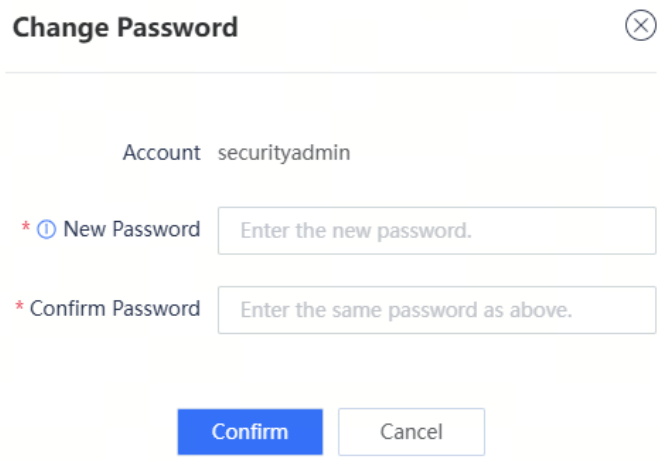
(1) Access the **Change Password** page.

a Choose **System** > **Admin** > **Account Mgmt**.

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



(2) Set a new password for the administrator.



- 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**.

7.2 System Configuration

You can modify the system time and service parameters, as well as import licenses in system configuration.

7.2.1 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

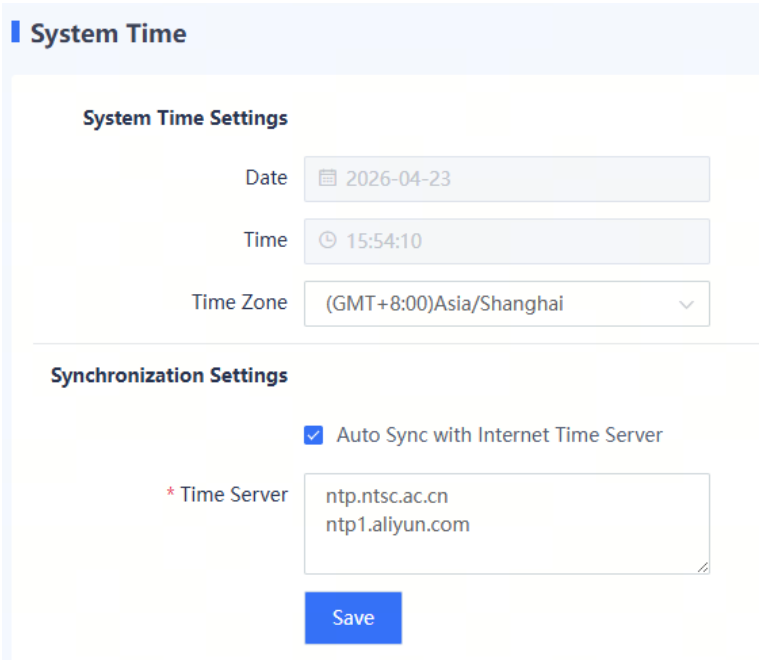
The system time setting consists of manual setting and automatic synchronization:

- 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.

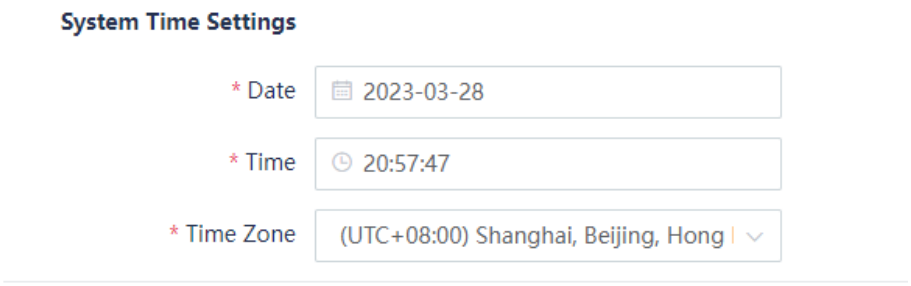
Choose **System** > **System Config** > **System Time**.



(2) Select different setting methods as required.

- Manual time synchronization

  In the **System Time Settings** area, set the date, time, and time zone.

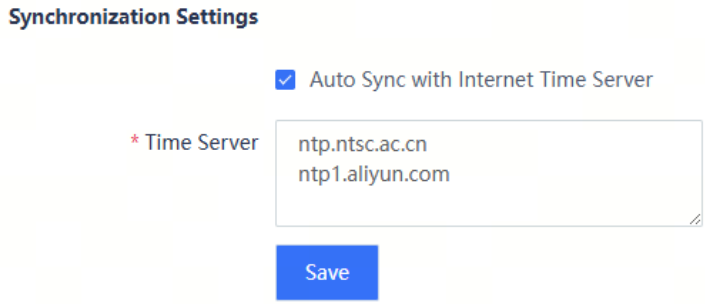


- Automatic time synchronization

  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.



(3) Click **Save**.

After you complete the configuration of automatic time synchronization, the system synchronizes the time within a few minutes.

7.2.2 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:

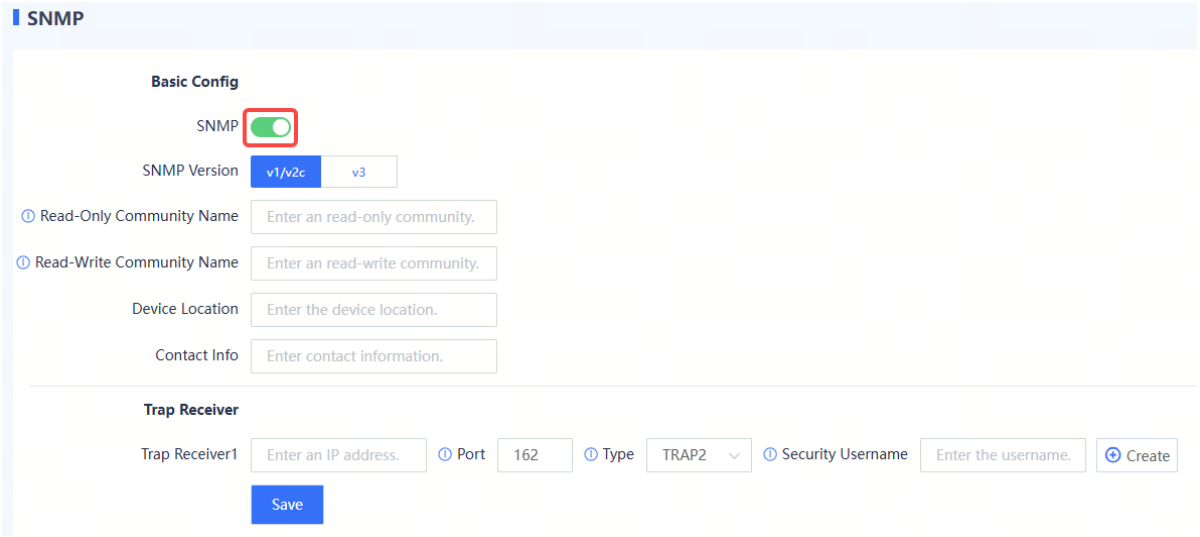
  - Ensures that data is not tampered during the transmission.
  - Ensures that data is sent by a valid data source.
  - Encrypts packets to ensure data confidentiality.

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		

Item	Description	Remarks
Read-Only Community Name	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. [Example] public
Read-Write Community Name	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. [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. [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
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

Item	Description	Remarks
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.	Enter a valid IPv4/IPv6 address. Example: 192.168.1.1 or 1234::100.
Port	Number of the port used by the managed device to send a Trap message to the destination host. The default value is **162**.	[Example] 162
Type	Trap type. The options are **TRAP**, **TRAP2**, and **INFORM**.	The type is **TRAP2** in most cases. [Example] TRAP2
Security Username	Credential used by the device to report alarm information to the NMS server.	The value must be the same as that on the NMS server. [Example] user1

(4) Click **Save**.

7.2.3 Configuring Service Parameters

1. Modifying the Web Login Configuration

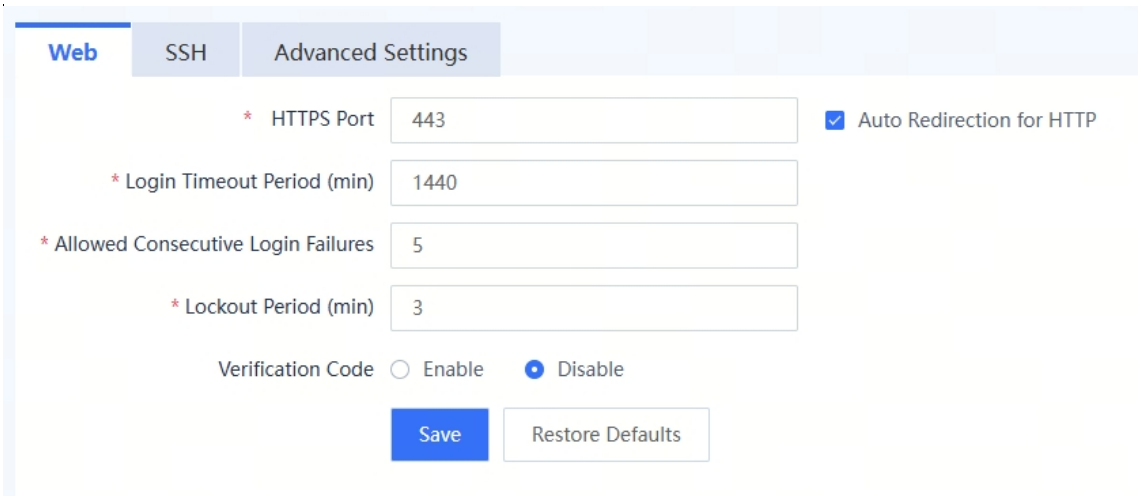
Application Scenario

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
HTTPS port	Port number used by the web service. The device supports automatic HTTP redirection. When users access the management address through HTTP, they are automatically redirected to the HTTPS address.	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.	Enter an integer in the range of 0 to 1440, in minutes. The default value is 30 minutes. [Example] 30
Allowed Consecutive Login Failures	Number of consecutive incorrect password attempts. If a user enters an incorrect password for a number of times exceeding the value specified by this parameter, the system automatically locks the user.	● Enter an integer in the range of 1 to 10. ● The default value is 6. [Example] 3

Item	Description	Remarks
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 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

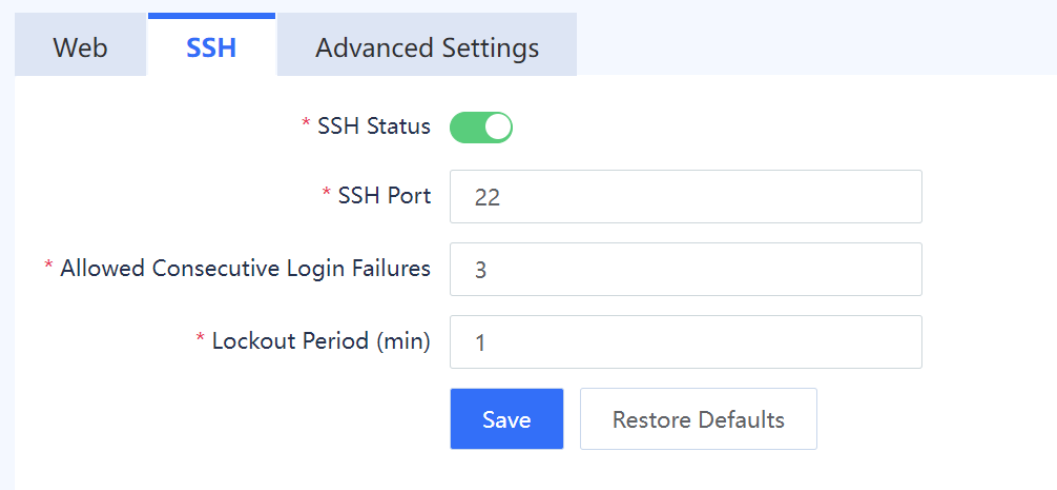
Application Scenario

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.



(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**.

Item	Description	Remarks
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. TCP State Check

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. The administrator can choose the TCP state check mode as required.

TCP connection status detection supports the following modes:

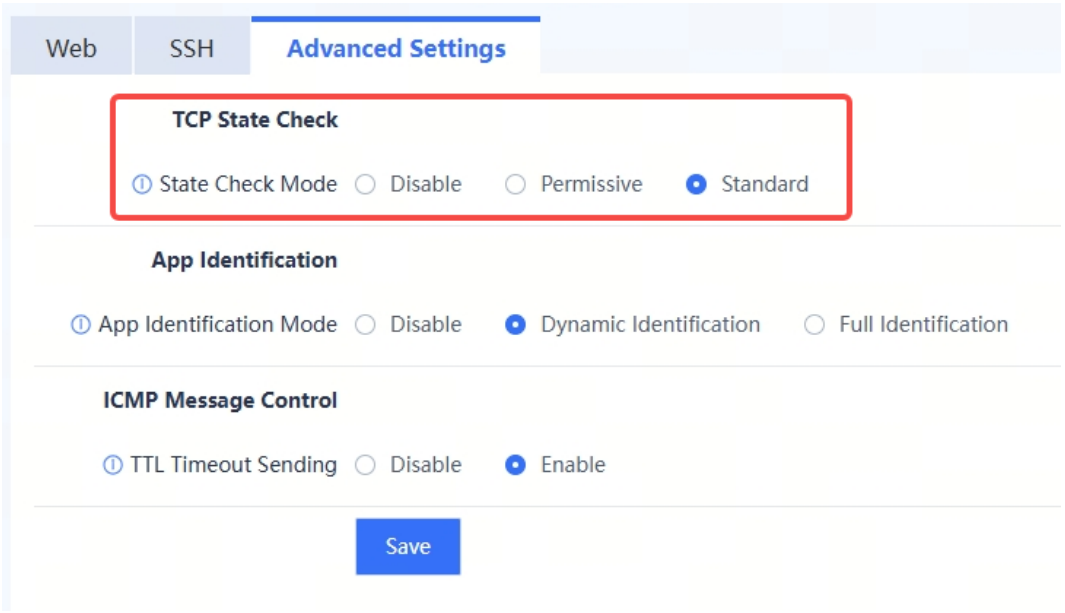
- Disable: In this mode, the device does not trace or detect the TCP traffic exchange process.
- Permissive: In this mode, the device permits TCP traffic that has not completed the handshake process. After TCP connection status check is enabled, the device tracks the status of TCP connections and considers only those TCP connections that complete the handshake process valid. However, in some special scenarios such as active/standby switchovers of HA devices, a device may fail to detect the complete connection status though a TCP connection has completed handshake. To avoid TCP connection interruption caused by incorrect discard of ACK packets in this case, configure the permissive mode for TCP connection status

check.

- Standard: In this mode, the device tracks and detects whether the interactive process of TCP traffic is valid. Only TCP traffic with complete handshake process is allowed to pass through.

Procedure

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



(2) Set the TCP connection status check mode and click **Save**.

4. Application Identification Mode

Application Scenario

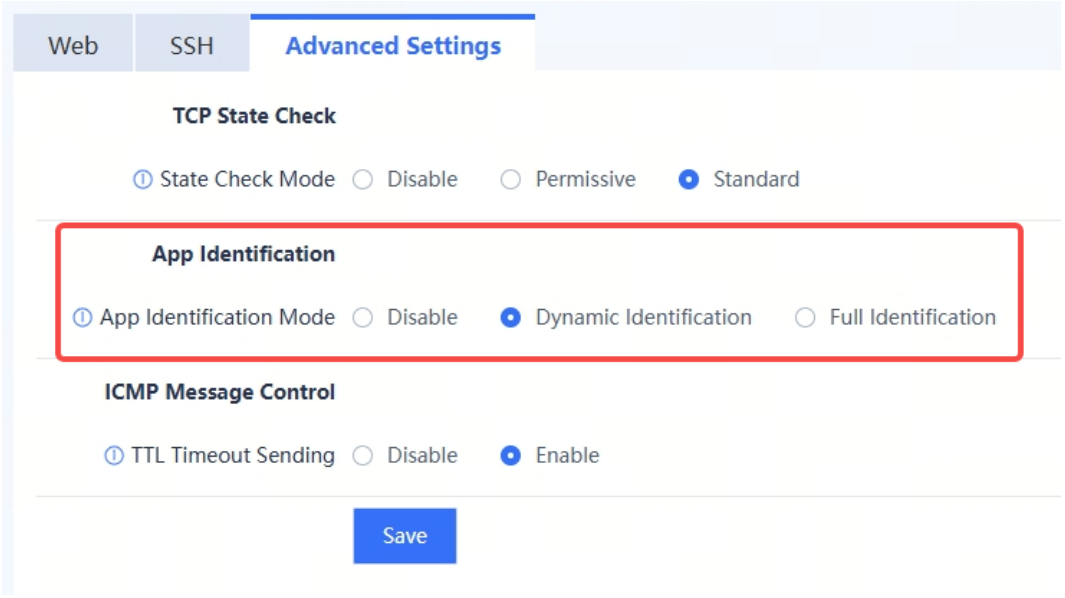
The application identification function identifies the application layer protocol to which the packet belongs and determines the application to which the traffic belongs. The administrator can control and monitor traffic based on the application identification result.

The device supports the following application identification modes:

- Full identification: The device performs application identification on all traffic.
- Dynamic identification: The device performs application identification on traffic only when the service requires such result, such as flow analysis and control.
- Disable: The application identification function is disabled and application identification is not performed on all traffic.

Procedure

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



(2) Select the service identification mode and click **Save**.

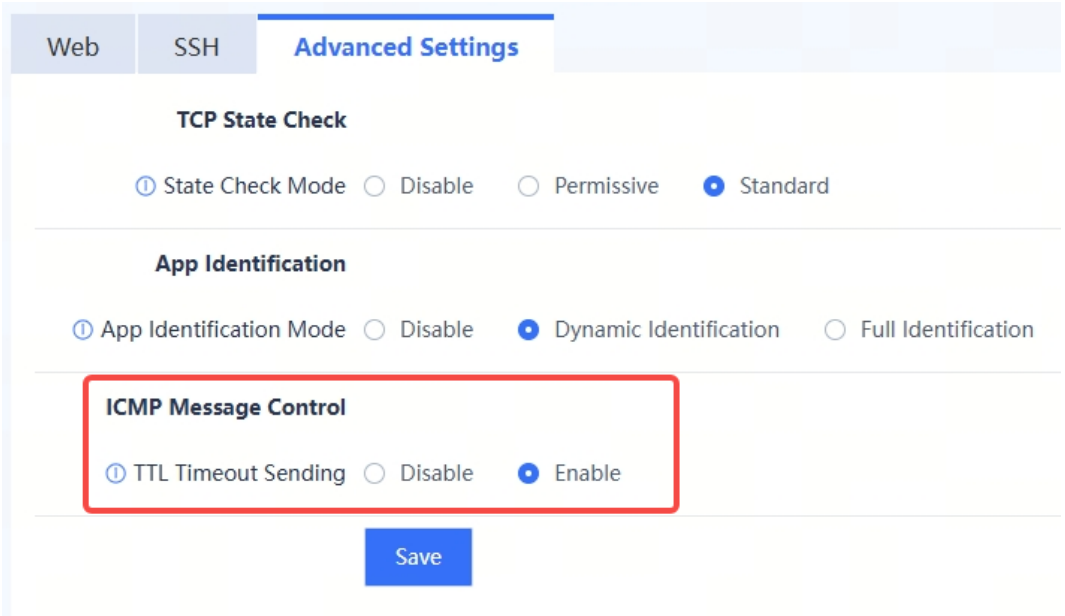
5. ICMP Message Control

Application Scenario

Traceroute network debugging is used to trace the path of data packets from the user end to the target object. After this function is enabled, the IP address of the local device will be displayed when the user end performs a traceroute test.

Procedure

(1) Choose **System** > **System Config** > **Service Parameters** > **Advanced Settings**.



(2) Configure whether to enable TTL timeout message sending, and click **Save**.

7.2.4 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.

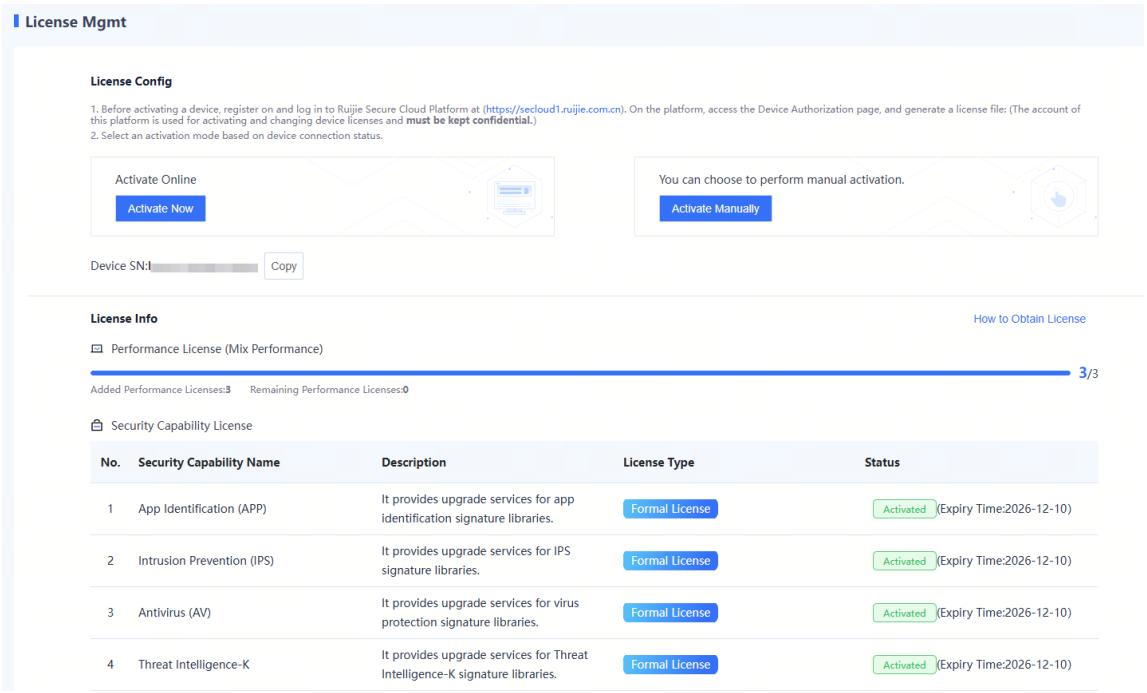
Prerequisites

You have performed the following operations: Log in to the Ruijie Secure Cloud Platform (https://secloud1.ruijie.com.cn), and choose **License Management** from the main menu. On the page that is displayed, click **License Activation**, and generate a license file.

Procedure

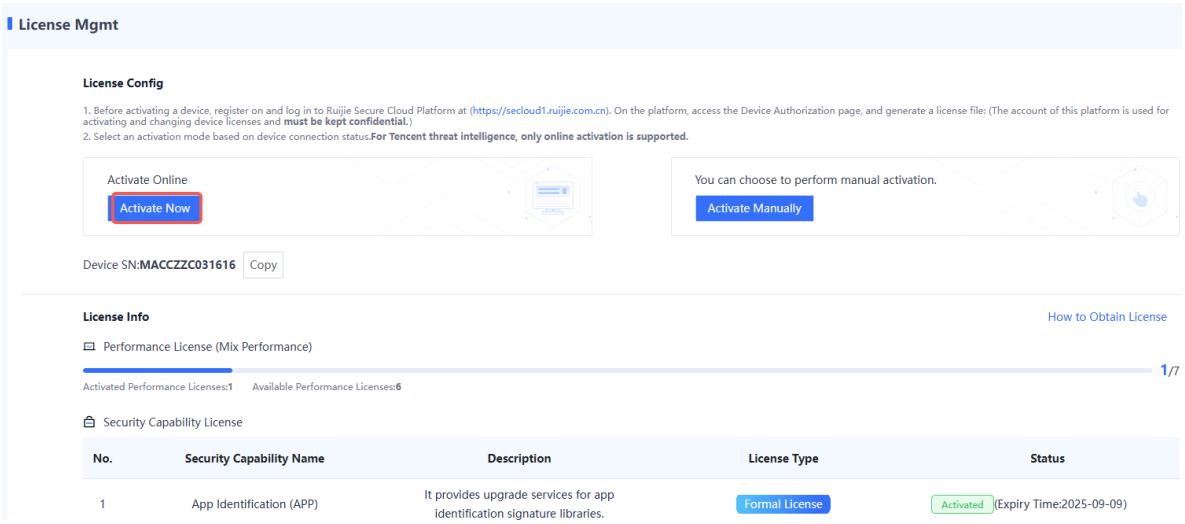
(1) Access the **License Mgmt** page.

Choose **System** > **System Config** > **License Mgmt**.

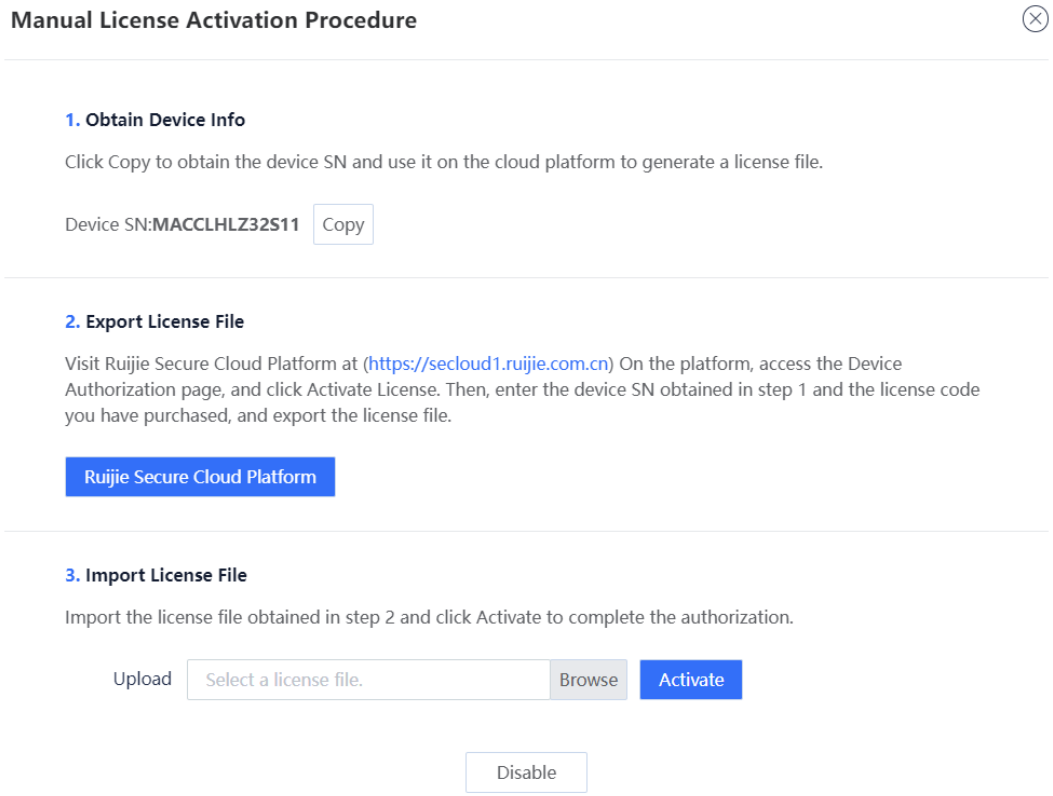


(2) Select an activation mode.

- To perform online activation, click **Active Now**.

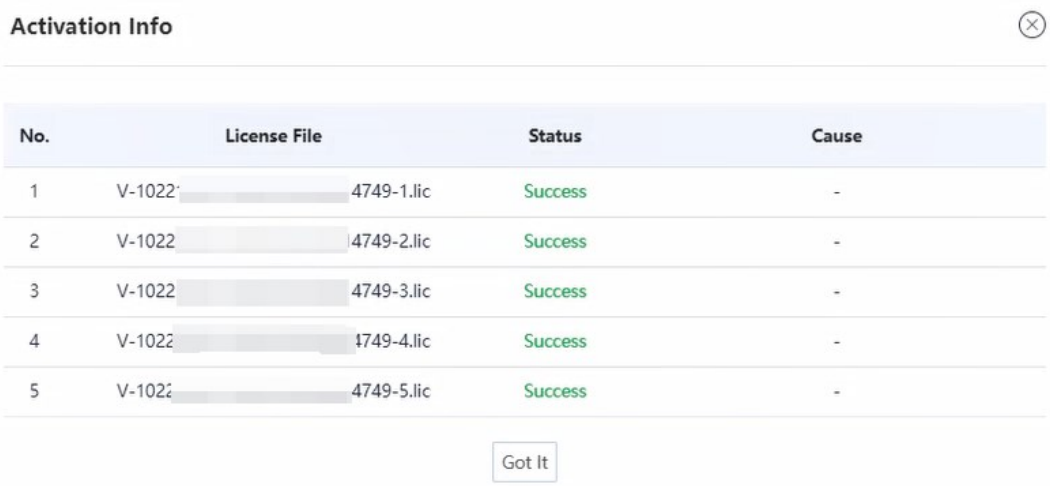


- To perform manual activation, click **Activate Manually**, upload the license file (in .zip or .lic format), and click **Activate**.



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

Figure 7-1 Successful License Activation



7.2.5 Hardware Acceleration

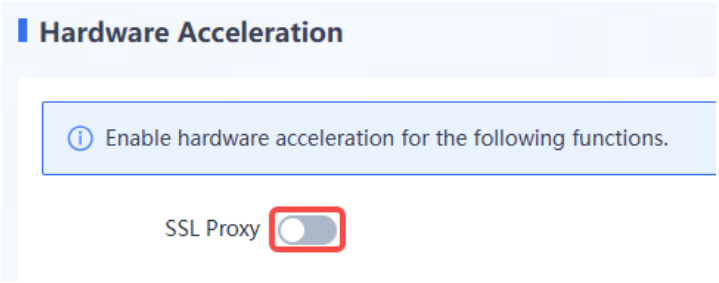
Application Scenario

You can enable hardware acceleration to improve the running performance of some functions and obtain better user experience.

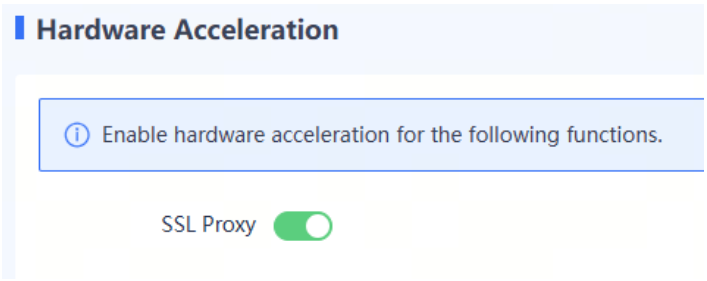
Procedure

(1) Choose **System** > **System Config** > **Hardware Acceleration**.

(2) Toggle on **SSL Proxy** to enable hardware acceleration for the specified functions.



(3) Hardware acceleration is enabled successfully, as shown in the following figure.



7.3 Association Configuration

7.3.1 Identity System Association

Application Scenario

The real-name user information synchronization function can be used to send authenticated user information on the local device to other devices (Ruijie security products) or allow the local device to receive authenticated user information from other devices (Ruijie security products). This achieves real-name user information synchronization between different authentication systems.

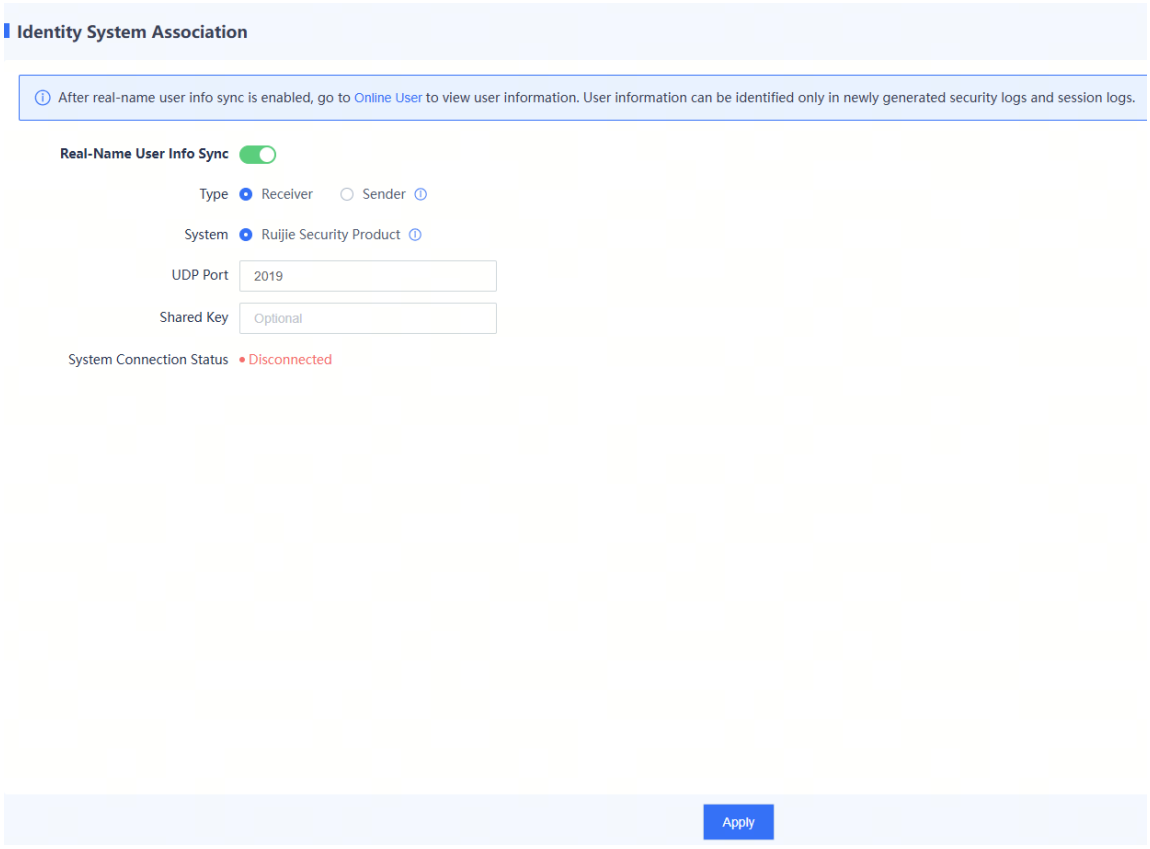
Prerequisites

Two devices can communicate with each other.

Procedure

(1) Choose **System** > **Association Config** > **Identity System Association**.

(2) Toggle on to enable the function and configure related information.



Item	Description	Remarks
Real-Name User Info Sync		

Item	Description	Remarks
Type	**Receiver**: Another device functions as the user authentication system, and the local device is used to receive user authentication information from the peer authentication device. **Sender**: When the device serves as the user authentication system, it synchronizes user authentication information to other Ruijie security product.	[Example] Receiver
Receiver		
System	User authentication system that can interoperate with the device. Only Ruijie security devices are supported.	[Example] Ruijie Security Product
UDP Port	UDP port for interconnecting the local device with the peer authentication device.	The UDP port number must be the same as that of the peer end; otherwise, synchronization fails. [Example] 2019
Shared Key	The local and remote devices use the key to encapsulate exchanged information.	[Example] Test12
System Connection Status	Status of the connection with the peer user authentication system.	-
Sender		
System	Only ruijie security products are supported as the user authentication system that can interoperate with the device.	[Example] Ruijie Security Product
Receiver IP	IP address of the peer device that receives user authentication synchronization information.	[Example] 192.168.21.2
UDP Port	UDP port used by the local device to communicate with the peer device that receives user authentication information.	The UDP port number must be the same as that on the peer end; otherwise, synchronization fails. [Example] 2019
Shared Key	The local and remote devices use this key to encapsulate and exchange information.	[Example] Test123

Item	Description	Remarks
Sending Source	**Default (Auto Routing)**: The device automatically selects a route to send user information to the peer device. **Interface**: The device sends user information to the peer device through a specified interface.	[Example] **Default (Auto Routing)**

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

7.3.2 Network Device Association

Application Scenario

The device can trace the MAC address and access point of terminals.

When terminal MAC identification is enabled, the device can identify the MAC addresses of terminals through SNMP or by analyzing DHCP packets. Newly generated logs will automatically display the MAC addresses.

After the function of identifying the access point of a terminal is enabled, the device can identify the physical location of the terminal access point through SNMP, and the related logs that are newly generated automatically display the location information.

Precautions

When multiple terminals are connected to an interface of an access switch, the access point of the terminals cannot be traced (for example, an unauthorized switch or hub).

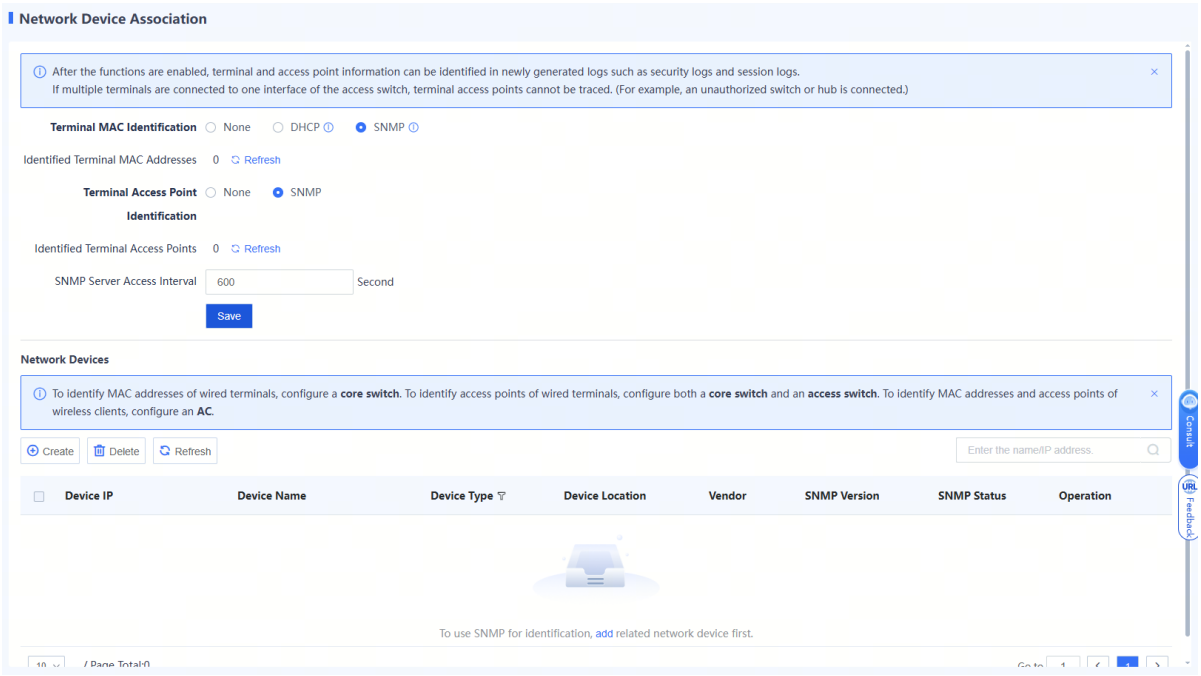
Prerequisites

- To enable terminal MAC identification by analyzing DHCP packets, ensure that the DHCP function has been configured, or other devices on the network can send DHCP packets to the local device. The scenarios are as follows:
  - The device functions as a DHCP server.
  - When the device functions as a DHCP relay agent.
  - The device interface is configured to work in transparent mode (Layer 2 interface) to obtain DHCP packets.
  - The device interface is configured to work in bypass mode, and DHCP packets can be obtained through switch mirroring.
- To identify the MAC address or access point of a terminal through SNMP, you need to configure the related network device (SNMP server) first.

Procedure

(1) Choose **System** > **Association Config** > **Network Device Association**.

(2) Complete configurations of the terminal MAC address and access point identification function.



Item	Description	Remarks
Terminal MAC Identification	● **None**: Disable terminal MAC identification. ● **DHCP**: Use DHCP to identify the MAC addresses of terminals. ● **SNMP**: Use SNMP to identify the MAC addresses of terminals.	[Example] DHCP
Terminal Access Point Identification	● None: The function of identifying the access point is disabled. ● SNMP: SNMP is used to identify the terminal access point. You need to select SNMP to identify the terminal MAC address before using this function.	[Example] SNMP
SNMP Server Access Interval	Interval for accessing the SNMP server.	This parameter can be configured only when SNMP is used for identification. [Example] 600 seconds
Network Devices The firewall communicates with the NAS (SNMP server) through SNMP to obtain MAC addresses of terminals or access points.		

Item	Description	Remarks
Device Type	Type of the configured network device. ● To enable the function of identifying the MAC address of wired terminals, configure a core switch. ● To enable the wired terminal access point identification function, you need to configure both a core switch and an access switch. If the wired terminal is only directly connected to the firewall through the access switch, the firewall needs to be configured as the core switch and the SNMP service needs to be enabled on the firewall. For details, see 7.2.2 Configuring SNMP. ● To enable the function of identifying the MAC address of an STA and the access point (AP), configure the AC.	[Example] Core
Device IP	IP address of the network device.	Enter a valid IPv4 or IPv6 address. Example: 192.168.1.1 or 1234::100
Device Name	Name of the network device.	[Example] Device1
Device Location	Physical location of the network device for quick locating.	[Example] Equipment room 1
Vendor	Vendor of the network device.	Select a value from the drop-down list.
SNMP Version	Version number of SNMP. The options are **v2c** and **v3**.	The selected version must match that on the SNMP server. [Example] v3
v2c		
SNMP Community Name	Community name used for authentication between the device and SNMP server.	The value must be the same as that on the SNMP server. [Example] public
v3		
Security Username	Username used for authentication between the device and SNMP server.	The value must be the same as that on the SNMP server. [Example] user1

Item	Description	Remarks
Authentication Algorithm	Authentication algorithm used for authentication between the device and SNMP server. MD5 and SHA algorithms are supported.	The value must be the same as that on the SNMP server. [Example] MD5
Authentication Key	Password used for authentication between the device and SNMP server.	The value must be the same as that configured on the SNMP server. [Example] authkey
Encryption Algorithm	Encryption algorithm used to encrypt the data transmitted between the device and SNMP server. AES and DES algorithms are supported.	The value must be the same as that on the SNMP server. [Example] AES
Encryption Key	Key used to encrypt the transmitted data.	The value must be the same as that configured on the SNMP server. [Example] prikey

Follow-up Procedure

- The SNMP service must be enabled on the core switch, and AC, and the SNMP parameters must be consistent with those on the firewall. For example, if an associated network device runs SNMPv2c, you need to enable the SNMP service on the network device and configure the same SNMP community name as that on the firewall.
- On the **O&M** > **Security** > **Source Tracing**, **O&M** > **Logs** > **Security Log**, **O&M** > **Logs** > **Session Log**, or **O&M > Logs** > **Behavior Analysis Log** > **URL Analysis** page, click a log to view its details and check identified MAC addresses.

7.4 Log Configuration

7.4.1 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.

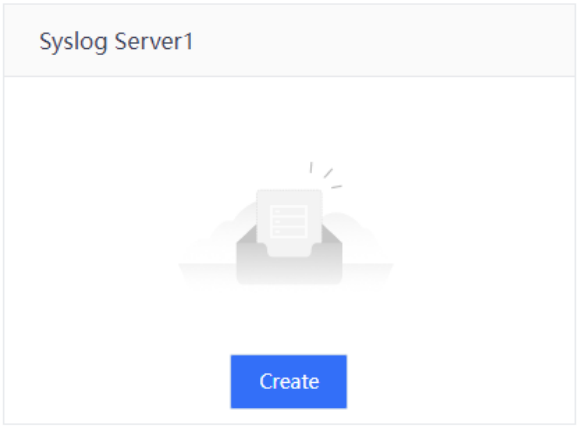
The system supports a maximum of three Syslog servers.

Procedure

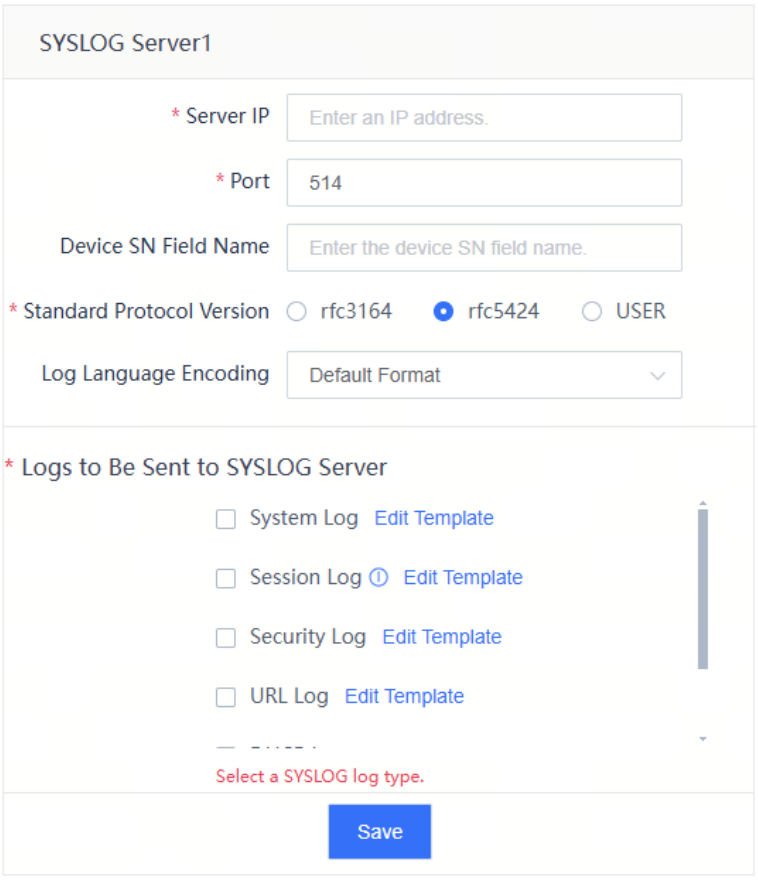
(1) Choose **System** > **Log Config** > **SYSLOG Settings**.

(2) Configure Syslog server 1.

a In the **Syslog Server1** area, click **Create**.



b Set parameters for Syslog server 1.



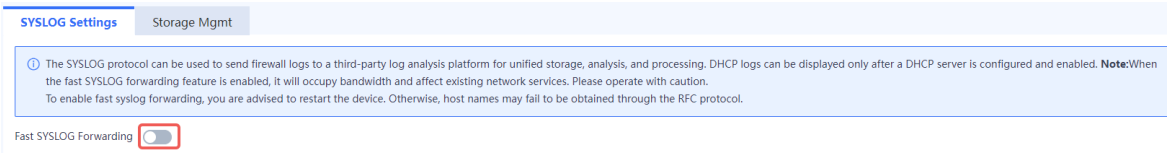
Item	Description	Remarks
Server IP	IP address of the Syslog server.	Set this parameter to the IP address of the Syslog server. [Example] 192.168.10.30
Port	Port number for receiving the log notifications.	The default value is 514. The value must be the same as that configured on the Syslog server. [Example] 80
Device SN Field Name	Customize the SN field name of the firewall. If the device SN is 123456789 and this field is configured as **test**, the SN field name displayed on the third-party log platform is test, namely, test="123456789". If this field is not configured, the default field name of the device SN sent by the device to the third-party log platform is deviceId, namely, deviceId="123456789".	[Example] test
Standard Protocol Version	Protocol used for formatting logs.	Select a protocol version supported by the Syslog server. [Example] RFC5424
Log Language Encoding	Encoding format of the Syslog language.	[Example] GBK
Logs to Be Sent to Syslog Server	Types of logs to be sent to the Syslog server. For session logs, you can select all the session logs or NAT logs.	Select specific log types to be 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.

7.4.2 Log Storage Management

Application Scenario

You can view the log storage capacity and storage details through the log storage management function. In addition, the storage space can be manually allocated for each service based on the hard disk capacity.

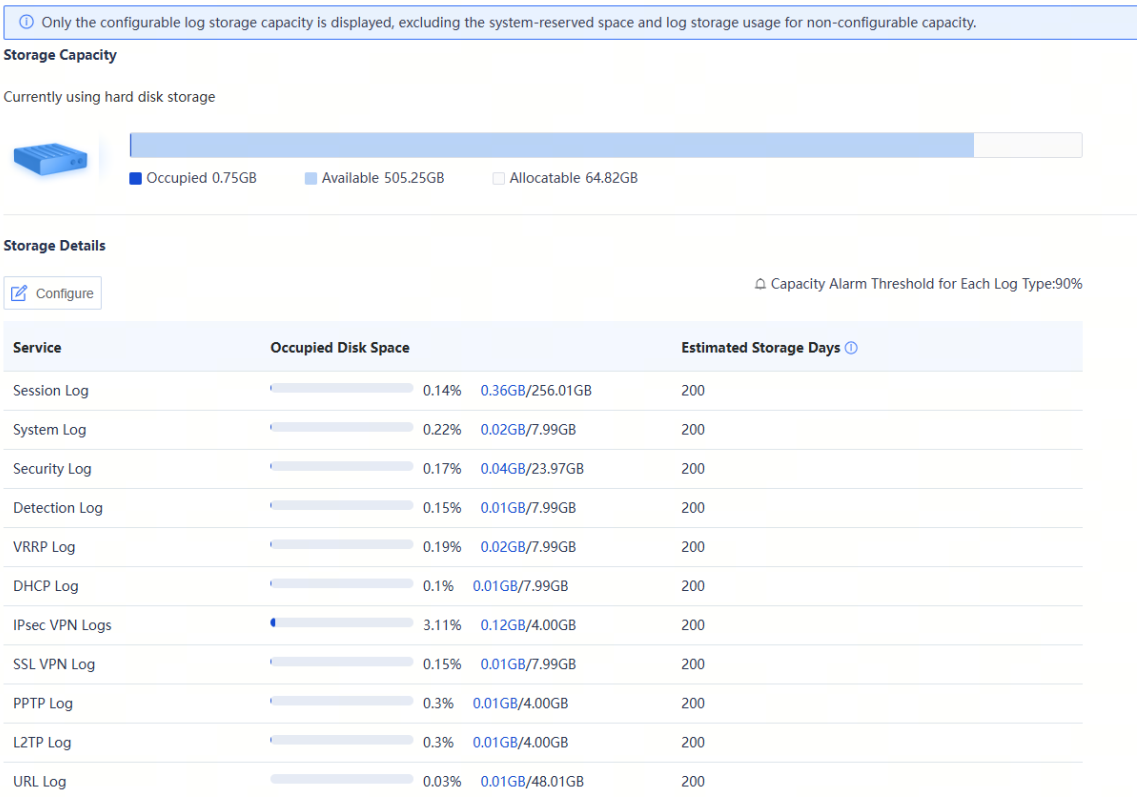
Precautions

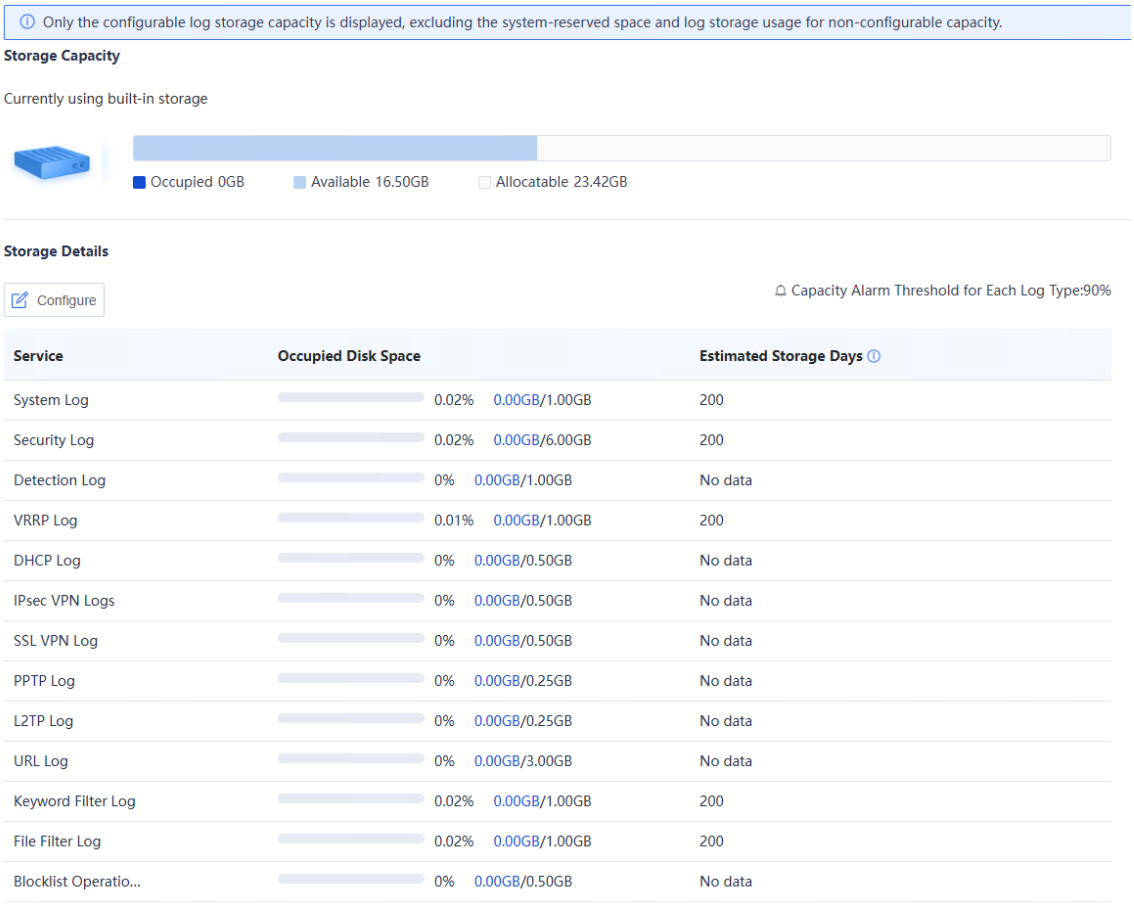
The device supports the log storage management function only when it has a built-in storage (eMMC) or is installed with a hard disk.

Procedure

(1) Check the log storage capacity and storage details.

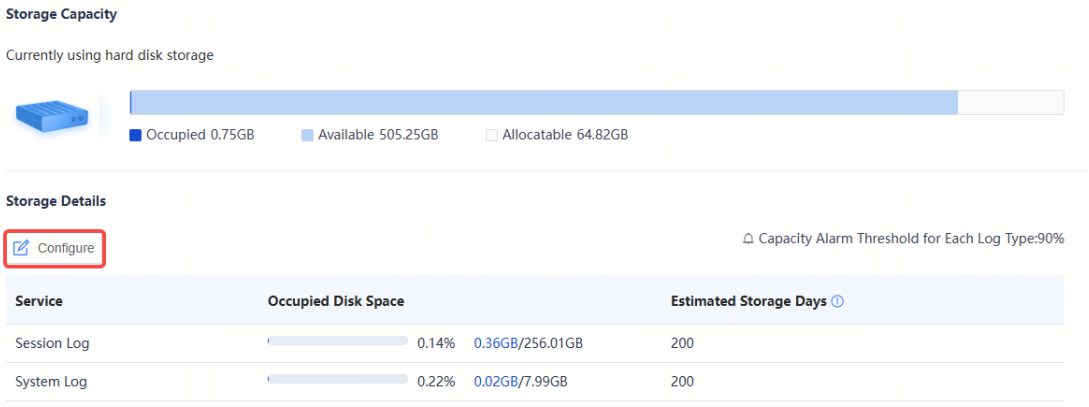
Choose **System** > **Log Config** > **Storage Mgmt**.



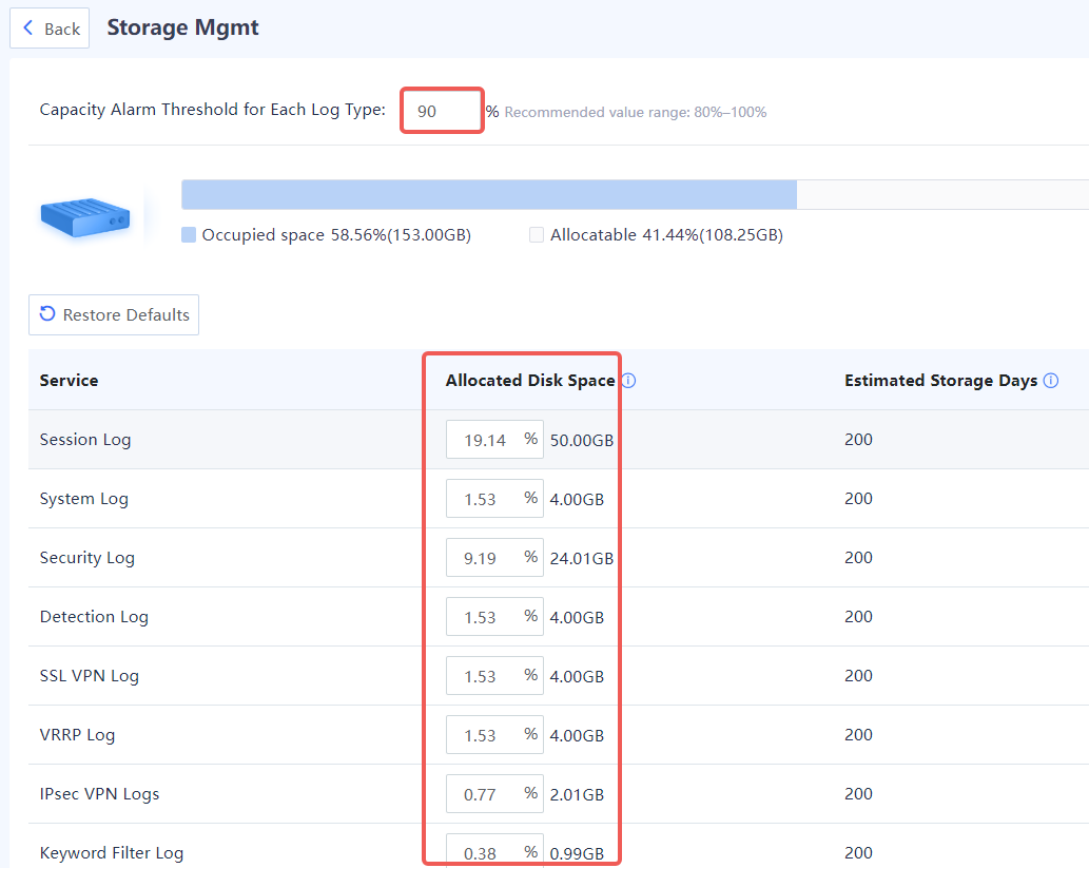


(2) Set the storage space for each service as required.

a Click **Configure**.

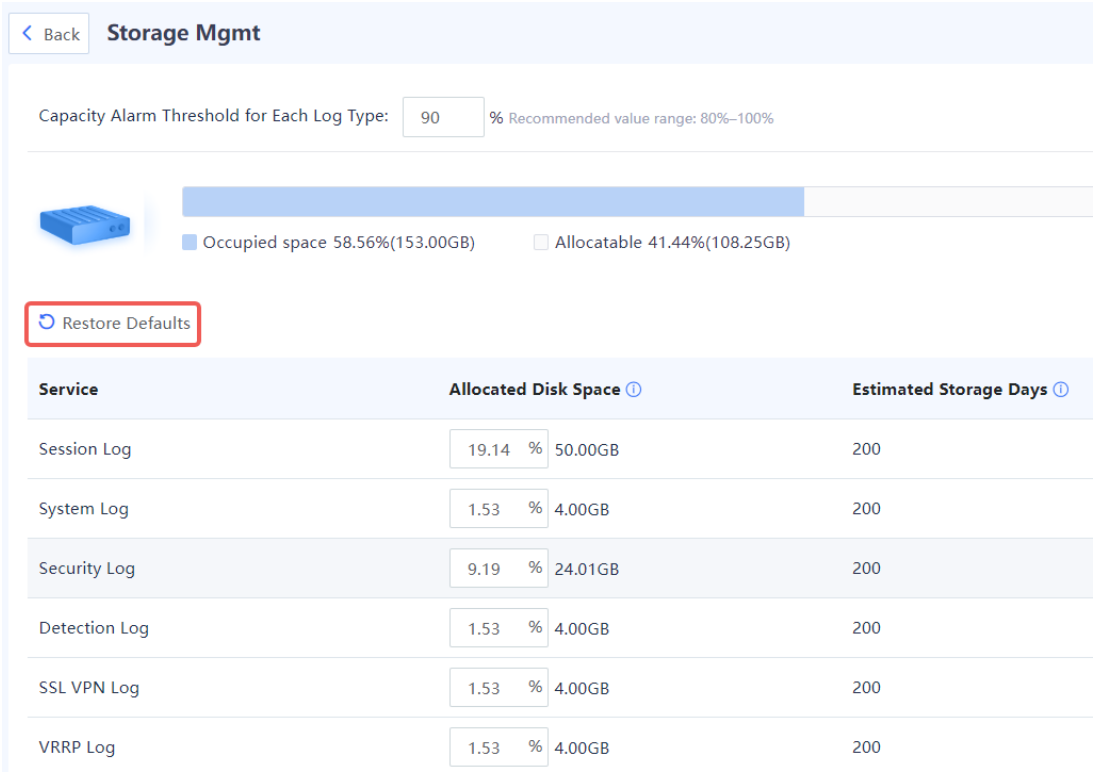


b Set the log capacity alarm threshold and disk allocation space for each service.



c Click **Save**.

Follow-up Procedure



- Click **Restore Defaults** to restore the disk allocation space of each service to the default value.

7.5 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.

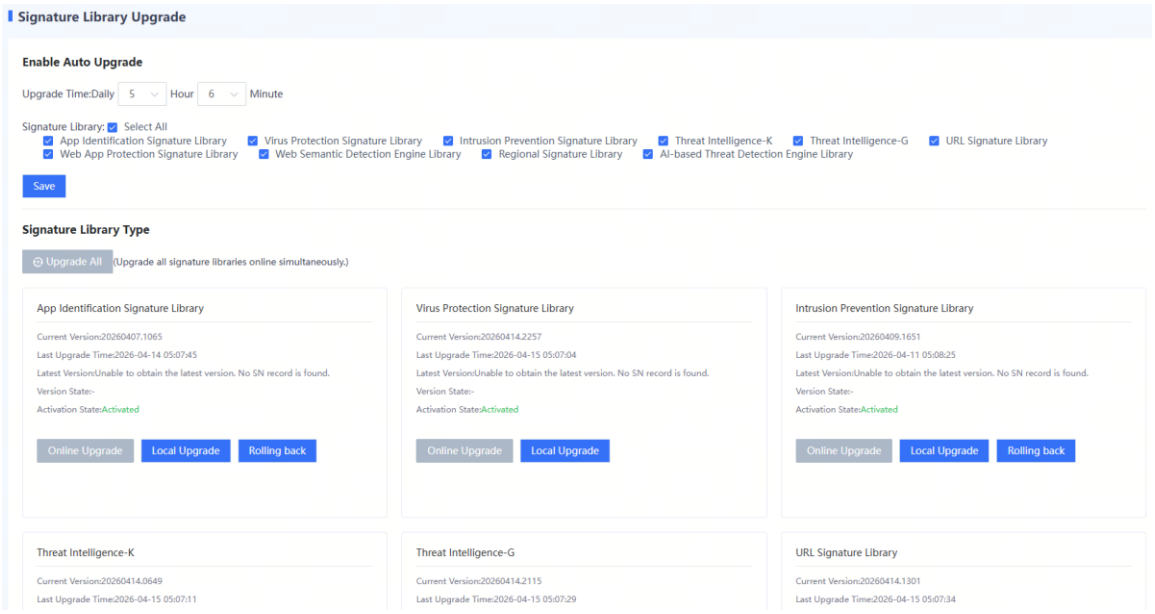
Prerequisites

- 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**.



The system displays information about the current signature libraries:

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

(2) Select a proper upgrade method:

- Scheduled automatic upgrade

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



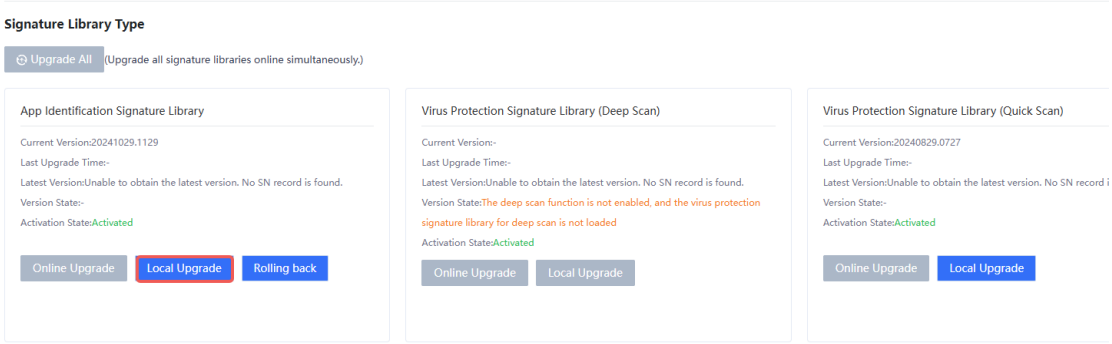
a) Set the time for automatic upgrade. You are advised to configure an off-peak period.

b) Select the type of signature library to be upgraded.

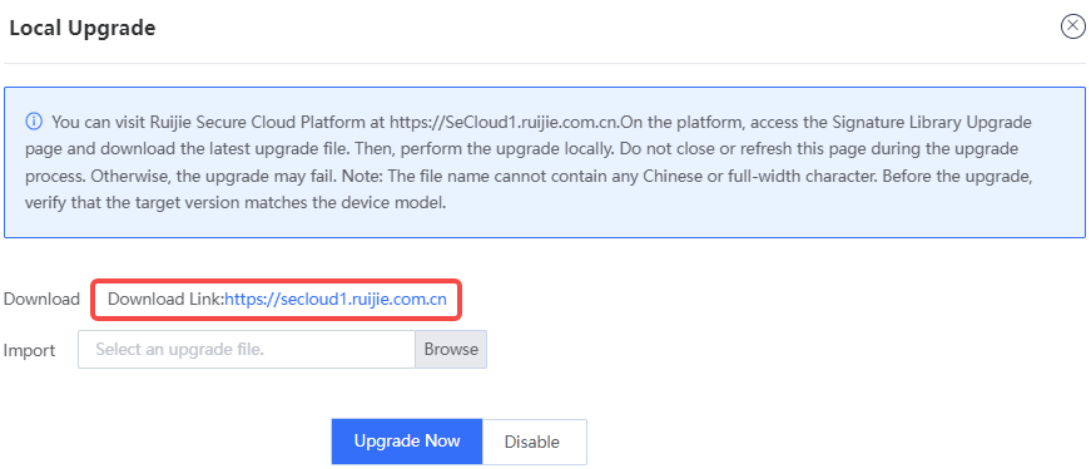
c) Click **Save**.

- Local upgrade

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



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



e) Click Browse to import the upgrade file.

f) Click Upgrade Now.

- 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**.

Follow-up Procedure

- If an exception occurs during the update of the signature database or you need to roll back the signature database to the early version, and the signature database file of the old version exists on the device, click **Rolling back** to roll back the specified signature database to the early version.

Description

Only the application identification signature database, and IPS signature database support the version rollback function.

7.6 High Availability

7.6.1 Overview

High availability (HA) ensures service continuity by eliminating single points of failure (SPOFs) through hot standby. Two devices negotiate the active/passive status through heartbeat interfaces. The active device forwards service packets and synchronizes information to the passive device. The passive device monitors the active device. When the active device fails, the passive device switches to the active device and forwards packets.

HA supports the active-passive mode and active-active mode.

7.6.2 Working Principle

1. Active/Passive Negotiation Process

HA uses the UDP for data communication and encapsulates Ruijie Redundancy Group Protocol (RRGP) data on the basis of the UDP for active/passive negotiation. The negotiation process is as follows:

(1) The active and passive devices establish an HA connection through the heartbeat interface and data synchronization interface. The two devices in an HA group send heartbeat packets to each other to notify each other of the status, priority, and other information of the local end.

(2) In preemption mode, HA compares the device attributes in the following order: number of monitoring interfaces > link detection object status > priority > HA running time > device SN. The process is as follows:

a The device with a greater number of monitoring interfaces functions as the active device. If the two devices have the same number of monitoring interfaces, the device with fewer abnormal monitoring interfaces is elected as the active device.

b If the number of normal monitoring interfaces is the same as that of abnormal monitoring interfaces, the link detection object becomes the master device.

c If the number of normal monitoring interfaces, number of abnormal monitoring interfaces, and link detection object status are the same, the device with a larger priority becomes the active device.

d If the number of normal monitoring interfaces, number of abnormal monitoring interfaces, link detection object status, and priorities are the same, the device with a longer HA running time becomes the active device.

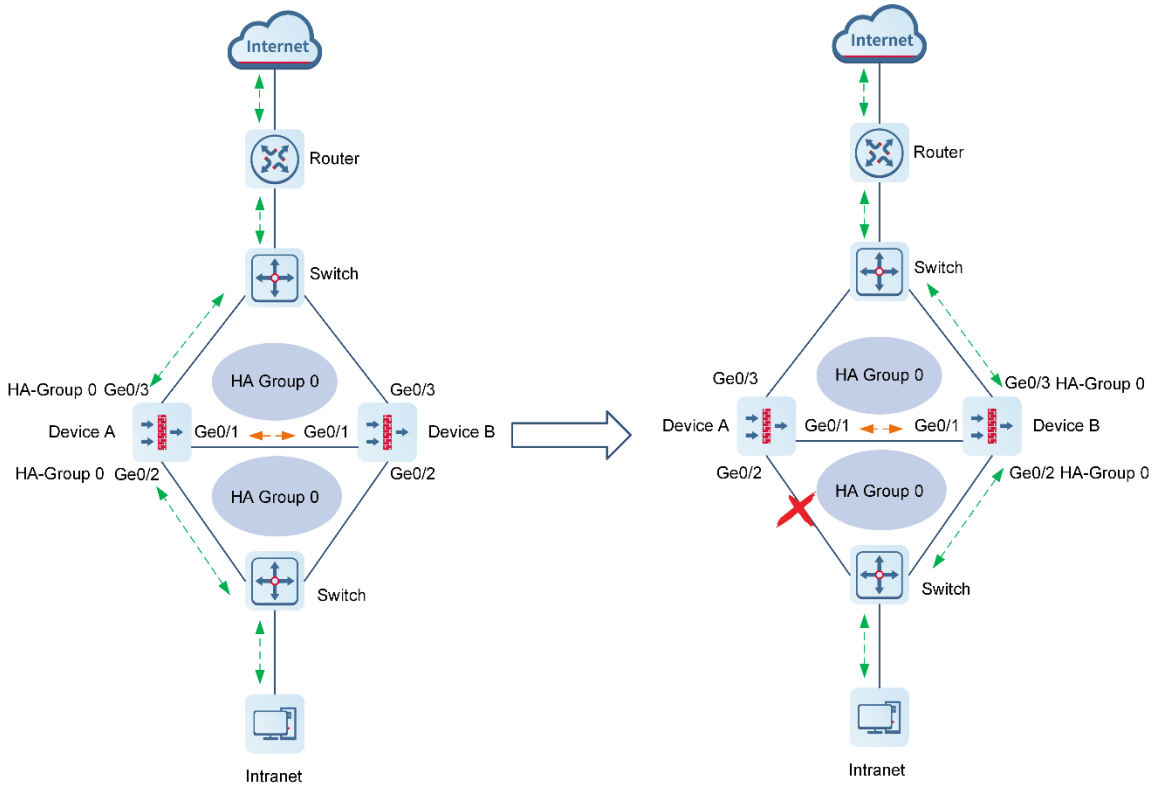
e If the number of normal monitoring interfaces, number of abnormal monitoring interfaces, link detection object status, priorities, and HA running time are the same, the device with the largest device SN is the active device.

In non-preemption mode, HA compares the device attributes in the following order: number of monitoring interfaces > link detection object status > HA running time > priority > device SN.

2. Active-Passive Mode

In active-passive mode, the active device processes services. The passive device takes over services only when the active device is faulty. In this mode, only one HA group is required, and different devices in the HA group have different priorities.

Figure 7-2 Active-Passive Mode



As shown in Figure 7-2, the working process of the active-passive mode is as follows:

(2) The upstream and downstream service ports of Device A and Device B work at Layer 2 or Layer 3 and are connected to the switches.

Assume that Device A is active and Device B is passive in HA Group 0 after negotiation. In this case, Device A processes and forwards traffic and synchronizes the configuration and status to Device B in real time to ensure configuration and status consistency between the two devices.

(3) When downstream Ge0/2 on Device A is faulty:

a Device A detects the fault based on interface monitoring. When the number of faulty monitored interfaces on Device A increases, Device A notifies Device B of the increase by sending a heartbeat packet.

b When receiving the heartbeat packet, Device B finds that the number of normal monitored interfaces on the local end is larger than that on the peer end and that the peer device is not in the active state. Therefore, Device B immediately takes over the active role.

If the service ports of both devices work at Layer 2: When Device A goes Up after going Down, the upstream and downstream switches update their MAC address tables.

If the service ports of both devices work at Layer 3: After Device B takes over the active role, it broadcasts gratuitous ARP/NS packets to instruct the upstream and downstream switches to update their MAC address tables.

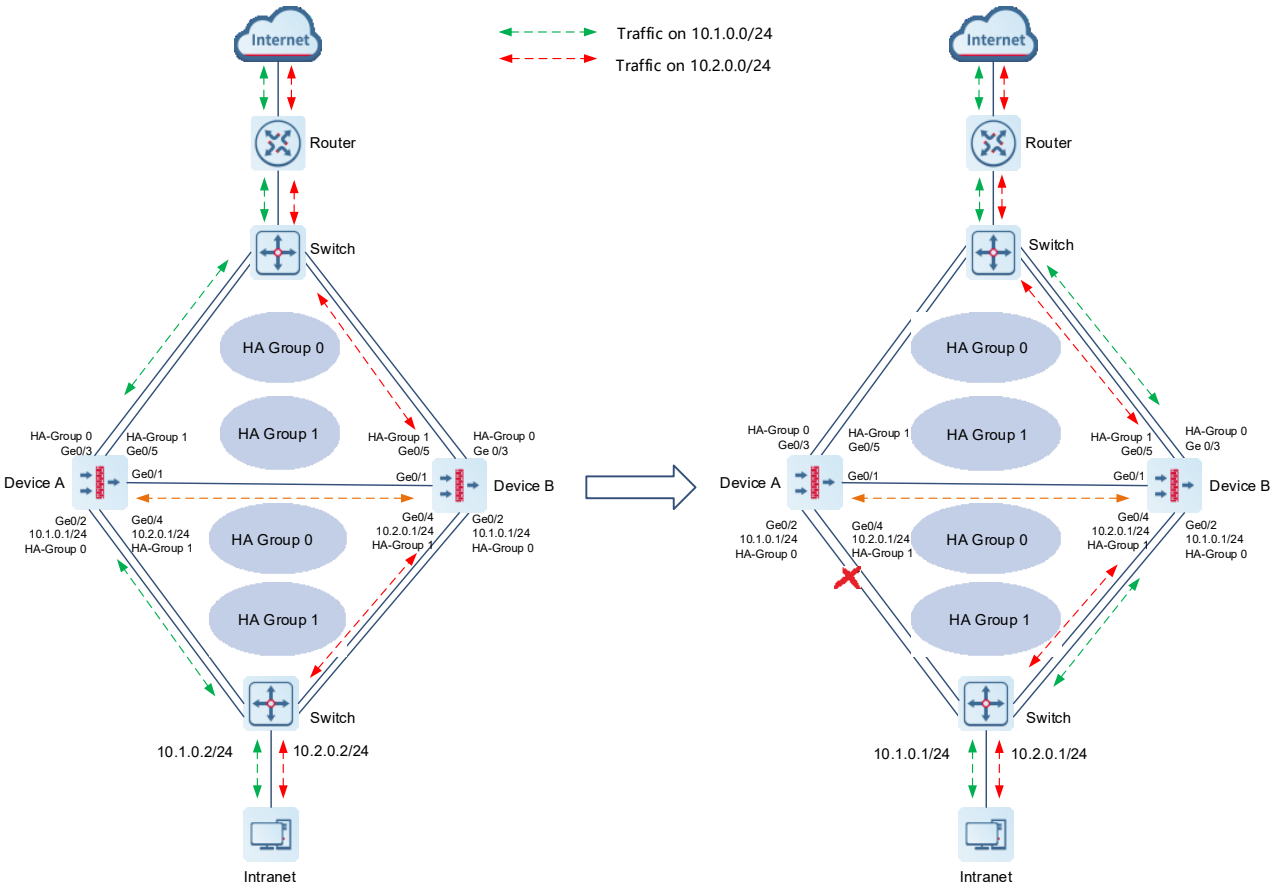
c The upstream and downstream switches query their updated MAC address tables and forward subsequent traffic through Device B.

Configuration and service entries (including session, routing, MAC address, and neighbor entries) between Device A and Device B are synchronized from the active device to the passive device in real time, ensuring service continuity.

3. Active-Active Mode

In active-active mode, two devices process services simultaneously, improving the system load balancing capability. If one device fails, the other device takes over its services immediately, ensuring service continuity. In this mode, two HA groups are required, and each group includes one active device and one passive device. A device can join two HA groups and has different priorities in different groups. That is, it can be the active device in one group and the passive device in another group. To implement load balancing between two devices, ensure that Device A has the highest priority in HA Group 0 and Device B has the highest priority in HA Group 1.

Figure 7-3 Active-Active Mode



As shown in Figure 7-3, the working process of the active-active load balancing mode is as follows:

(2) The upstream and downstream service ports of Device A and Device B work at Layer 3 and are connected to the switches.

Assume that after negotiation, Device A is active in HA Group 0 and passive in HA Group 1, and Device B is passive in HA Group 0 and active in HA Group 1. Traffic on the 10.1.0.0/24 network segment is allocated to HA Group 0, and traffic on the 10.2.0.0/24 network segment is allocated to HA Group 1.

As the active device in HA Group 0, Device A forwards traffic on the 10.1.0.0/24 network segment and synchronizes session information, service configurations, and status to Device B in real time.

As the active device in HA Group 1, Device B forwards traffic on the 10.2.0.0/24 network segment and synchronizes session information to Device A in real time.

(3) When downstream Ge0/2 on Device A is faulty:

a HA Group 0 of Device A detects the interface faults based on interface monitoring. When the number of faulty monitored interfaces on Device A increases, Device A notifies HA Group 0 of Device B of the increase by sending a heartbeat packet.

b When receiving the heartbeat packet, HA Group 0 of Device B finds that the number of normal monitored interfaces on the local end is larger than that on the peer end and that the peer device is not in the active state. Therefore, Device B immediately takes over the active role and broadcasts gratuitous ARP/NS packets to update the MAC address tables of upstream and downstream switches.

c The upstream and downstream switches query their updated MAC address tables and switch traffic on the 10.1.0.0/24 network segment to Device B for forwarding. In this case, all service traffic is forwarded by Device B.

Session information is separately synchronized from the active devices in HA Group 0 and HA Group 1 to the passive devices in the two groups in real time, and the other information is synchronized only from the active device in HA Group 0 to the passive device in HA Group 0 in real time, ensuring service continuity.

7.6.3 Configuring High Availability

Application Scenario

HA applies to scenarios with demands for high network reliability and service continuity. By eliminating SPOFs, HA can avoid network service interruptions.

Precautions

- The HA function cannot be configured together with the VRRP function.
- The software version and device models of the two firewalls that form an HA network must be the same.
- Between the two firewalls that form an HA network, the configurations of the HA enabled state, HA security, heartbeat interfaces, data synchronization interfaces, priorities, and link detection are not synchronized.
- Before an HA system is set up, the device running modes, heartbeat interfaces, data synchronization interfaces, heartbeat intervals, preemption modes, preemption delays, and virtual MAC prefixes must be manually configured to be consistent. After the HA system is set up, the device running modes, heartbeat intervals, preemption modes, preemption delays, and virtual MAC prefixes can be synchronized.
- On the passive device, configuration that does not support active/passive synchronization can be modified, but configuration that supports active/passive synchronization cannot be modified.
- Only physical interfaces and aggregate interfaces can be configured as heartbeat interfaces and data synchronization interfaces.
- After HA is enabled, no heartbeat interface and data synchronization interface can be configured. The two interfaces can be added only after HA is disabled.
- Only physical interfaces can be management interfaces. Two devices in the HA system must use the same management interface name (such as Ge0/0) and different interface IP addresses.
- Only physical interfaces, aggregate interfaces, and sub-interfaces can be configured as monitoring interfaces in a group, and heartbeat interface, data synchronization interface, and management interface cannot be configured as the monitoring interface. At least two interfaces can be configured as monitoring interfaces in each HA group.
- In HA networking, the interfaces configured for active and passive devices must be the same. For example, for both devices, set the uplink interface, downlink interface, heartbeat interface, and data synchronization interface to Ge0/1, Ge0/2, Ge0/3, and Ge0/4, respectively.
- After HA is enabled, all interfaces on the device cannot be configured to work in bypass mode.
- After HA is enabled, all interfaces except heartbeat interfaces, data synchronization interfaces, and management interfaces are added to HA group 0 by default, and interfaces can be moved from group 0 to group 1 through interface monitoring.
- Interfaces that obtain IP addresses dynamically via PPPoE or DHCP cannot be used for HA deployment.

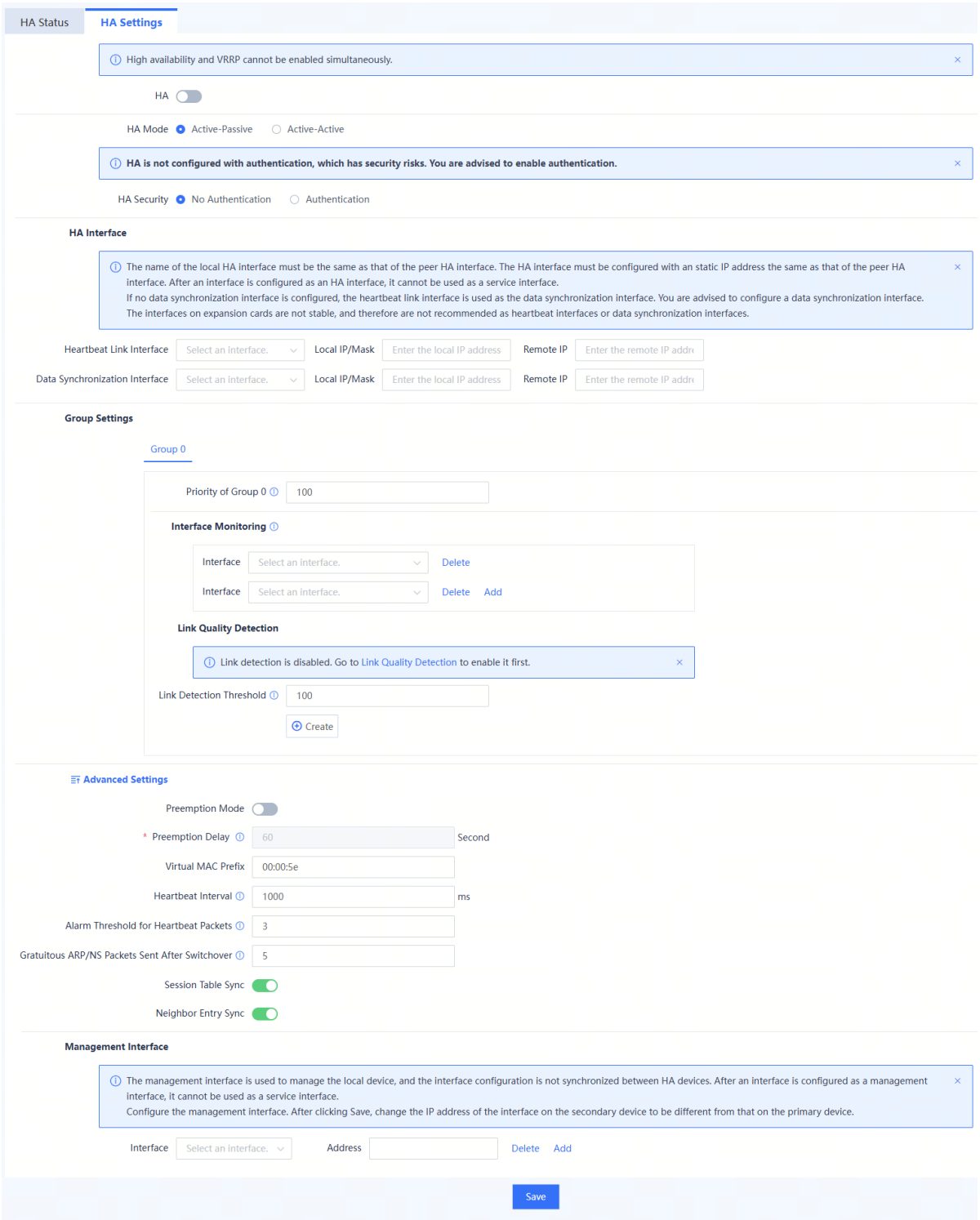
- Traffic cannot be forwarded across HA groups.

Prerequisites

- In active-passive mode, if all service ports of the device work at Layer 2, you need to add the service ports associated with HA to the same bridge port first.
- Dedicated interfaces are planned as heartbeat interfaces, data synchronization interfaces, and management interfaces, which cannot be used as service forwarding interfaces.
- The heartbeat interfaces or data synchronization interfaces are directly connected using a physical link. That is, two devices that need to form an HA group are installed on the same rack or adjacent racks.
- The management interface cannot be configured as a heartbeat interface or data synchronization interface.
- Only the primary IP address can be configured for a heartbeat interface or data synchronization interface.

Procedure

(1) Choose **System** > **High Availability** > **HA Settings** and click the HA Settings tab.



(2) Configure HA parameters.

Item	Description	Remarks
HA	Whether to enable the HA function. Related parameters can be configured only when this function is enabled.	[Example] Enable

Item	Description	Remarks
HA Mode	Device running mode. The values are as follows: ● **Active-Passive**: Only the active device forwards services. The passive device takes over services only when the active device fails. ● **Active-Active**: Both devices in an HA group forward services to implement load balancing.	[Example] Active-Passive
HA Security	If no authentication is configured, the HA function has security risks. Therefore, you are advised to enable HA authentication. When authentication is used, the local and remote devices must both use authentication with the same password; otherwise, the two devices cannot form an HA group.	[Example] Authentication
Password	Configure the HA authentication password. The authentication passwords configured on the local and remote ends must be the same.	[Example] Test@123
Heartbeat Link Interface		
Heartbeat Link Interface	Select the heartbeat interface of the local device. The heartbeat interfaces of the active and passive devices must be the same.	[Example] Ge0/1
Local IP/Mask	IP address of the heartbeat interface on the local device.	If an IP address has been configured for the interface, the IP address is automatically filled in after you select the heartbeat interface. Otherwise, you need to configure the interface IP address manually. The local and remote IP addresses must be on the same network segment. [Example] 10.1.1.2/24
Remote IP	IP address of the heartbeat interface on the peer device.	[Example] 10.1.1.1
Data synchronization interface		

Item	Description	Remarks
Data Synchronization Interface	Select a data synchronization interface. If no data synchronization interface is configured, the heartbeat interface is used as the data synchronization interface. The port numbers of the data synchronization interfaces on the active and passive devices must be the same.	[Example] Ge0/1
Local IP/Mask	IP address of the data synchronization interface on the local device.	If an IP address has been configured for an interface, the IP address is automatically filled in after you select the data synchronization interface. Otherwise, you need to configure the interface IP address manually. The local and remote IP addresses must be on the same network segment. [Example] 10.1.1.3/24
Remote IP	IP address of the data synchronization interface on the peer device.	[Example] 10.1.1.11
Group Settings		
Priority	Priority value of the device in the HA group. A larger value indicates a higher priority.	[Example] 100
Interface Monitoring	The service forwarding interface cannot be the same as the configured heartbeat interface, data synchronization interface or management interface. If the service interface of the device works at Layer 3, you need to assign an IP address to an interface for HA uplink and downlink communication. If the service interface works at Layer 2, you do not need to assign an IP address to an interface.	Select a value from the drop-down list. [Example] Ge0/2

Item	Description	Remarks
Link Detection Threshold	Weight threshold for a link detection object. When the sum of the weight values of all the failed monitoring interfaces in the link detection object list is greater than or equal to the link detection threshold, the link detection object is faulty. A link detection object can monitor the status of multiple interfaces (that is, multiple link detection nodes can be added). You need to configure the link detection threshold and interface weight properly as required to ensure service continuity.	● Click **Create** to add a link detection node for interface monitoring. ● Before configuring a detection node, enable the link detection function. For details, see 6.14.1 Link Quality Detection. ● Both LAN and WAN interfaces support link detection.
Advanced Settings		
Preemption Mode	If the active device fails, the passive device immediately switches to the active state. After this function is enabled, traffic is switched back to the original active device when the device restores the active state. This function is disabled by default.	[Example] Enable
Preemption Delay	Delay time before the passive device declares its active state.	[Example] 60
Virtual MAC Prefix	Virtual MAC address prefix of the upstream and downstream service ports. The default value is 00:00:5e.	[Example] 00:00:5e
Heartbeat Interval	Interval at which heartbeat packets are sent.	[Example] 600
Alarm Threshold for Heartbeat Packets	The default value is 3, which indicates that if the local device does not receive a heartbeat packet from the peer device within three consecutive heartbeat intervals, it considers the peer device as unavailable. The value can be modified as required.	[Example] 6
Gratuitous ARP/NS Packets Sent After Switchover	Number of times that the device sends gratuitous ARP/NS packets to update the MAC address table of upstream and downstream switches when the service ports work at Layer 3.	[Example] 6

Item	Description	Remarks
Session Table Sync	Whether to enable session synchronization. After this function is enabled, the local device automatically synchronizes session information to the peer device. You are advised to enable session synchronization to ensure smooth service switching without interruption during an active/standby switchover.	[Example] Enable
Neighbor Entry Sync	Whether to enable neighbor entry synchronization. After this function is enabled, the local device automatically synchronizes neighbor entry information to the peer device. To ensure smooth service switching without interruption during an active/standby switchover, you are advised to enable neighbor table synchronization.	[Example] Enable
Management Interface		
Interface	Device management interface to be selected (used only for out-of-band management and not for service traffic forwarding). HA supports synchronizing the interface name configuration. Both the active and passive devices can be managed through the default management interfaces. If no management interface is configured on the passive device, the passive device cannot be managed separately. Management traffic must be transmitted and received through the management interface. Otherwise, the passive device cannot be managed.	[Example] Ge0/0
Address	IP address of the management interface. The HA system does not synchronize the interface address.	If an interface is configured with an IP address, the IP address is automatically filled in after you select the interface. Otherwise, you need to configure the interface IP address manually. [Example] 192.168.1.3/24

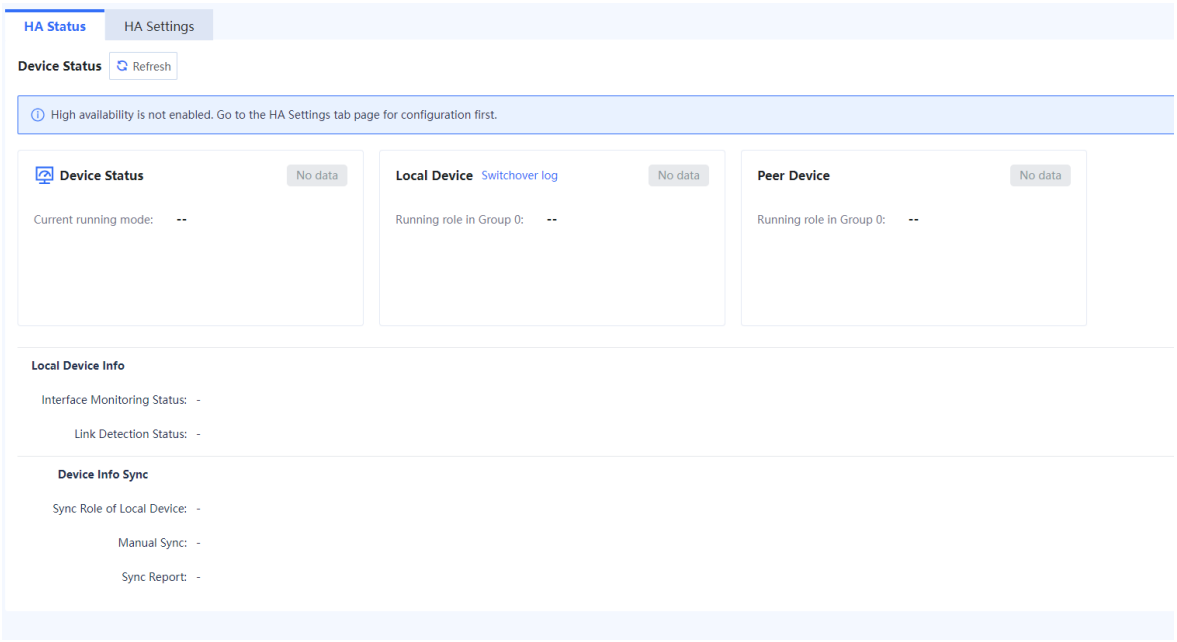
7.6.4 Viewing High Availability Status

Application Scenario

View the high availability configuration status of the firewall, including the local device information and configuration synchronization status.

Procedure

(1) Choose **System** > **High Availability** > **HA Status**.



7.7 Overload Protection

7.7.1 Configuring System Overload Protection

Application Scenario

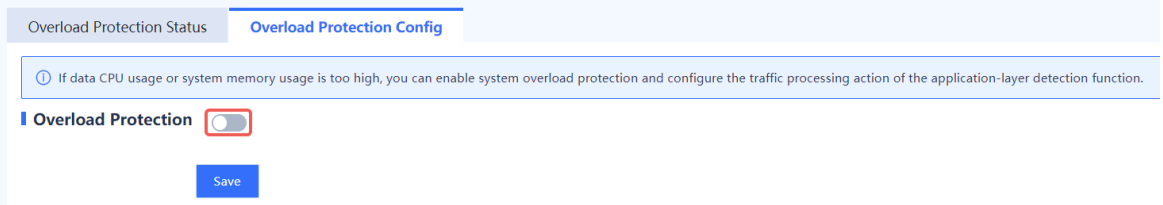
When the CPU or memory usage is high, the device enabled with overload protection permits packets by default and does not perform security check on the received packets. In a scenario that has high security requirements, you can set the action to block to prevent traffic for which security service detection is not performed.

You can also set the action to security service self-adaptation and set the security service priority. When the overload exceeds the configured threshold, the device automatically skips check of security services with lower priorities. When the load is lower than the specified threshold, security service check is restored.

Procedure

(1) Choose **System** > Overload Protection > Overload Protection Config.

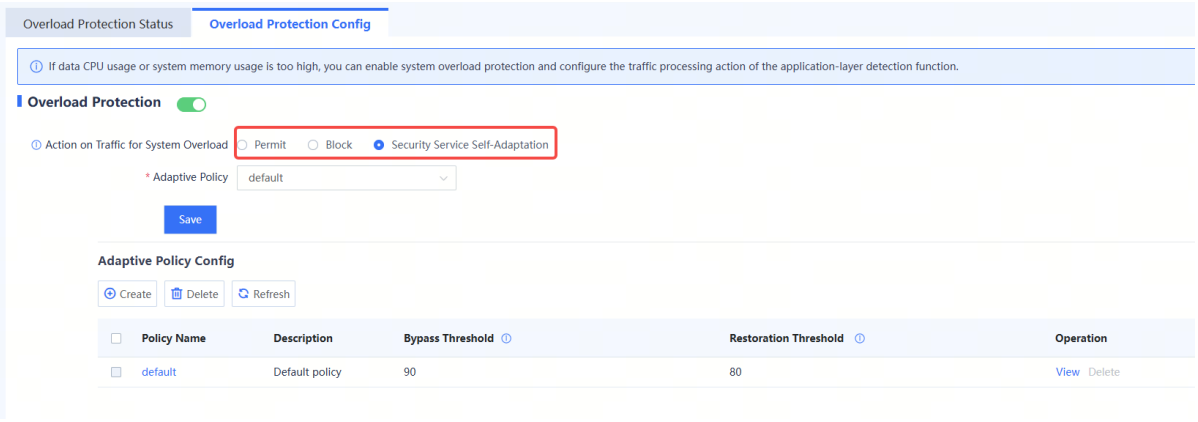
(2) Toggle on  to enable the overload protection function.

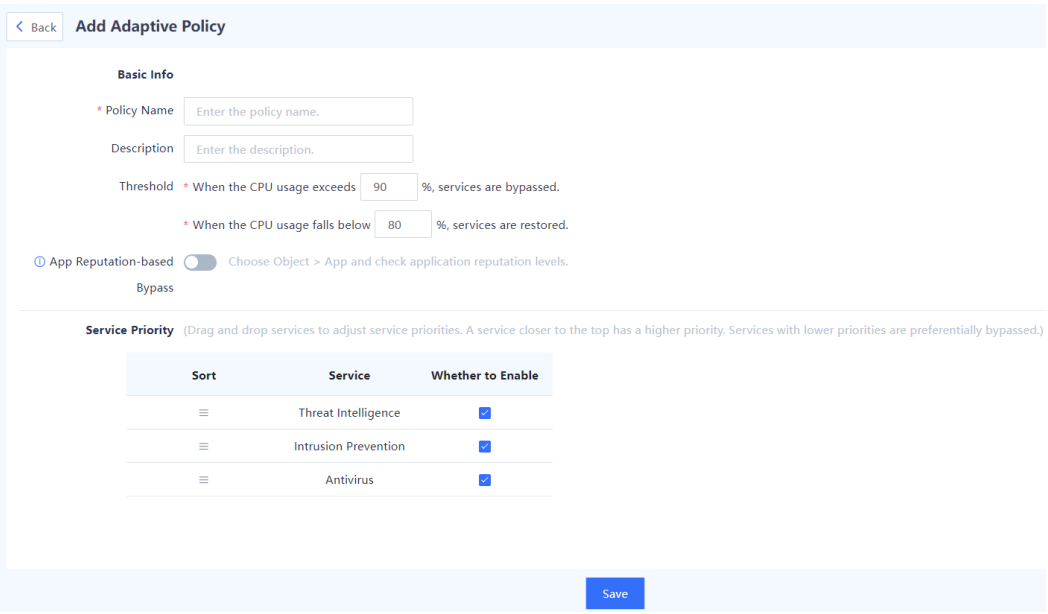


(3) Configure the action to be taken on traffic when overload is detected. If you select **Security Service Self-Adaptive**, you need to configure a self-adaptation policy.

The device provides a predefined adaptation policy **default**, which can only be queried but cannot be deleted or modified.

You can also click **Create** to create a custom self-adaptation policy.





Item	Description	Remarks
Policy Name	Self-adaptation policy name.	[Example] Policy
Description	Description of a self-adaptation policy.	-
Threshold	When the overload exceeds the configured threshold, the device automatically skips check of security services with lower priorities. When the load falls below the specified threshold, security service check is restored one by one based on the configured service priority, and security services with higher priorities are restored preferentially.	The bypass service threshold must be 10% higher than the restoration threshold.
App Reputation-based Bypass	After this function is enabled, security check for applications with the highest reputation level is automatically skipped. Choose **Object** > **App** > **App** to view the reputation of an application. For details, see 5.2.2 Viewing Application Information in a Signature Library.	[Example] Enable
Service Priority	Priority of security service check.	● Drag services to sort services, with the top service having the highest priority and the bottom service having the lowest priority. ● You can select whether to enable security service check.

(4) Click **Save**.

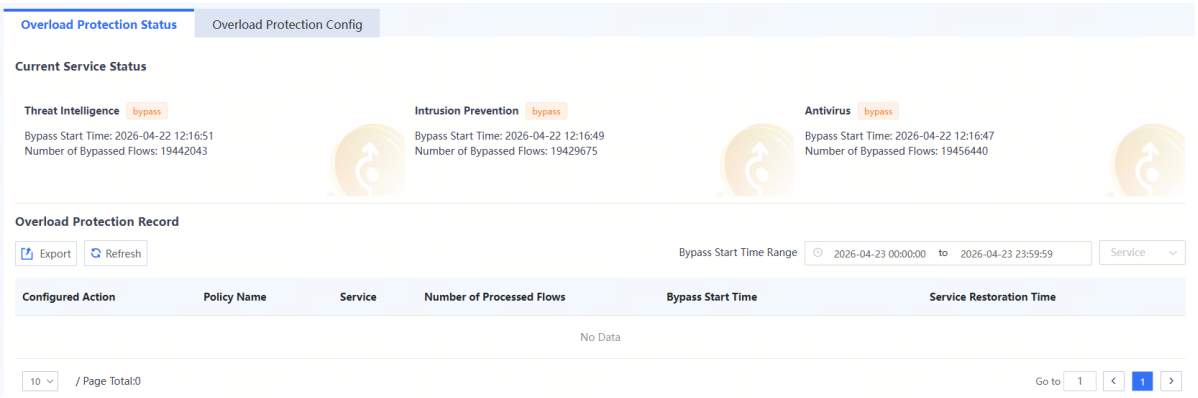
7.7.2 Displaying the System Overload Protection Status

Application Scenario

By viewing the system overload protection status, you can learn about the current security service status and system overload protection records.

Procedure

(1) Choose **System** > **Overload Protection** > **Overload Protection Status**.



Follow-up Procedure

- Click **Export** to export the current system overload protection record to the local device for future query.
- You can set **Bypass Start Time** to view protection records within a specified time range.
- You can select different services in the search box to view protection records.

7.8 Information Push

7.8.1 Overview

If traffic is blocked by the virus protection policy, URL filtering, user blocklist, or MAC blacklist, the device pushes the blocking reason, blocking duration, and other information to the blocked terminal.

The device provides a predefined push page. You can customize some HTML page styles to meet personalized requirements, including modifying the logo image and text information and previewing the push page.

Caution

- This function supports only IPv4, but does not support IPv6.
- This function supports only HTTP and HTTPS.
- For URL filtering detection and antivirus detection based on HTTPS, SSL proxy must be enabled first.
- This function takes effect only when the actions of virus protection and URL filtering are set to blocking.
- The Info Push page is displayed only for antivirus-based blocking of downloaded data, and is not displayed for antivirus-based blocking of uploaded data.
- The blocking page is pushed only when traffic matches the virus protection policy or URL filtering for the second time.

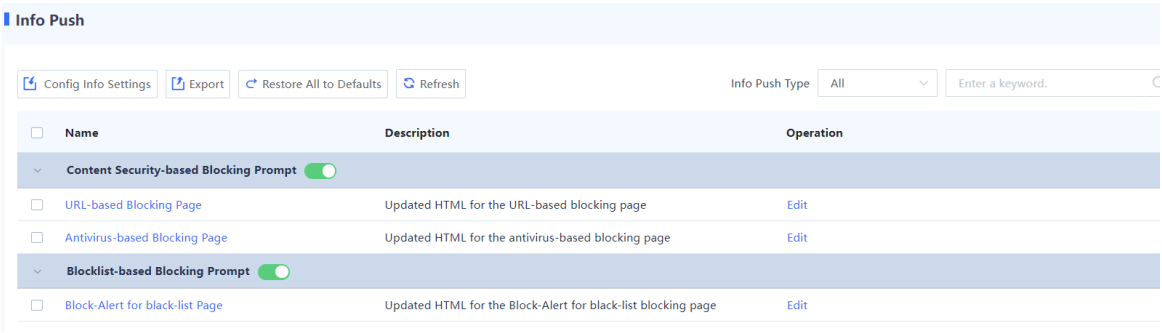
7.8.2 Setting the Logo Image

Application Scenario

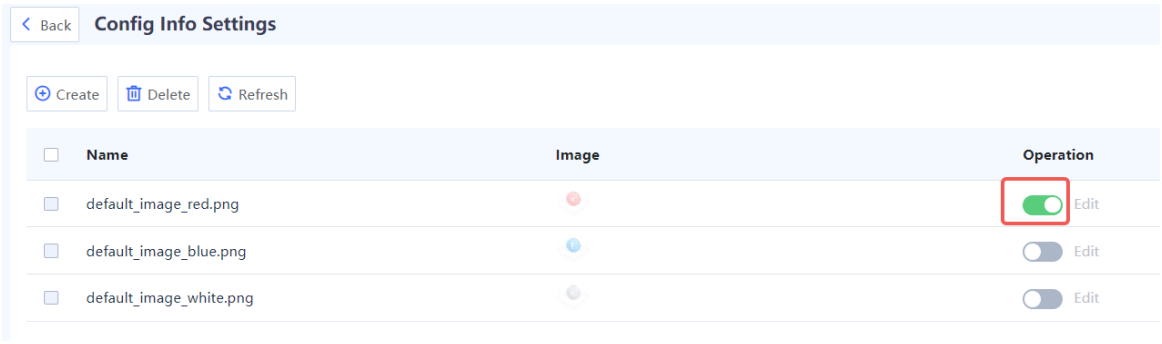
The device provides three predefined logos, which cannot be edited or deleted. You can also customize the logo image.

Procedure

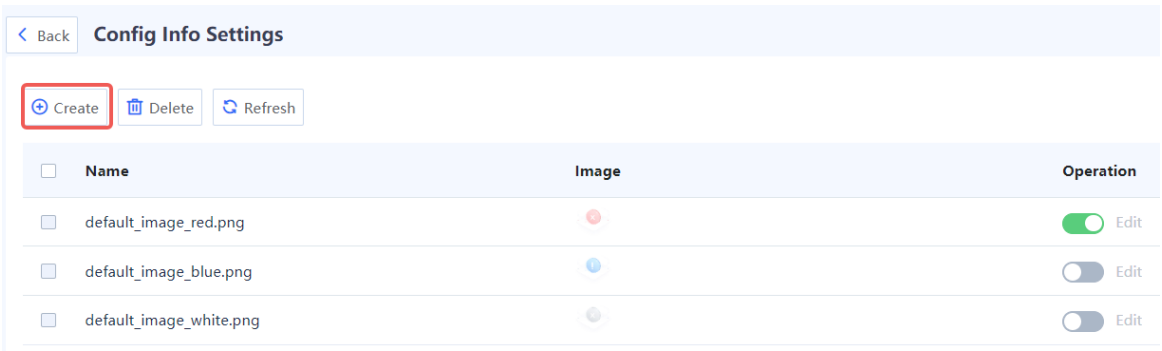
(1) Choose **System** > Info Push.



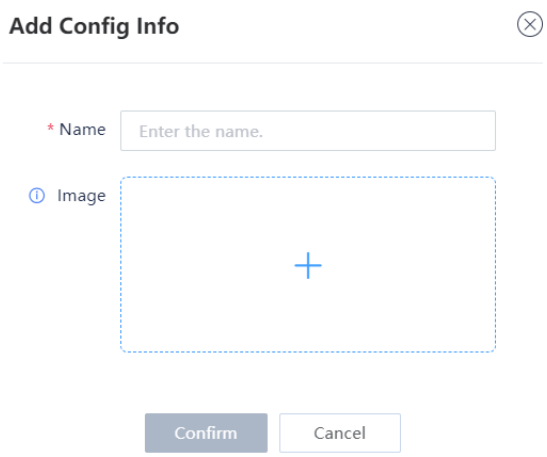
(2) Click **Config Info Settings**. The device provides three predefined logo images for selection. Toggle on or off the switch button in the **Operation** column to enable or disable them as required.



(3) Click **Create**.



(4) Add a logo image. The image format must be PNG or JPEG, and the image size cannot exceed 32 KB.



(5) Click **Confirm**.

Follow-up Procedure

You can modify or delete a custom logo image.

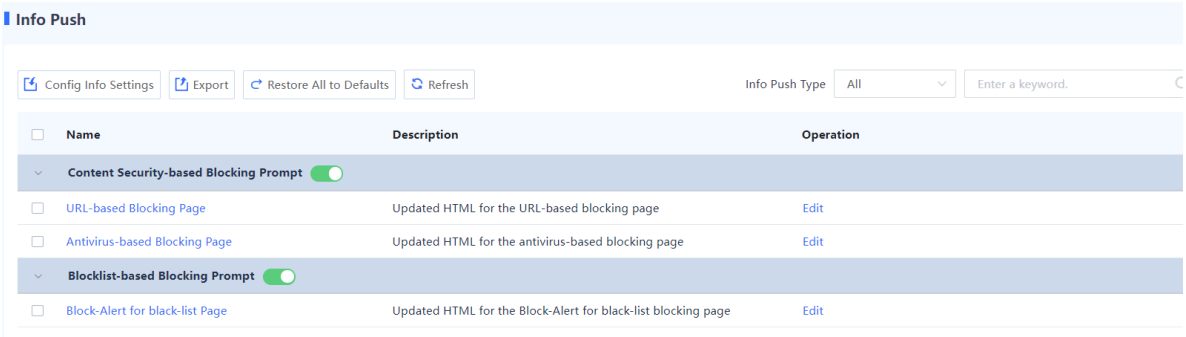
7.8.3 Editing Text Information

Application Scenario

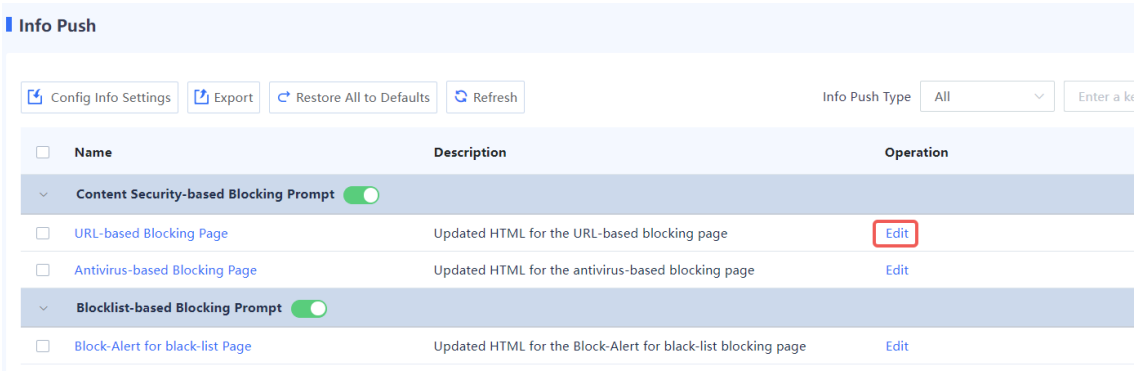
The device supports online editing of push information for virus protection and URL filtering, as well as push notifications for blocking by the blocklist. After traffic is blocked by a security service (virus protection or URL filtering) or blocklist, the custom traffic blocking page or text configured for the service is displayed. The page or text can be previewed.

Procedure

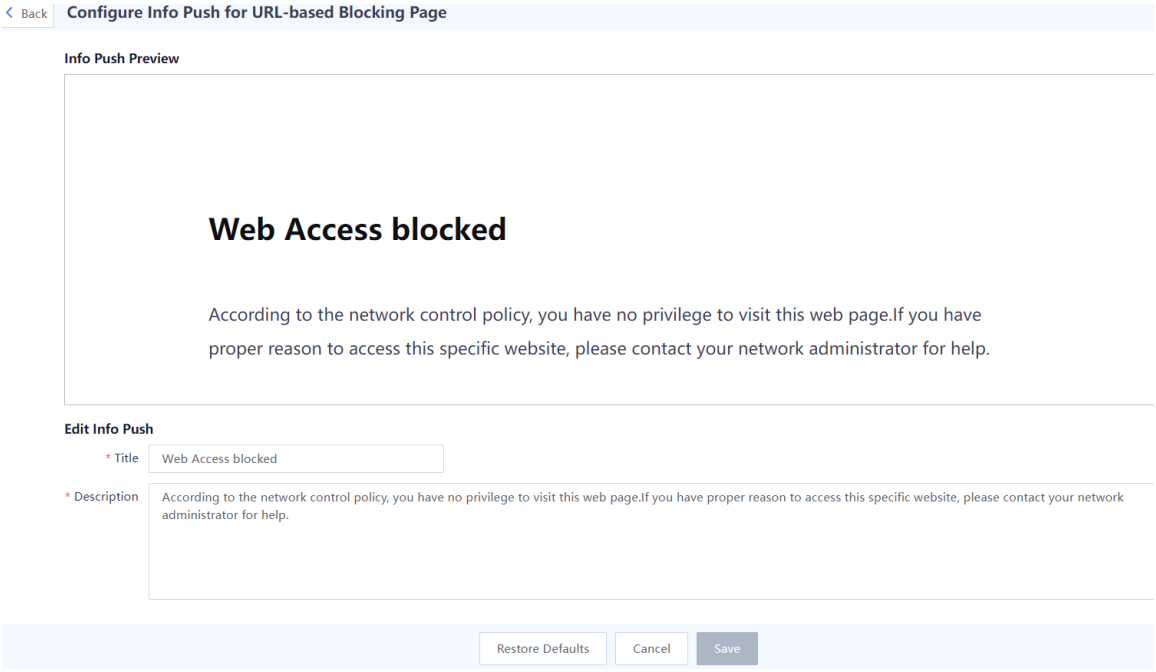
(1) Choose **System** > **Info Push**.



(2) Click **Edit** in the **Operation** column.



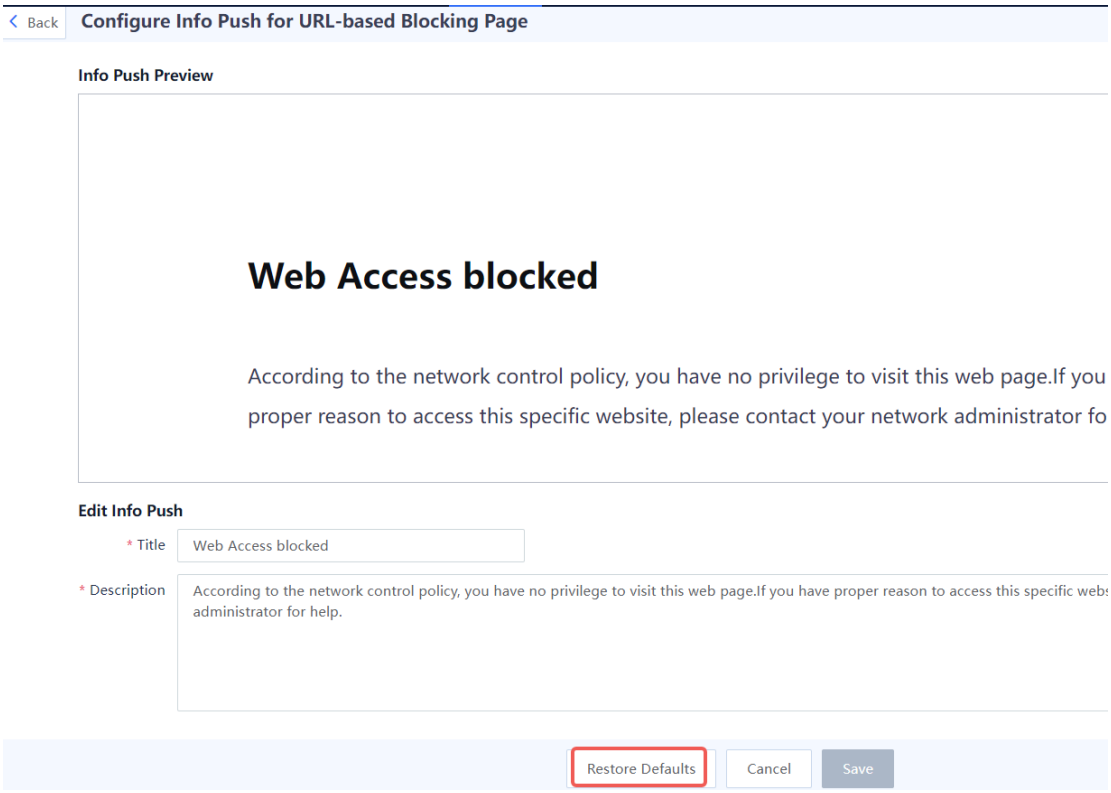
(3) Configure the push text.



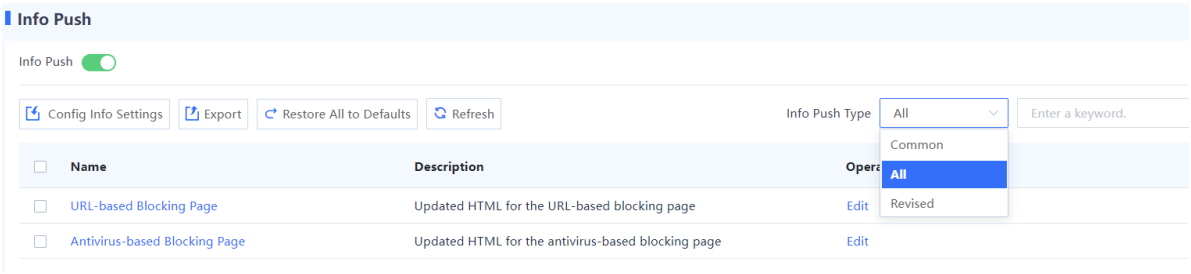
Field	Description
Title	Title of the traffic blocking page of the security service.
Description	Description of blocking details on the traffic blocking page of the security service.

(4) Click **Save**.

(5) (Optional) Click **Restore Defaults** to restore the default text.



Follow-up Procedure



- Select push pages and click **Export** to export the push page information to the local device.
- Click **Restore All to Defaults** to restore the default configurations on a page, including the logo and text.
- Click **Refresh** to obtain the latest push information.
- Select **Common**, **All**, or **Revised** from the **Info Push Type** drop-down list to view information on corresponding traffic blocking pages.

7.8.4 Enabling Information Push

Application Scenario

The device can independently enable information push of blocked security contents and blocklist block information push. After information push is enabled, if traffic is blocked by security services (antivirus and URL filtering) or the blocklist, information about the custom blocking page will be displayed.

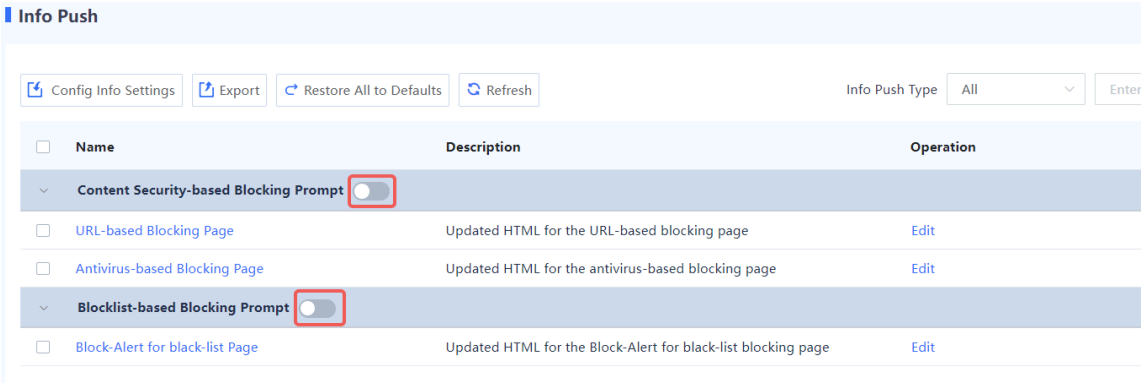
Procedure

(1) Choose **System** > **Info Push**.

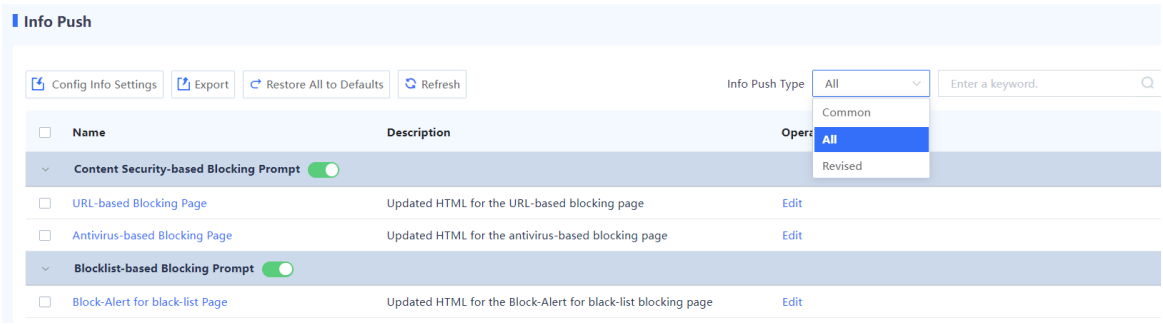
(2) Click  as required. You can enable the push information of corresponding services.

Caution

After the blocklist blocking prompt is disabled, all prompts for users in the user or MAC address blocklist will be disabled. Exercise caution when performing this operation.



Follow-up Procedure



- Select the push information to export and click **Export** to export the push information to the local device.
- Click **Restore All to Defaults** to restore the default page configuration, including the logo and text.
- Click **Refresh** to obtain the latest push information.
- Set **Info Push Type** to **Common**, **All**, or **Revised**. The page will display common, all, or modified blocking page information.

7.9 System Maintenance

7.9.1 Viewing Device Information

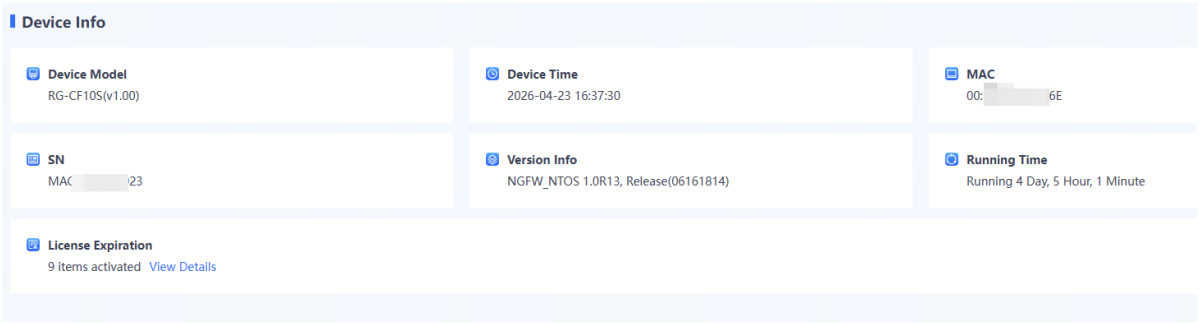
Application Scenario

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.



7.9.2 Managing Configuration Backup

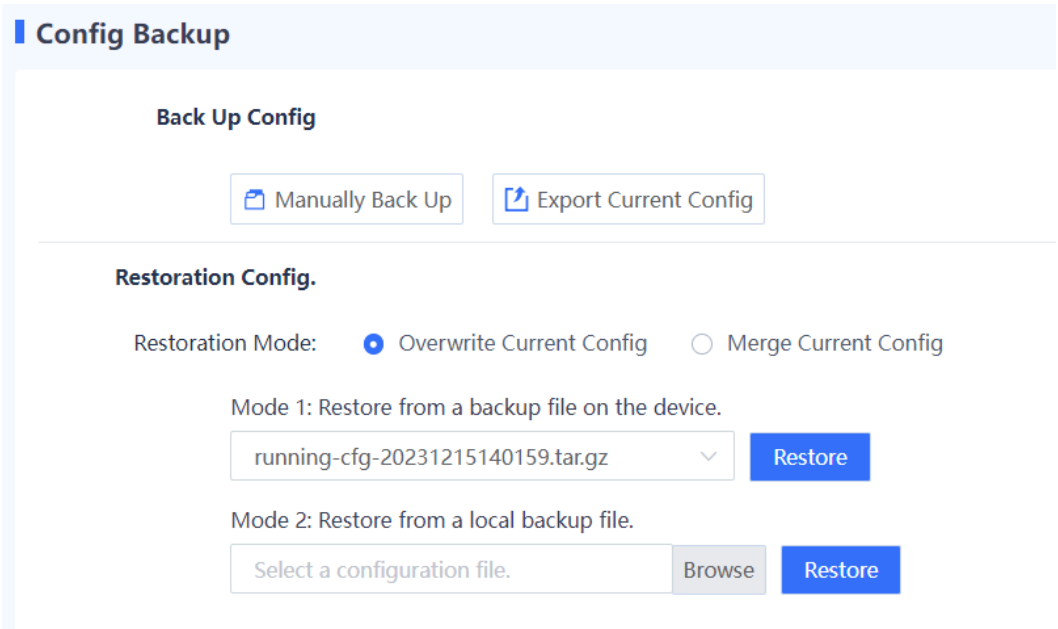
1. Backing Up Configuration Files

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.

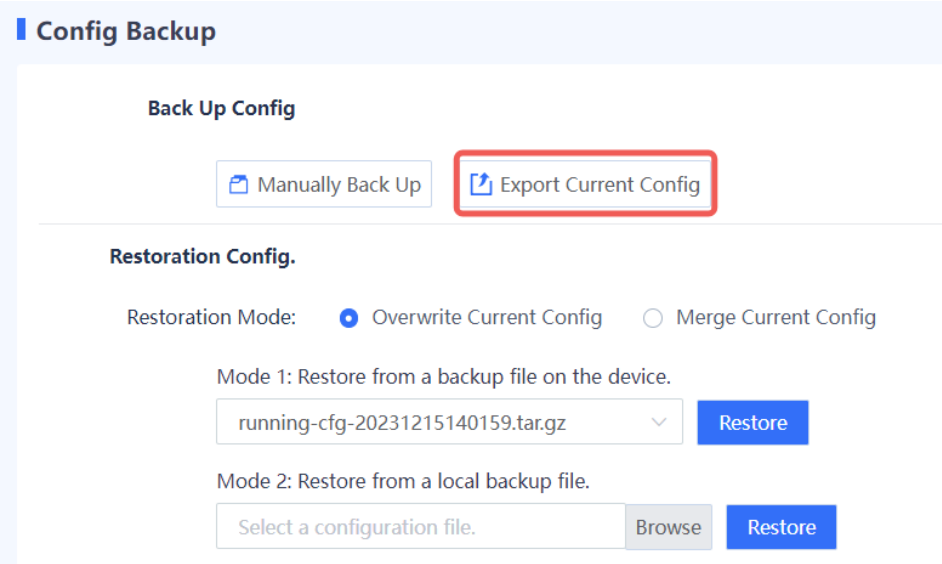
Procedure

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

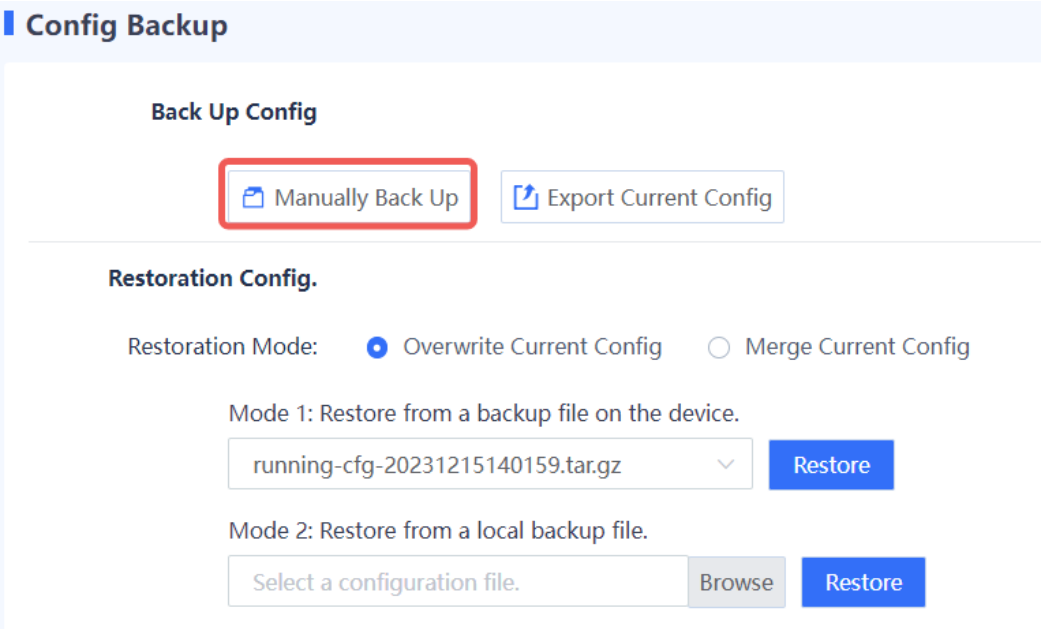


(2) You can back up configuration files in one of the following ways:

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



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



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.

The device supports two restoration modes:

- **Overwrite Current Config**: After the backup configuration file is imported, the entire configuration file of the

device is replaced, and the original configuration is overwritten.

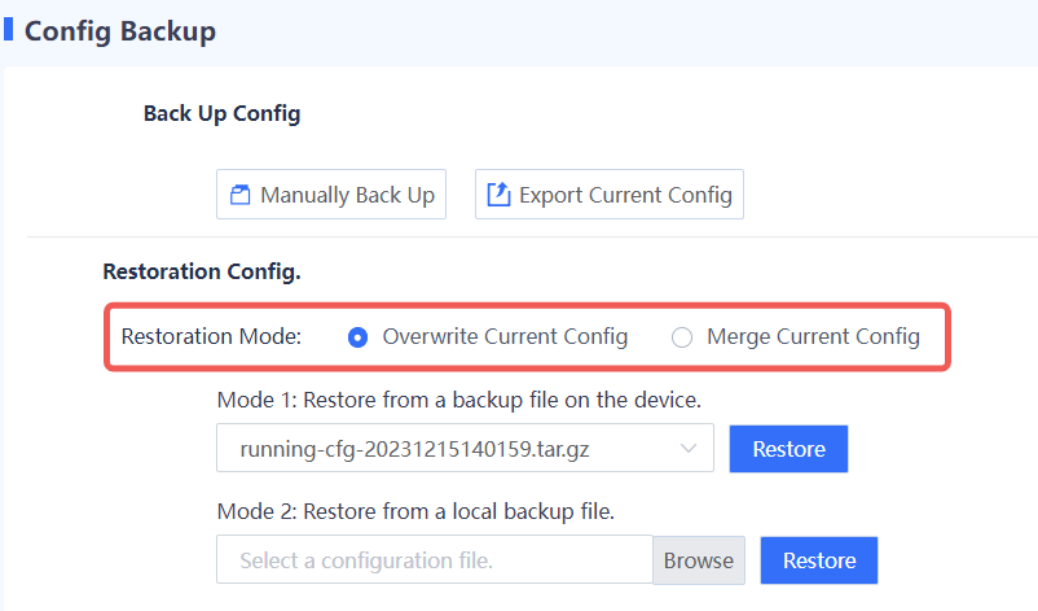
- **Merge Current Config**: After the backup configuration file is imported, the current configuration file and the backup configuration file are merged. (Unique configurations in the two configuration files are retained. For conflicting configurations, configuration in the backup configuration file overwrites the original configuration).

Procedure

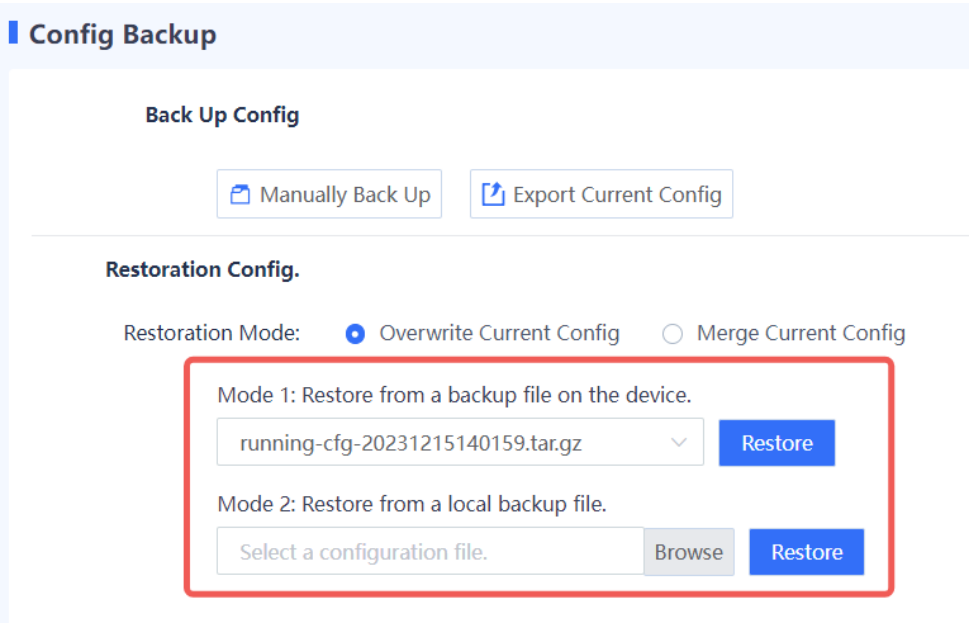
(1) Choose **System** > **System Maintenance** > **Config Backup**.

(2) In the **Restoration Config** area, configure parameters as required.

- Select a restoration mode.



- 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.

7.9.3 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

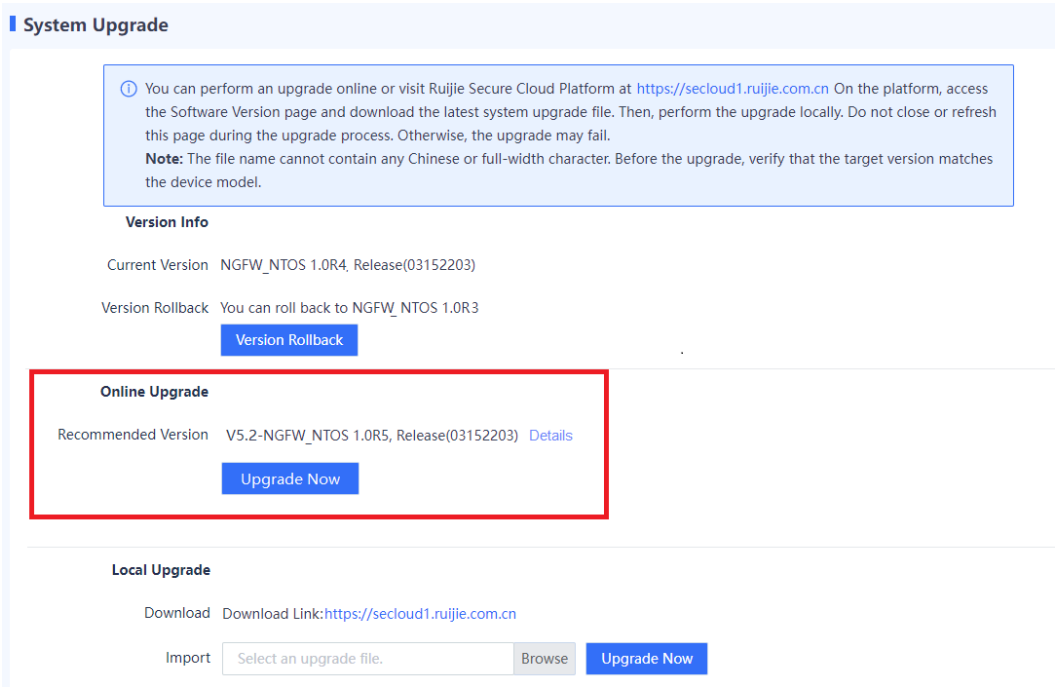
When the network communication between the device and Ruijie Secure Cloud Platform is normal, and the system displays a recommended version, you can upgrade the software version in online mode.

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**.

Note

In HA mode, the device supports In-Service Software Upgrade (ISSU). Click **Upgrade Now** on the web UI of the active device, the software version of the standby device will also be automatically upgraded. In active-active mode, the active and standby devices of ISSU are the same as the active and passive devices in HA Group 0. The ISSU process is as follows:

(1) The standby device is upgraded first and takes over service traffic after the upgrade succeeds.

(2) After switching the service traffic to the standby device, the active device starts the upgrade.

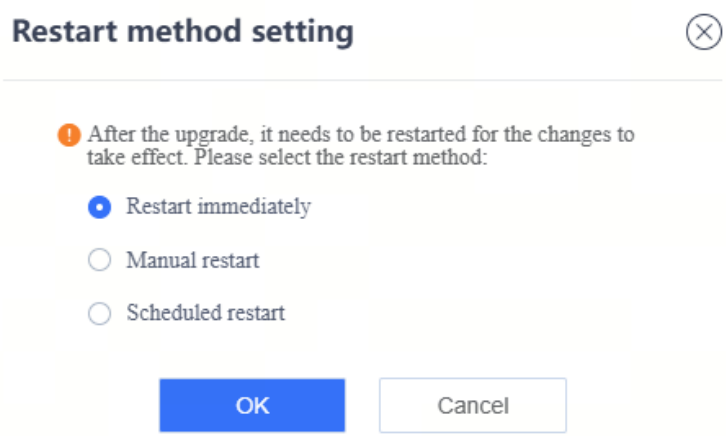
(3) After the active device is upgraded, it becomes the standby device.

(3) In the dialog box that is displayed, select a restart mode after successful upgrade and click **OK**. The upgraded version takes effect after device restart.

- **Restart immediately**: Automatically restart the device immediately after version upgrade.
- **Manual restart**: Manually restart the device after version upgrade.
- **Scheduled restart**: Automatically restart the device at the specified time after version upgrade.

Note

In the HA scenario, the backup device is automatically upgraded after the master device is upgraded, and the master and backup devices must be restarted automatically. You cannot select **Manual restart** or **Scheduled restart** in the HA scenario.



Follow-up Procedure

- When you set the restart mode to **Scheduled restart** or **Manual restart** after successful upgrade, you can modify the restart mode or scheduled restart time after importing the upgrade file.
- Choose **System** > **System Maintenance** > **Device Info** to view the software version information and confirm whether the upgrade is successful.

2. Offline Upgrade

Application Scenario

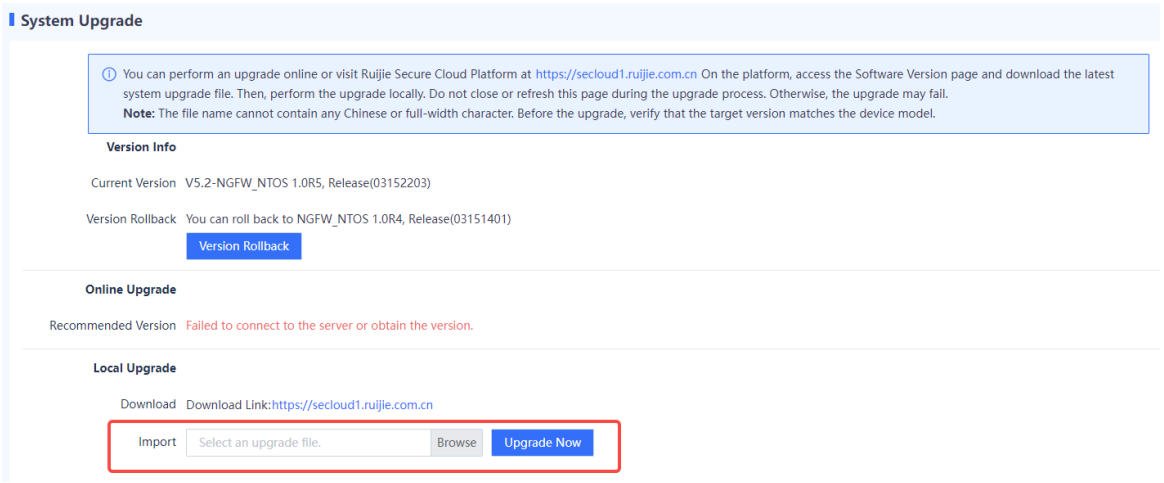
When a network exception occurs between the device and Ruijie Secure Cloud Platform, the system cannot automatically obtain the latest software version. You can upgrade or roll back the software version in offline mode.

Prerequisites

You have obtained the upgrade file in advance. To obtain the upgrade file, log in to the Ruijie Secure Cloud Platform (https://secloud1.ruijie.com.cn), choose **Version Management** > **Software Version Management** > **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.

Note

In HA mode, the device supports In-Service Software Upgrade (ISSU) in online mode. Select an upgrade file on the active device and click **Upgrade Now**. The software version of the standby device is upgraded automatically. In active-active load balancing mode, the ISSU active and standby devices are the active and standby devices in group 0. ISSU upgrade process:

(1) The standby device is upgraded to the new version and then takes over traffic forwarding after the upgrade succeeds.

(2) After the standby device is successfully upgraded, the active device switches service traffic to the standby device and starts the upgrade.

(3) After the active device is upgraded successfully, it becomes the standby device.

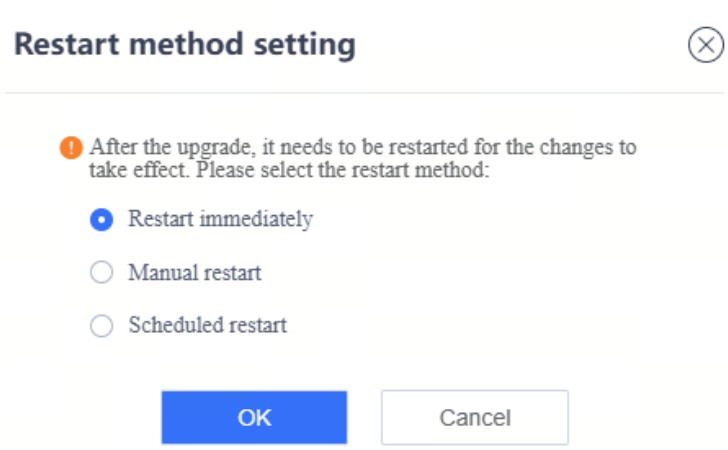
(3) Click **Upgrade Now** to start system upgrade.

(4) In the dialog box that is displayed, select a restart mode after successful upgrade and click **OK**. The upgraded version takes effect after device restart.

- **Restart immediately**: Automatically restart the device immediately after version upgrade.
- **Manual restart**: Manually restart the device after version upgrade.
- **Scheduled restart**: Automatically restart the device at the specified time after version upgrade.

Note

In the HA scenario, the backup device is automatically upgraded after the master device is upgraded, and the master and backup devices must be restarted automatically. You cannot select **Manual restart** or **Scheduled restart** in the HA scenario.



Follow-up Procedure

- When you set the restart mode to **Scheduled restart** or **Manual restart** after successful upgrade, you can modify the restart mode or scheduled restart time after importing the upgrade file.
- Choose **System** > **System Maintenance** > **Device Info** to view the software version information and confirm whether the upgrade is successful.

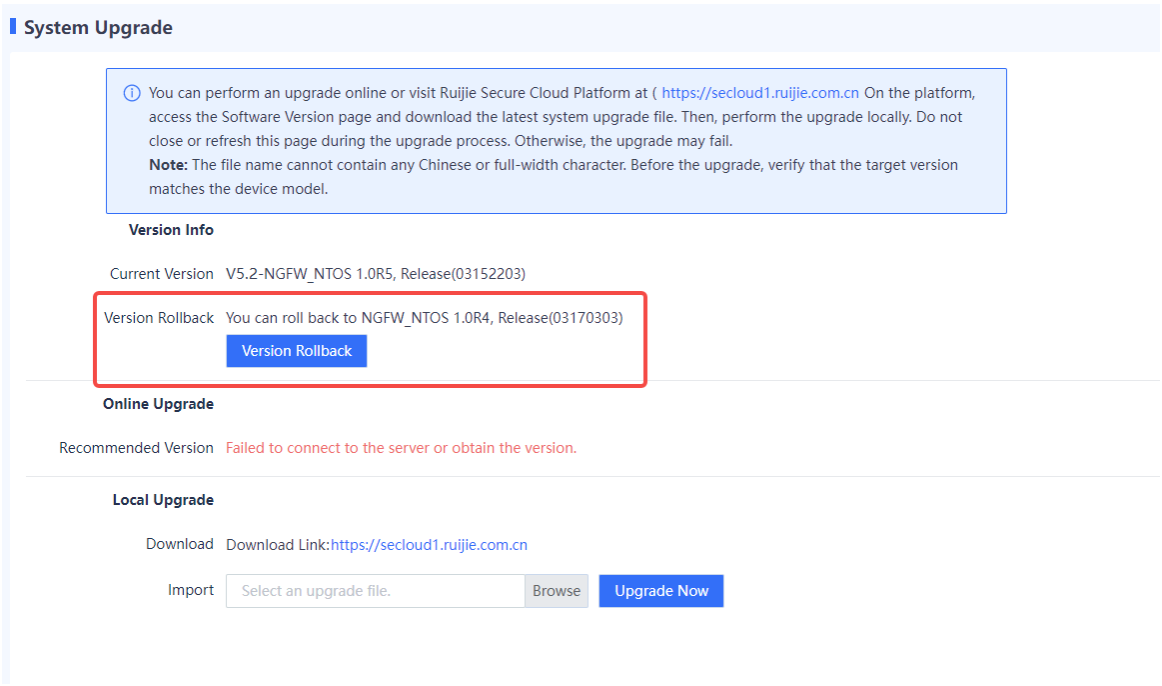
3. Version Rollback

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**.

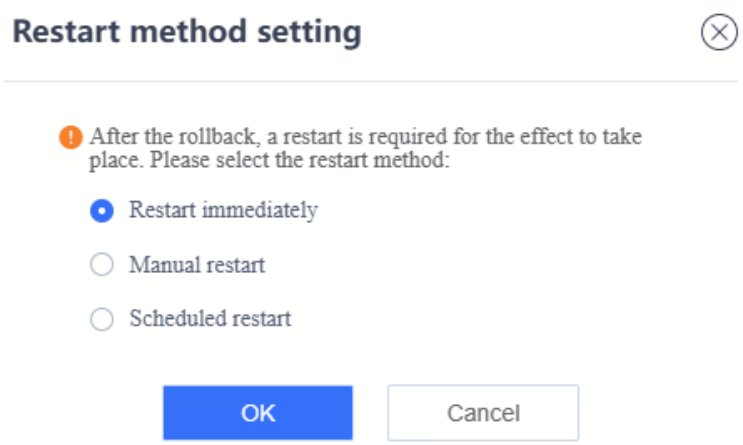


(2) In the **Version Info** area, click **Version Rollback**.

(3) In the dialog box that is displayed, select a restart mode, and click **OK**. The version rolled back takes effect after device restart.

Note

In the HA scenario, the backup device is automatically rolled back after the master device is rolled back, and the master and backup devices must be restarted automatically. You cannot select **Manual restart** or **Scheduled restart** in the HA scenario.



Follow-up Procedure

- When you set the restart mode to **Scheduled restart** or **Manual restart** after successful rollback, you can modify the restart mode or scheduled restart time.
- Choose **System** > **System Maintenance** > **Device Info** to view the software version information and check whether the version is successfully rolled back.

7.9.4 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

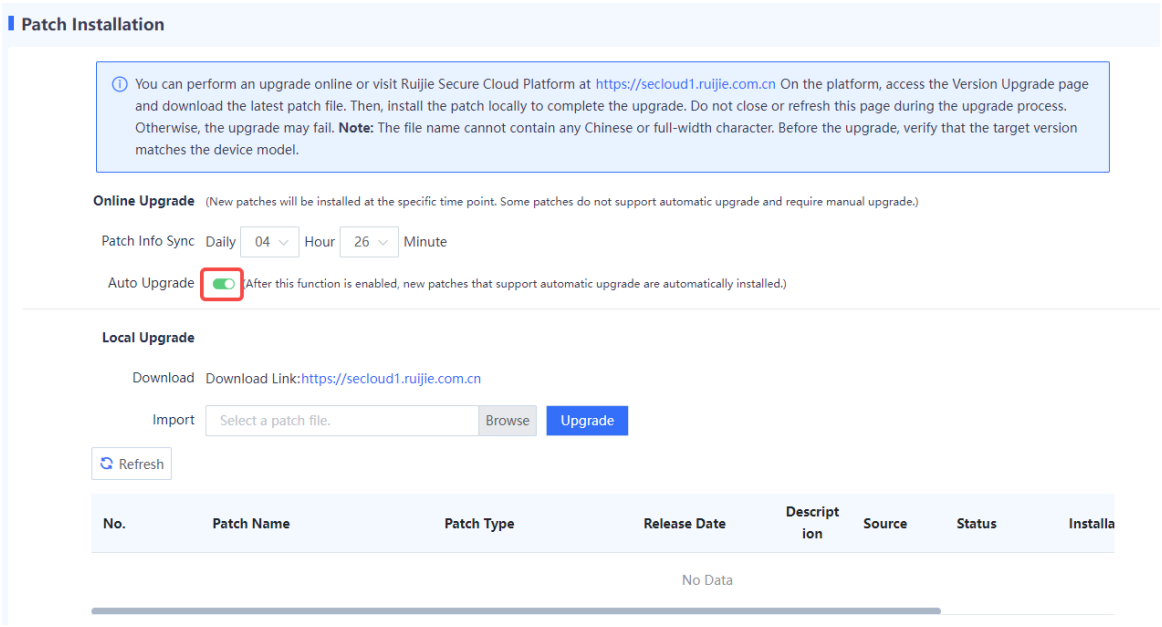
You can perform online upgrade when the device can properly communicate with the Ruijie Secure Cloud Platform.

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

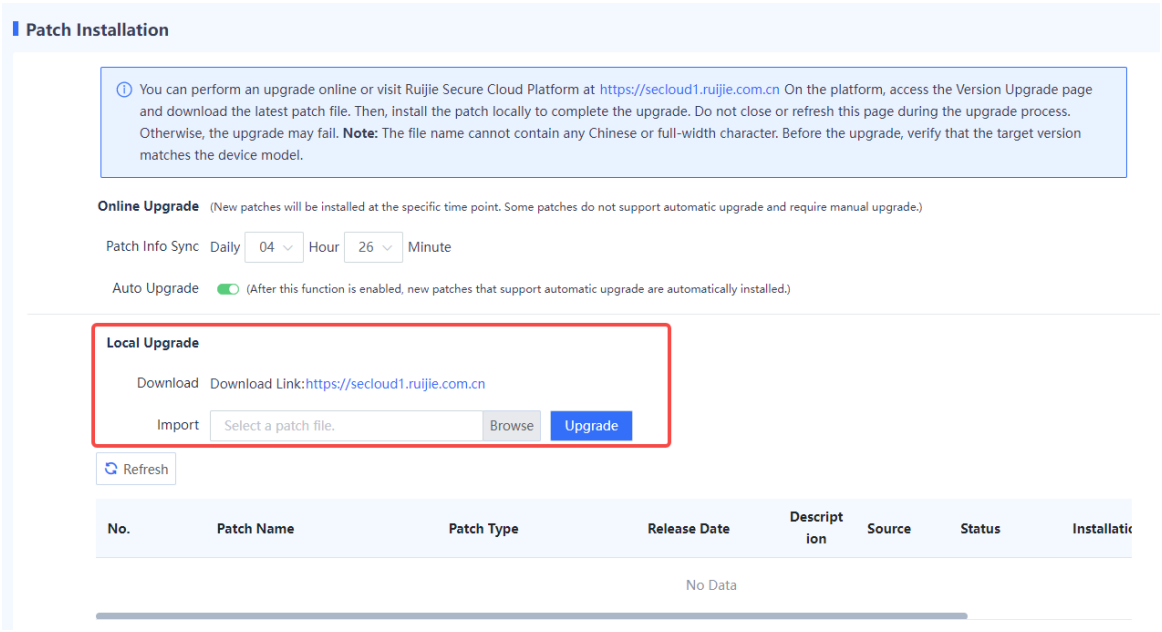
When a network exception occurs between the device and Ruijie Secure Cloud Platform, the system cannot automatically obtain the latest software version. You can install patches in offline mode.

Prerequisites

You have obtained the patch file in advance. To obtain the patch file, log in to the Ruijie Secure Cloud Platform (https://secloud1.ruijie.com.cn/), choose **Version Management** > **Software Version Management** > **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.

7.9.5 Speed Test Mode

Application Scenario

Security functions, such as application identification, flow control, session control, user authentication, flow analysis, and threat intelligence, may occupy some device performance. Therefore, during network speed test, you can enable the speed test mode to reduce the impact of security functions on the test result and obtain a more accurate test result.

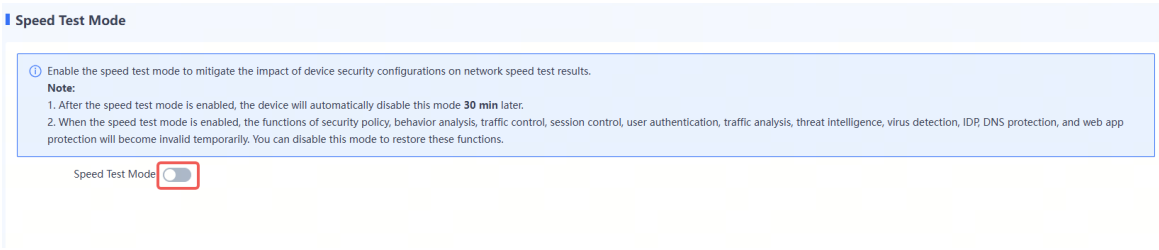
Caution

- After the speed test function is enabled, the device automatically disables the speed test mode 30 minutes later.
- After the speed test function is enabled, the security policy, application identification, flow control, session control, user authentication, flow analysis, and threat intelligence functions will become invalid temporarily. You can disable the speed test function to restore the functions.
- Do not enable the speed test mode in non-test scenarios, and disable the speed test mode immediately after the test is complete to ensure the normal operation of security services.

Procedure

(1) Choose **System** > **System Maintenance** > **Speed Test Mode**.

(2) Toggle on **Speed Test Mode**. In the displayed dialog box, click **Confirm**.



Follow-up Procedure

Turn off Speed Test Mode to disable it.

7.9.6 Restarting the Device

Application Scenario

You can restart the device when it fails and cannot be restored.

Prerequisites

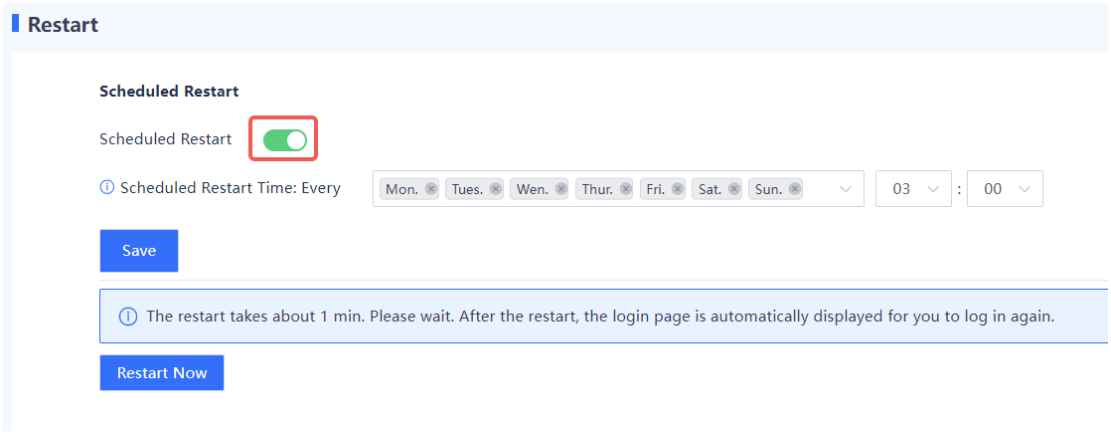
- When a firewall is not running properly, troubleshoot the issue first rather than simply restarting the system, which prevents services from being affected.
- However, if you have to restart the system, you are advised to do so during an off-peak period to minimize impact on the services, such as late at night.
- To avoid loss of temporary data due to restart, ensure that you have saved configuration files before restarting.

Procedure

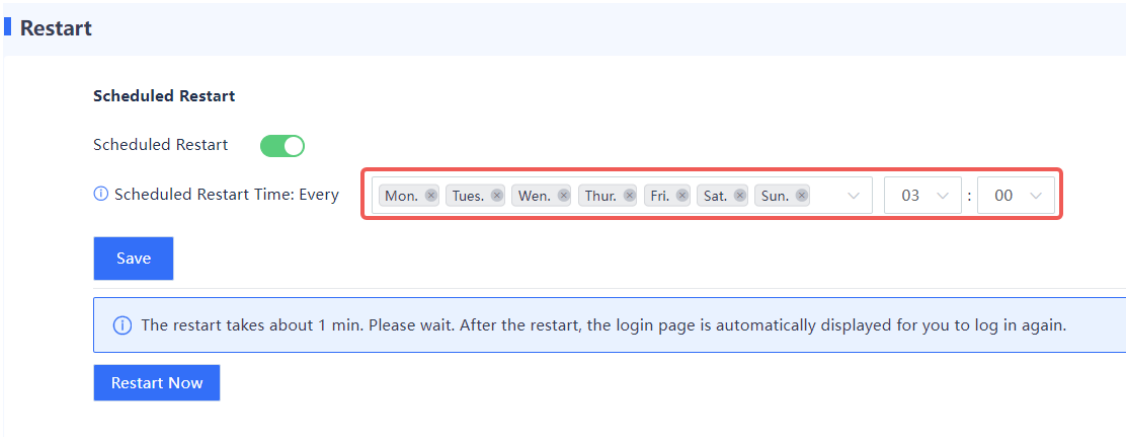
(1) Choose **System** > **System Maintenance** > **Restart**.

(2) Enable scheduled restart.

a Toggle on  to enable scheduled restart.

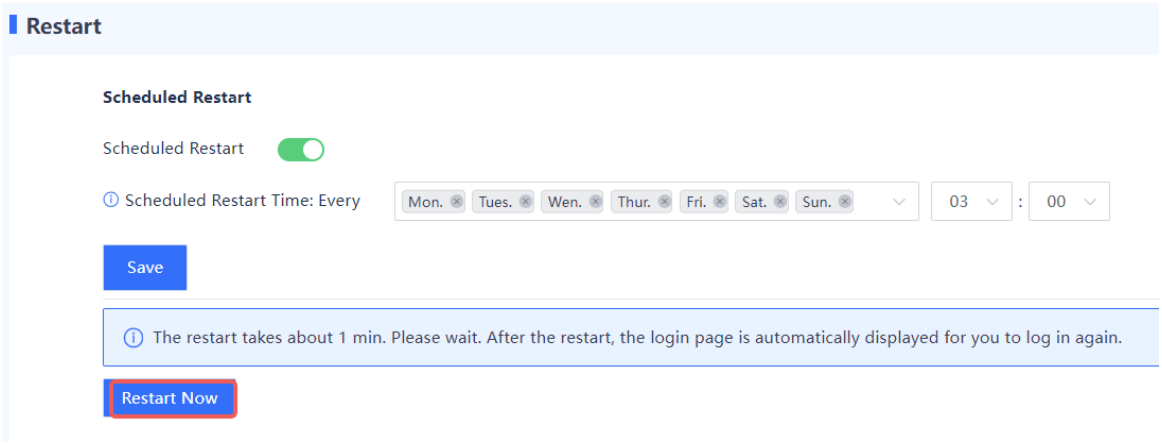


b Set the time points for scheduled restart.



c Click **Save**. The scheduled restart takes effect, and the device will restart at the set time points.

(3) (Optional) Click **Restart Now**. In the dialog box that is displayed, click **OK** to restart the device immediately.



7.9.7 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.

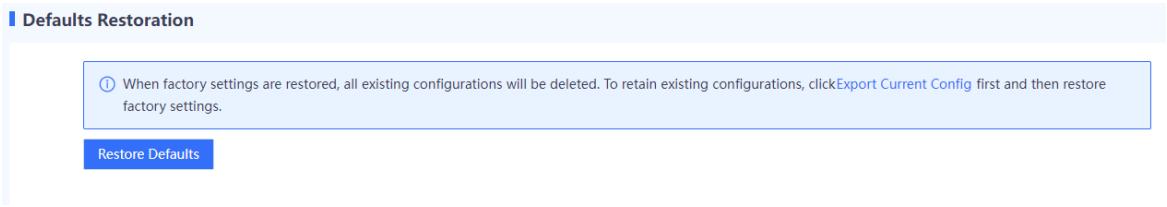
Caution

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 10.20.30.42.
- The administrator account name and password are restored to **admin/firewall**.

8 Operation Management

8.1 Viewing Authenticated Online Users

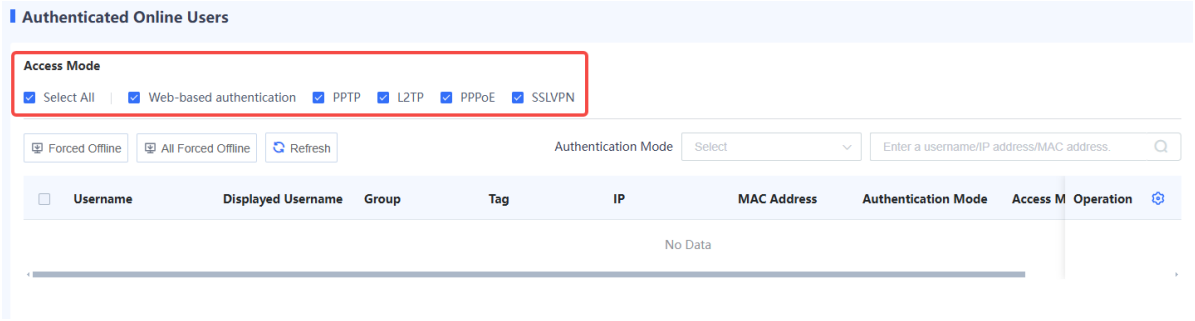
Application Scenario

This page displays details about online users who access the network through various authentication modes, including web authentication, PPPoE authentication, Secure Sockets Layer Virtual Private Network (SSL VPN), and PPTP VPN. You can disconnect users on this page.

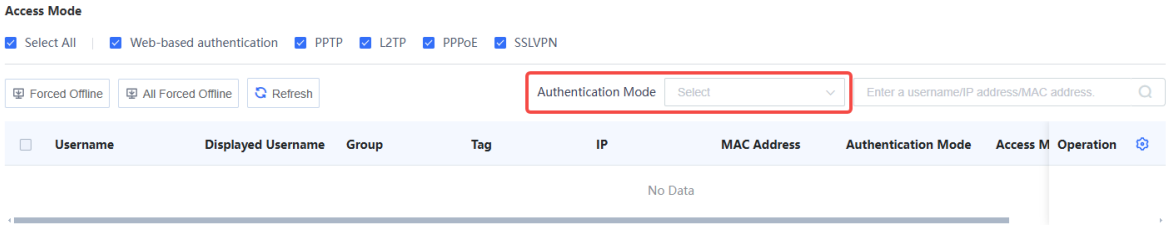
Procedure

(1) Choose **O&M** > **Authenticated Online Users**.

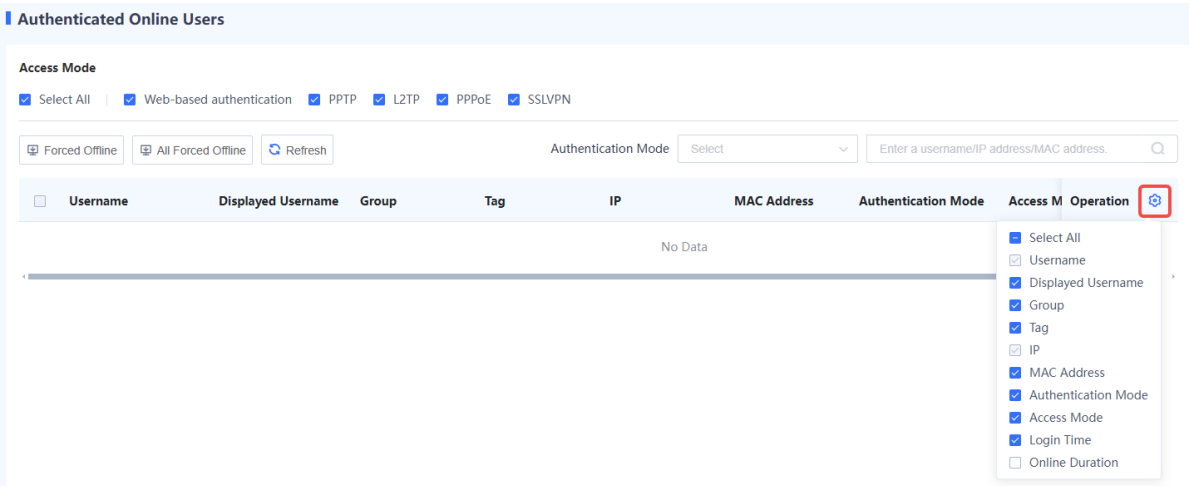
(2) Set **Access Mode**. Online user data of the corresponding access mode is displayed.



If you select **Web-based authentication**, you can set **Authentication Mode** to display online users who are authenticated using that mode.



(3) Click the icon next to **Operation** to select the fields for display.



(4) Click **Refresh** to view the latest online user data.

(5) In the **Operation** column of an online user record, click **Offline** in the **Operation** column to force the user offline.

To disconnect users in batches, select multiple records and click **Forced Offline**.

To force all online users offline, click **All Forced Offline** at the top of the page.

8.2 Security

8.2.1 Security Cockpit

1. Traffic Overview

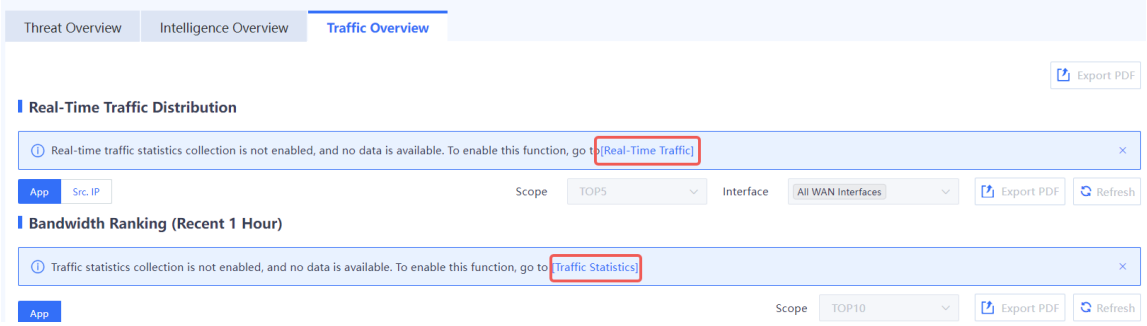
Application Scenario

The traffic overview function of the security cockpit helps you understand the real-time traffic distribution and bandwidth ranking.

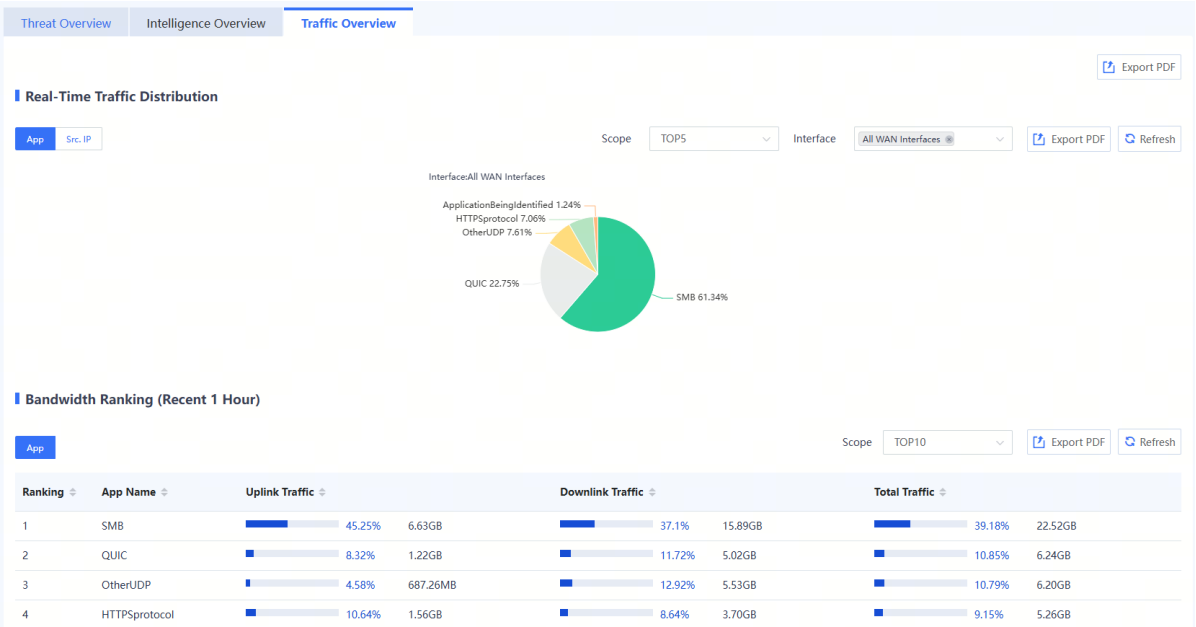
Procedure

(1) Choose **O&M** > **Security** > **Security Cockpit** > **Traffic Overview**.

Traffic analysis is disabled by default. Data is available only when traffic analysis is enabled.



(2) View the real-time traffic distribution of the corresponding application or source IP address and application bandwidth ranking.



Follow-up Procedure

- Set **Scope** to view specific traffic statistics.
- Set **Interface** to view traffic statistics on specified interfaces.
- Click **Export PDF** in the upper right corner to export statistics (including traffic statistics of source IP addresses as well as traffic statistics and bandwidth ranking of applications) in the last 5 seconds to a local PDF file for subsequent reading and query.
- Click **Export PDF** in the **Real-Time Traffic Distribution** area to export statistics (including traffic statistics of source IP addresses and traffic statistics of applications) in the last 5 seconds to a local PDF file for subsequent reading and query.
- Click **Export PDF** in the **Bandwidth Ranking** area to export the application bandwidth statistics in the last 1 hour to a local PDF file for subsequent reading and query.
- Click **Refresh** to obtain the latest traffic distribution and bandwidth ranking.

2. Threat Overview

Application Scenario

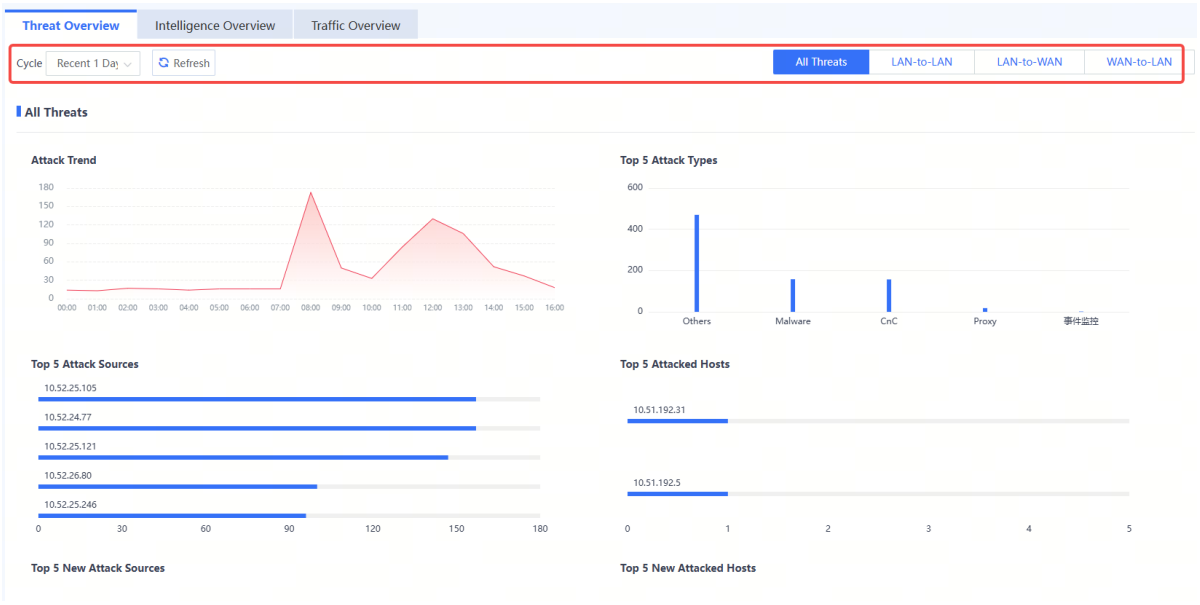
The threat overview function of the security cockpit is the attack statistics collection function of the firewall. It effectively helps you identify the most common types of threats, frequent attackers engaged in malicious network activities, and objects that are frequently targeted in attacks. This information allows you 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 **O&M** > **Security** > **Security Cockpit** > **Threat Overview**. On the page that is displayed, select **Recent** from the **Cycle** drop-down list.

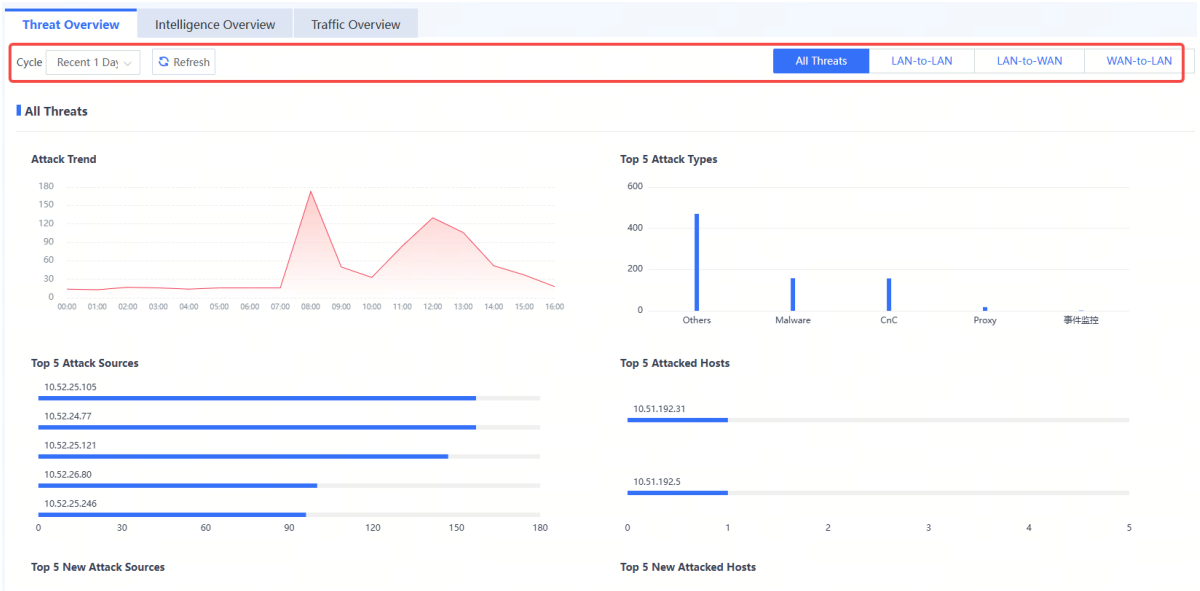
(2) Set the display cycle, and select the attack type.



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.



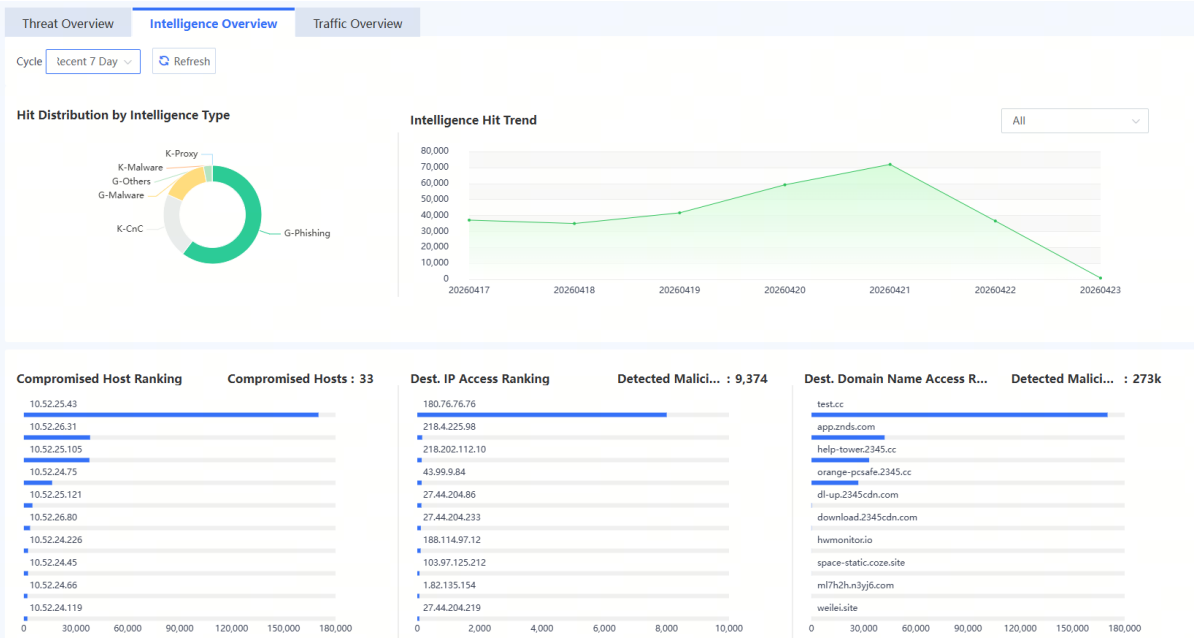
3. Intelligence Overview

Application Scenario

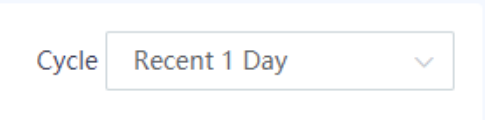
The intelligence overview function is used to display the hit distribution by intelligence type and the intelligence hit trend. This information can help administrators effectively learn about threats on the live network and then define more refined protection policies to protect LAN hosts.

Procedure

(1) Choose **O&M** > **Security** > **Security Cockpit** > **Intelligence Overview**.



(2) Click the drop-down list 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 seven 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.

Item	Description
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.
Compromised Host Ranking	When an intranet host accesses an external website and the destination IP address or domain name of the access traffic matches outbound TI, the system ranks the IP addresses of the intranet hosts by the hit count. This helps the administrator analyze the hosts controlled or compromised by malicious programs on the network and thereby take corresponding defense measures to block traffic from these host IP addresses. Click an IP address to switch to the security log page. Security logs of the host IP address are automatically displayed.
Dest. IP Access Ranking	When an intranet host accesses an external malicious website, the system ranks the destination IP addresses by the hit count of outbound TI. This helps the administrator analyze malicious IP addresses and thereby take corresponding defense measures to protect hosts. Click an IP address to switch to the security log page. Security logs of this destination IP address are automatically displayed.
Dest. Domain Name Access Ranking	When an intranet host accesses an external malicious website, the system ranks the domain names by the hit count of outbound TI. This helps the administrator analyze malicious domain names and thereby take corresponding defense measures to block traffic and protect hosts. Click a domain name to switch to the security log page. Security logs of this domain name are automatically displayed.
Top 5 Attack Sources	For WAN-to-LAN attacks, the source IP addresses matching inbound threat intelligence are ranked by the number of hits. This information helps administrators analyze the threat source and then develop corresponding protection measures to block the traffic from these source IP addresses. Click an IP address to switch to the security log page. Security logs of this source IP address are automatically displayed.

Item	Description
Top 5 Attacked Hosts	For WAN-to-LAN attacks, the destination IP addresses matching inbound threat intelligence are ranked by the number of hits. This information helps administrators identify intranet hosts vulnerable to attacks and then develop corresponding protection measures to protect these hosts. Click an IP address to switch to the security log page. Security logs of this destination IP address are automatically displayed.

8.2.2 Source Tracing

Application Scenario

During routine security operations, you can enter the IP address and other related information to trace the MAC address of the corresponding user or terminal in one click mode, so as to analyze the traffic on the live network and protect and process the user or terminal accordingly. If a device is deployed in non-routing mode, the device cannot record NAT-translated source addresses. The device uses other information such as the destination address for source tracing.

The source tracing feature is used to query database logs, including session logs, security logs, and URL audit logs. Typically, session logs can be used to locate the user or MAC address, and security logs and URL audit logs are used for reference.

Precautions

- The source tracing function is supported only when a hard disk is installed.

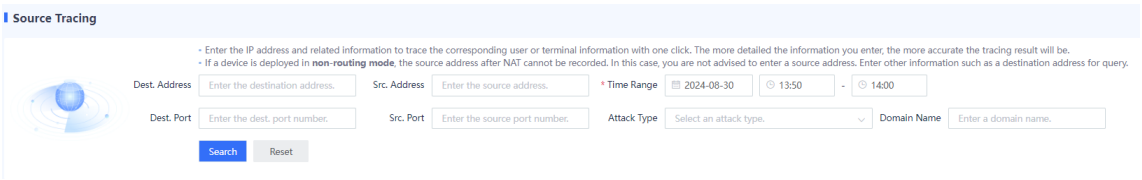
Prerequisites

- To trace terminal MAC addresses, enable terminal MAC address identification. For details, see 7.3.2 Network Device Association.
- To trace usernames, enable real-name user information reception. For details, see 7.3.1 Identity System Association.

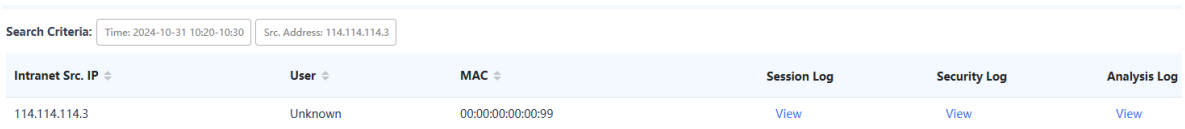
Procedure

(1) Choose **O&M** > **Security** > **Source Tracing**.

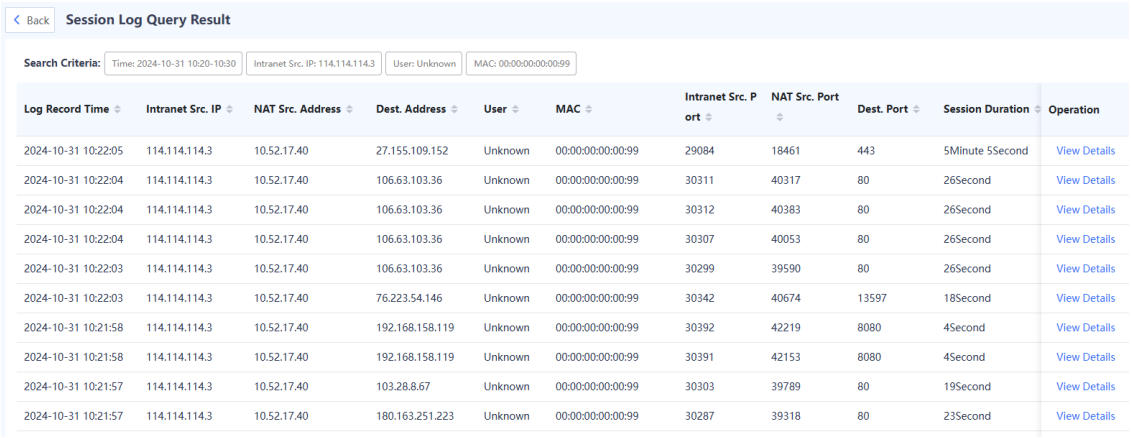
(2) Enter the IP address and other information about the attack source to be traced.



(3) Click **Search** to display query results.



(4) Click **View** to display the specific log query result.

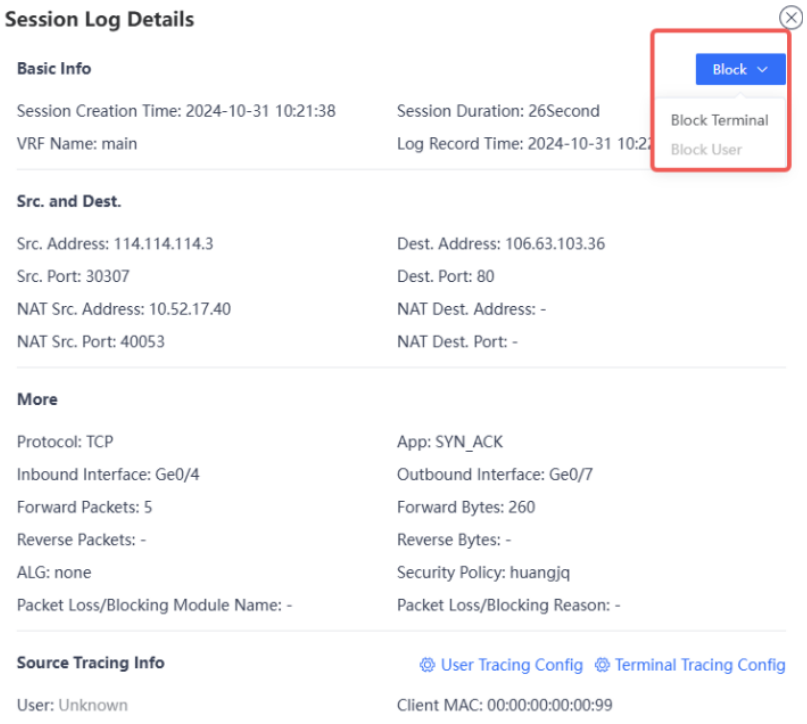


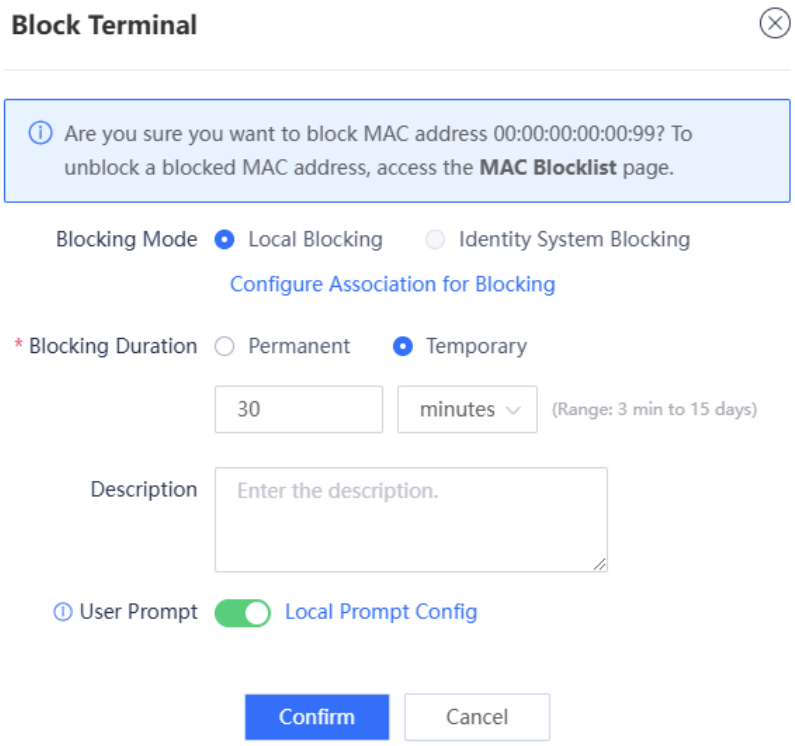
Log Record Time	Intranet Src. IP	NAT Src. Address	Dest. Address	User	MAC	Intranet Src. Port	NAT Src. Port	Dest. Port	Session Duration	Operation
2024-10-31 10:22:05	114.114.114.3	10.52.17.40	27.155.109.152	Unknown	00:00:00:00:00:99	29084	18461	443	5Minute 5Second	View Details
2024-10-31 10:22:04	114.114.114.3	10.52.17.40	106.63.103.36	Unknown	00:00:00:00:00:99	30311	40317	80	26Second	View Details
2024-10-31 10:22:04	114.114.114.3	10.52.17.40	106.63.103.36	Unknown	00:00:00:00:00:99	30312	40383	80	26Second	View Details
2024-10-31 10:22:04	114.114.114.3	10.52.17.40	106.63.103.36	Unknown	00:00:00:00:00:99	30307	40053	80	26Second	View Details
2024-10-31 10:22:03	114.114.114.3	10.52.17.40	106.63.103.36	Unknown	00:00:00:00:00:99	30299	39590	80	26Second	View Details
2024-10-31 10:22:03	114.114.114.3	10.52.17.40	76.223.54.146	Unknown	00:00:00:00:00:99	30342	40674	13597	18Second	View Details
2024-10-31 10:21:58	114.114.114.3	10.52.17.40	192.168.158.119	Unknown	00:00:00:00:00:99	30392	42219	8080	4Second	View Details
2024-10-31 10:21:58	114.114.114.3	10.52.17.40	192.168.158.119	Unknown	00:00:00:00:00:99	30391	42153	8080	4Second	View Details
2024-10-31 10:21:57	114.114.114.3	10.52.17.40	103.28.8.67	Unknown	00:00:00:00:00:99	30303	39789	80	19Second	View Details
2024-10-31 10:21:57	114.114.114.3	10.52.17.40	180.163.251.223	Unknown	00:00:00:00:00:99	30287	39318	80	23Second	View Details

(5) Click **View Details** in the **Operation** column to query log details. On the **Session Log Details** page, click **Block User** or **Block Terminal** to add the user/terminal to the user/MAC address blocklist. Blocking users may prevent authorized users from accessing the Internet. MAC address-based blocking is more precise in blocking abnormal terminals.

Note

- When the user name is empty, that is, **User** is displayed as **Unknown**, the **Block User** button is unavailable.
- When the MAC address of a terminal is empty, that is, **Client MAC** is displayed as **Unknown**, the **Block Terminal** button is unavailable.





8.3 Log Monitoring Management

8.3.1 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.

8.3.2 Querying Logs

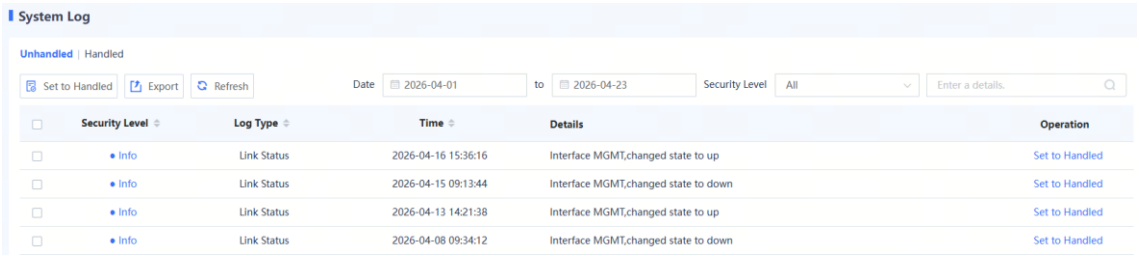
1. Querying System Logs

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 **O&M** > **Logs** > **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 **O&M** > **Logs** > **Security Log**.

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

Note

Click the drop-down list icon next to **Operation** to set the fields to be displayed on the page.



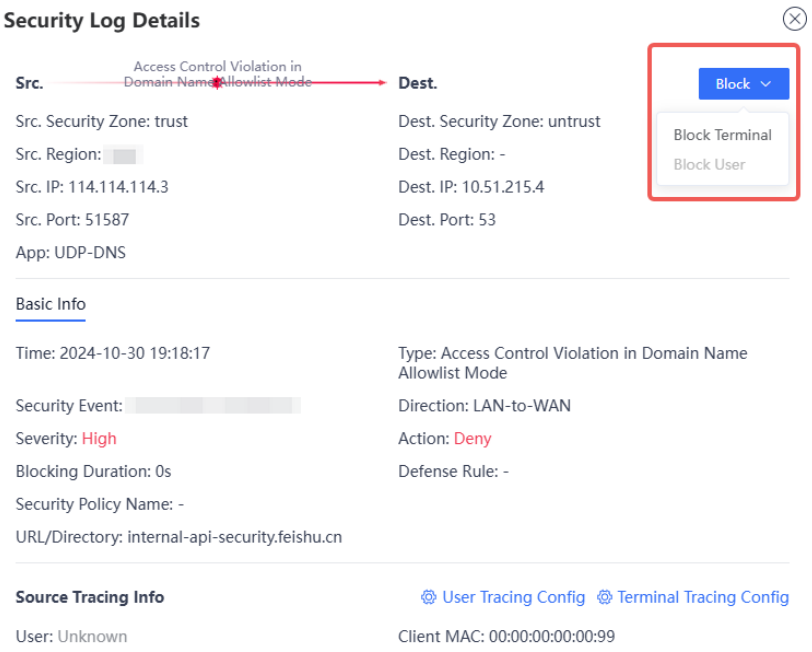
Field	Description
Severity	Severity level of a problem marked in the security log.
Security Event	Description of a security event recorded in the log.
Log Type	Type of a security event recorded in the log. [Example] IPS attack
Attack Type	Type of the attack recorded in the log. [Example] Heap Overflow
Defense Rule	Rule ID, which corresponds to the rule ID in the security rule base.
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. Region	Source region of 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.
Ruijie Reyee App	Application type of the session recorded in the log.
Action	Operation result of a security policy on the traffic.
User	User of the security policy. If the user is authenticated, the account name is displayed. Otherwise, the source IP address is displayed.
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. Up to 10,000 latest logs in the list can be exported.
- Click **Refresh** to obtain the latest security logs.
- Click **View Details** in the **Operation** column to query log details. On the **Session Log Details** page, click **Block User** or **Block Terminal** to add a user or terminal to the user or MAC address blocklist. When the user name is empty, that is, **User** is displayed as **Unknown**, the **Block User** button is unavailable. When the MAC address of a terminal is empty, that is, **Client MAC** is displayed as **Unknown**, the **Block Terminal** button is unavailable.



3. Querying URL Logs

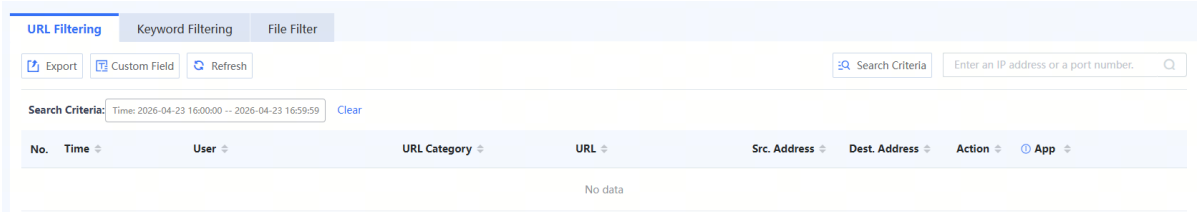
Application Scenario

By viewing URL logs, administrators can check the hit status of the URL filtering templates.

Procedure

(1) Choose **O&M** > **Logs** > **Content Filtering Log** > **URL Filtering**.

(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 **Custom Field**, and set the fields displayed on the page.
- Click **Refresh** to obtain the latest URL logs.

4. Querying Keyword Filter Logs

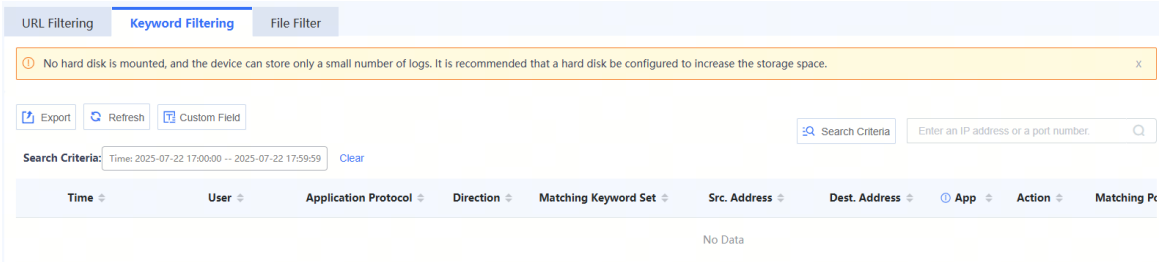
Application Scenario

By viewing the logs, administrators can check the hit status of the keyword filtering templates.

Procedure

(1) Choose **O&M** > **Logs** > **Content Filtering Log** > **Keyword Filtering**.

(2) The keyword filter log information is displayed on the web page.



Note

You can click **Search Criteria** to set the keywords for log query. Only keyword filter logs matching the search criteria are displayed on the page.

Follow-up Procedure

- Click **Export** to export keyword filter logs to the local device in the Excel format, facilitating subsequent queries.
- Click **Custom Field,** and set the fields displayed on the page.
- Click **Refresh** to obtain the latest keyword filter logs.

5. Query File Filtering Logs

Application Scenario

After a file filter template is referenced in a security policy, the device will perform content inspection on traffic that matches the policy. If the transmitted files hit file filtering rules with actions of blocking or alarming, file filtering logs will be generated.

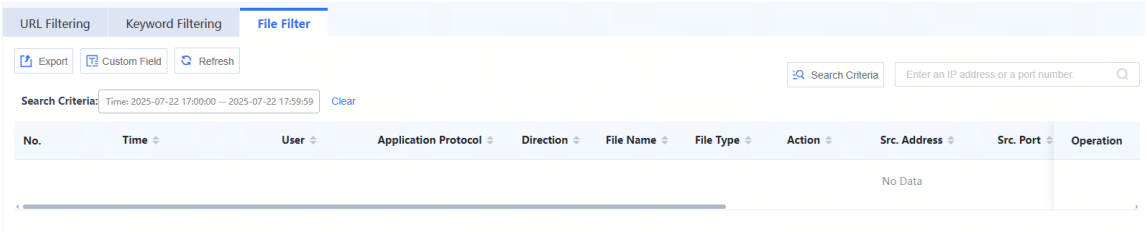
By viewing file filtering logs, you can check whether file filtering rules are matched and verify whether the file filtering function takes effect.

Procedure

(1) Choose **O&M** > **Logs** > **Content Filtering Log** > **File Filter**.

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

(3) Information about file filtering logs is displayed on the web UI.



Field	Description
No.	Log ID.
Time	Time when a log was generated.
User	User that uploads or downloads files.
MAC	MAC address of the terminal that uploads or downloads files.
Application Protocol	Application layer protocol used for transmitting the file, such as HTTP and FTP.
Direction	File transfer direction, which can be upload or download.
File Name	Name of a file.
File Type	File type.
Action	File processing action.
Src. Address	File transfer source IP address.
Src. Port	File transfer source port.
Dest. Address	File transfer destination IP address.
Dest. Port	File transfer destination port.
App	Application for transmitting the file.

Field	Description
Matching Policy	Matched security policy.
Matching Template	Matched file filter template.

Note

Click **Search Criteria** to set search criteria. Only logs that meet the search criteria are displayed on the page.

Follow-up Procedure

- Click **Export** to export logs to an Excel file locally for reading and query.
- Click **Custom Field** to set the fields to be displayed on the page.
- Click **Refresh** to obtain the latest logs.

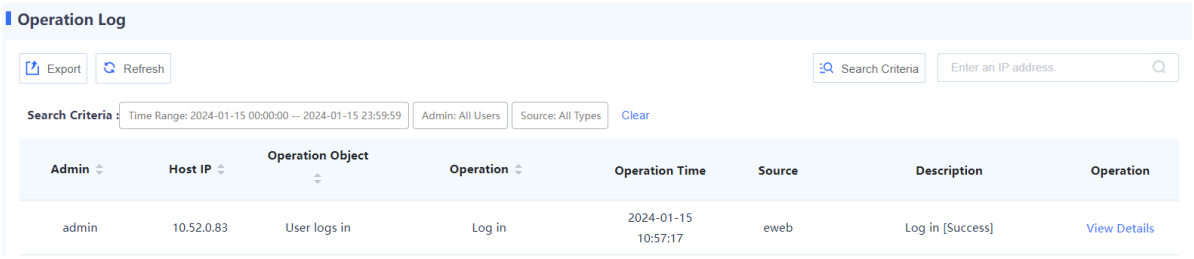
6. Querying Operation Logs

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 **O&M** > **Logs** > **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.

Field	Description
Source	Operation mode of the administrator, including Eweb, SSH, Bash, and login.
Test Result	Execution result of the administrator's 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.

7. Querying SSL VPN Logs

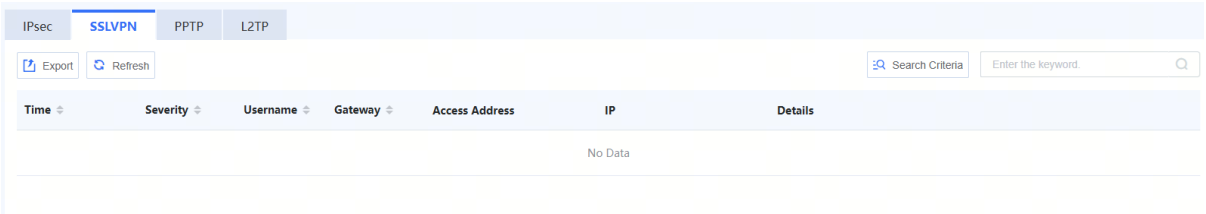
Application Scenario

By viewing the logs, administrators can check details about SSL VPN sessions.

Procedure

(1) Choose **O&M** > **Logs** > **VPN Log** > **SSLVPN**.

(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.

8. Querying IPsec VPN Logs

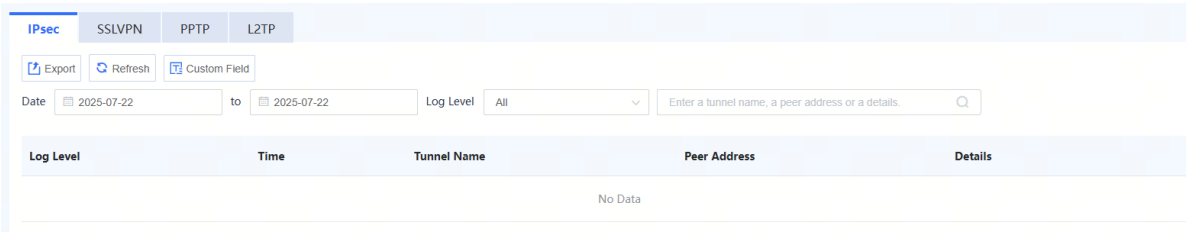
Application Scenario

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 **O&M** > **Logs** > **VPN Log** > **IPsec**.

(2) The information about IPsec VPN logs is displayed on the web page.



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.

9. Querying PPTP Logs

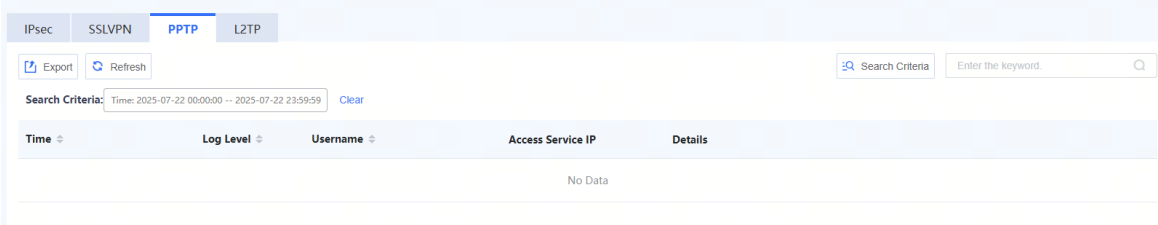
Application Scenario

PPTP logs record important events and exceptions occurring during PPTP tunnel running. They help administrators understand the running status of PPTP tunnels and locate and solve exceptions of the PPTP VPN function.

Procedure

(1) Choose **O&M** > **Logs** > **VPN Log** > **PPTP**.

(2) This page displays PPTP log information.



Field	Description
Time	Time when a log is recorded.
Log Level	The importance level of log. Logs are classified into four levels in descending order of importance: informational, low, medium, and high.
Username	Username for accessing a PPTP server.
Access Service IP	Actual IP address of the peer (PPTP client) of the tunnel.
Details	Log content.

Note

You can set query criteria such as the log record date, log level, and access service IP address. The web UI displays only the logs that meet the query criteria.

Follow-up Procedure

- Click **Export** to export logs to an Excel file locally for reading and query.
- Click **Refresh** to obtain the latest logs.

10. Querying L2TP Logs

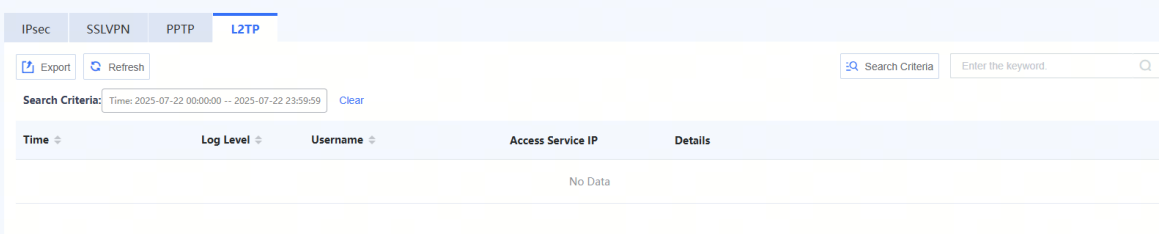
Application Scenario

L2TP logs record important events and exceptions occurring during the L2TP tunnel running. They help administrators understand the L2TP tunnel running status and locate and solve exceptions of the L2TP VPN function.

Procedure

(1) Choose **O&M > Logs > VPN Log** > **L2TP**.

(2) This page displays L2TP log information.



Field	Description
Time	Time when a log is recorded.
Log Level	The importance level of log. Logs are classified into four levels in descending order of importance: informational, low, medium, and high.
Username	Username for accessing an L2TP server.
Access Service IP	Actual IP address of the peer end (L2TP client) of the tunnel.
Details	Log content.

Note

You can set query criteria such as the log record date, log level, and access service IP address. The web UI displays only the logs that meet the query criteria.

Follow-up Procedure

- Click **Export** to export logs to an Excel file locally for reading and query.
- Click **Refresh** to obtain the latest logs.

11. Querying High Availability Logs

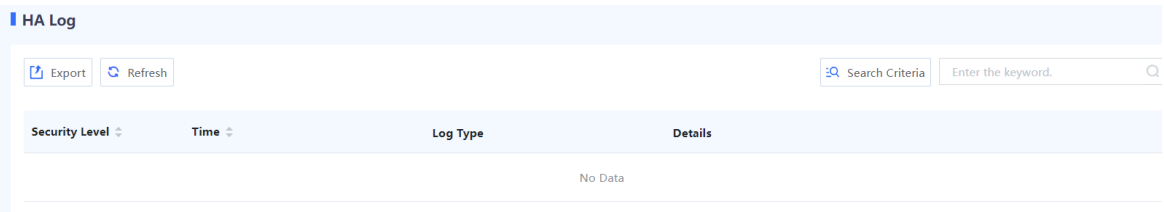
Application Scenario

By viewing high availability logs, an administrator can learn about the running status of high availability functions.

Procedure

(1) Choose **O&M** > **Logs** > **HA Log**.

(2) Information related to high availability logs is displayed on the web UI.



Note

You can set **Search Criteria** to specify the time range, security, and log type.

Follow-up Procedure

- Click **Export** to export the latest logs (no more than 10,000 logs) in the current list to an Excel file on the local device for convenient reading and query.
- Click **Refresh** to obtain the latest high availability logs.

12. 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.

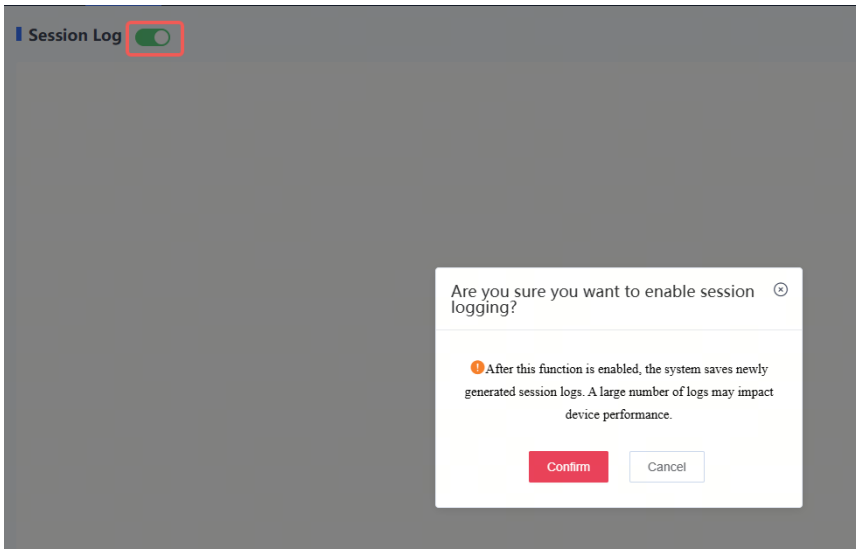
Procedure

(1) Choose **O&M** > **Logs** > **Session Log**.

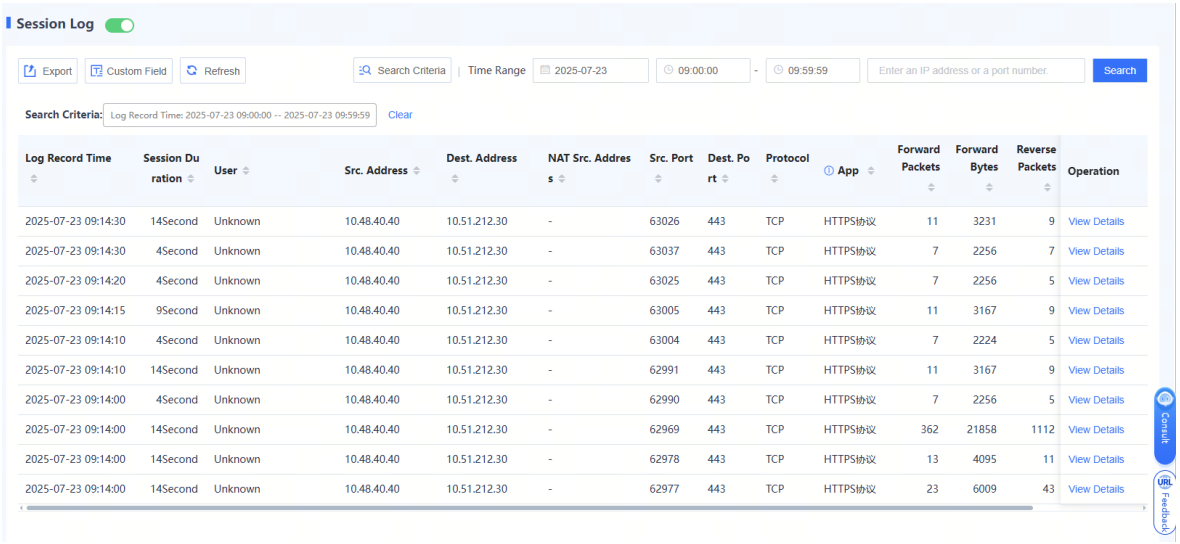
(2) Toggle on tp enable session log monitoring.

Caution

Session log monitoring is disabled by default. After this function is enabled, the system saves new session logs. A large number of logs may affect device performance. If this function is disabled, the system stops saving new session logs. Determine whether to enable this function as required.



(3) When session log monitoring is enabled, the session log-related information is displayed on the web page.

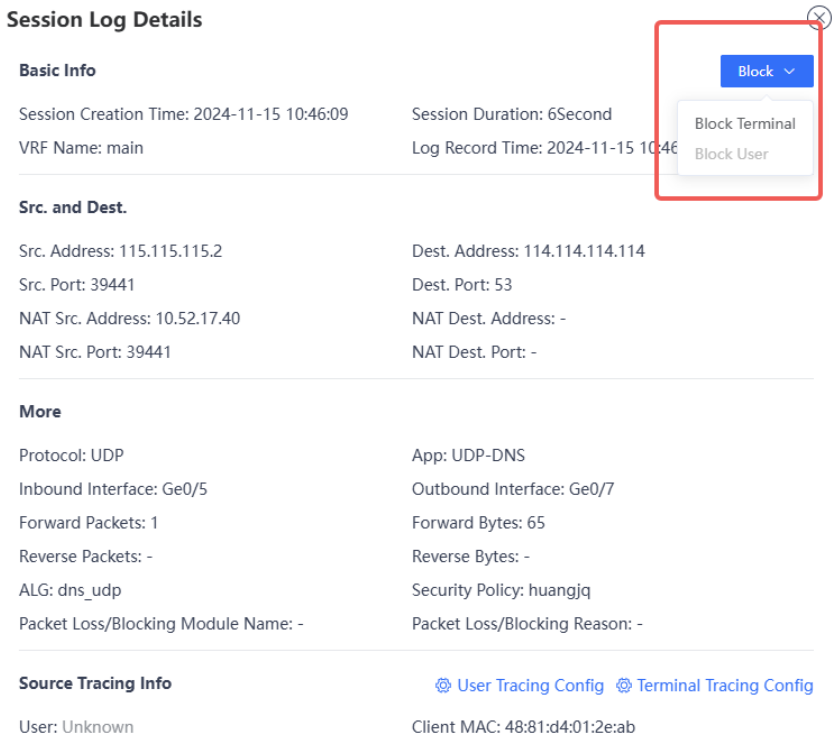


Note

You can click **Search Criteria** to set the keywords for log query. Only session logs matching the search criteria are displayed on the page.

Follow-up Procedure

- Click **Export** to export session logs to the local device in the Excel format, facilitating subsequent query.
- Click **Custom Field** to set the fields to be displayed on the page.
- Click **Refresh** to obtain the latest session logs.
- Enter the source/destination IP address or source/destination port number in the search box in the upper right corner, and click **Search** to quickly query session logs.
- Click **View Details** in the **Operation** column to query log details. On the **Session Log Details** page, click **Block User** or **Block Terminal** to add a user or terminal to the user or MAC address blocklist. When the user name is empty, that is, **User** is displayed as **Unknown**, the **Block User** button is unavailable. When the MAC address of a terminal is empty, that is, **Client MAC** is displayed as **Unknown**, the **Block Terminal** button is unavailable.



13. Querying DHCP Logs

Application Scenario

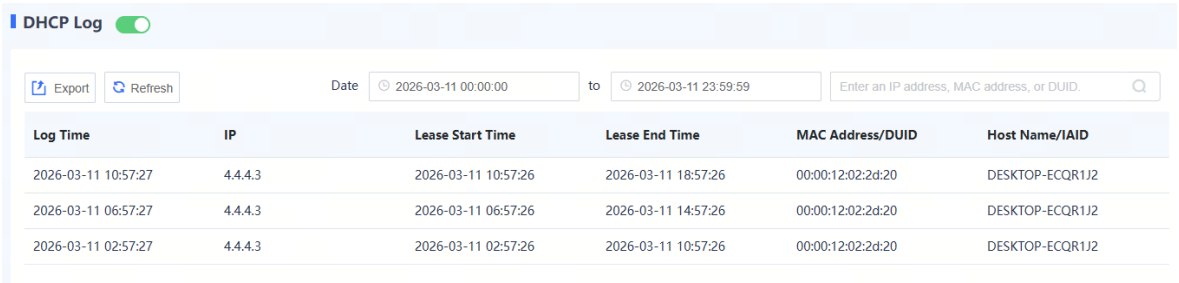
You can query DHCP logs to master allocation of IP addresses in the address pool.

Procedure

(1) Choose **O&M** > **Logs** > **DHCP Log**.

(2) Information about DHCP logs is displayed on the web UI.

(3) Set query criteria such as the log time, IP address, and MAC address to filter out logs matching the query criteria.



Follow-up Procedure

- Click **Export** to export DHCP logs to the local device in the Excel format, facilitating subsequent query.
- Click **Refresh** to obtain the latest logs.

8.4 Network

8.4.1 Traffic Monitoring

1. Interface Traffic

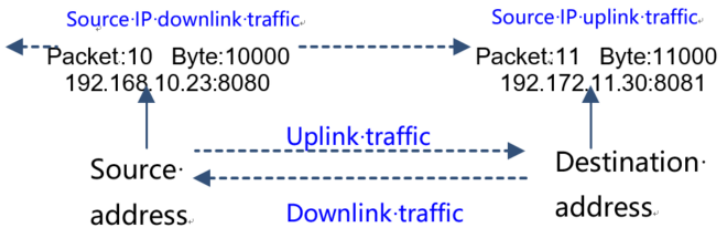
Application Scenario

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.

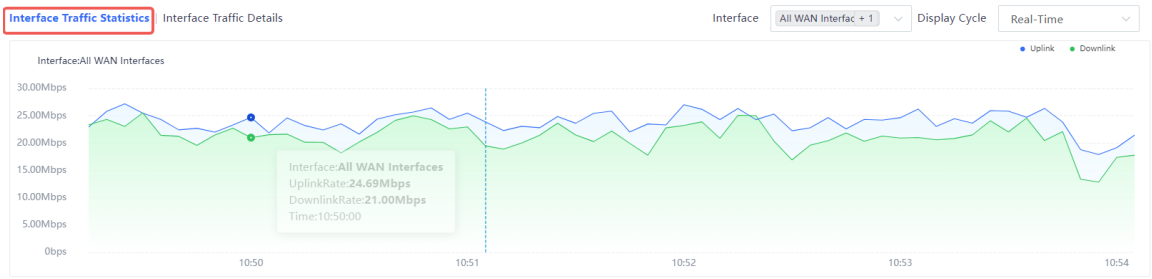
  The following figure shows the uplink traffic and downlink traffic:



Procedure

(1) Choose **O&M** > **Network** > **Traffic** > **Interface Traffic**.

(2) Click **Interface Traffic Statistics** Select the interface to be queried and set the query cycle. The system displays the interface traffic trend chart, including the uplink traffic and downlink traffic. By selecting different display periods, you can view interface traffic statistics in real time, last 24 hours, last 7 days, or last 30 days.



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



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.

2. Real-Time Traffic

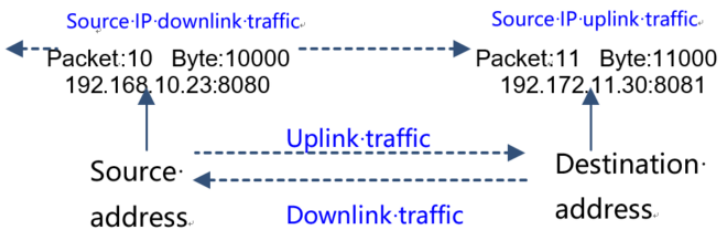
Application Scenario

The real-time flow analysis function is used to display the real-time distribution of network traffic. The device collects traffic information in real time and performs analysis based on dimensions such as lines, applications, and terminals. It helps administrators quickly understand the traffic distribution situation and manage egress lines and intranets through visual statistical graphs.

Background

- Uplink traffic: traffic transmitted from the interface.
- Downlink traffic: traffic received by the interface.

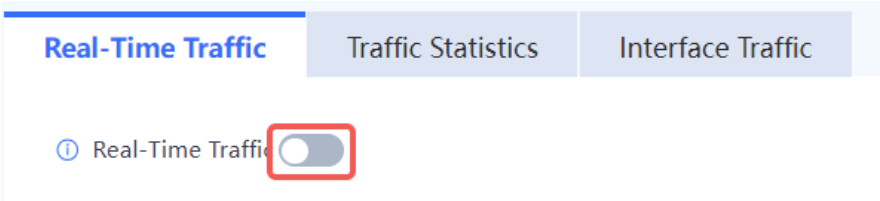
  The following figure shows the uplink traffic and downlink traffic:



Procedure

(1) Choose **O&M** > **Network** > **Traffic** > **Real-Time Traffic**.

(2) Toggle on to enable real-time traffic statistics.



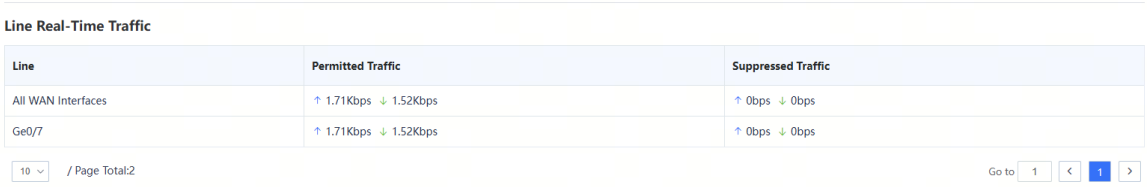
Note

The real-time flow analysis function takes effect only on the traffic generated after this function is enabled.

Follow-up Procedure

The **Real-Time Traffic** page displays the following information:

- Line Real-Time Traffic: Displays the real-time total uplink and downlink traffic of each egress line, including the traffic passing through the line and the suppressed traffic.



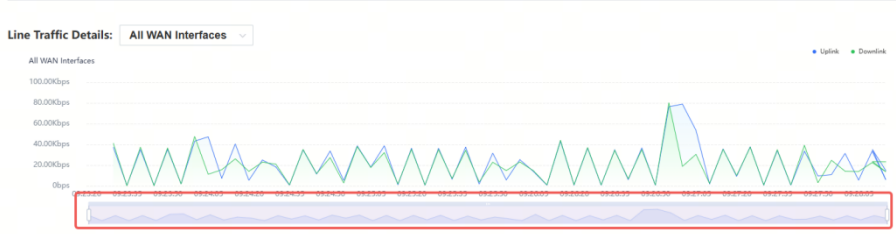
- Line Traffic Details: Select a port in the upper left drop-down list to specify the port for traffic display. By default, traffic of all WAN ports is displayed.
  - Real-time traffic trend: The real-time traffic trend within the last 5 minutes is displayed by default. If a hard disk is installed on the device, data within the last 5 minutes, last 24 hours, and last 7 days can be viewed, and the traffic is collected by source IP address, application, or user.

    Hover the cursor over a data point to display the detailed data at the corresponding time point. Click the data point to view the traffic ranking list at that moment.

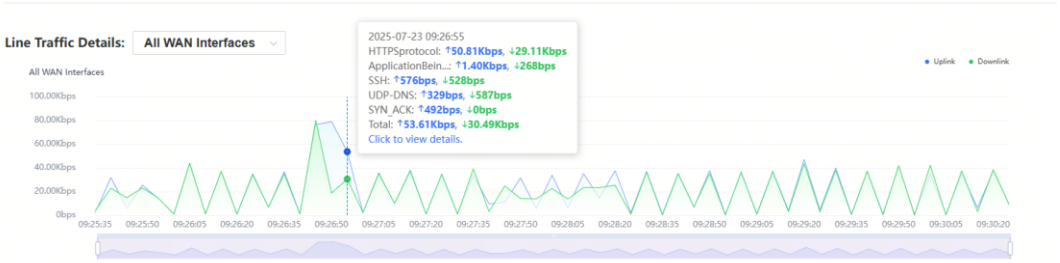


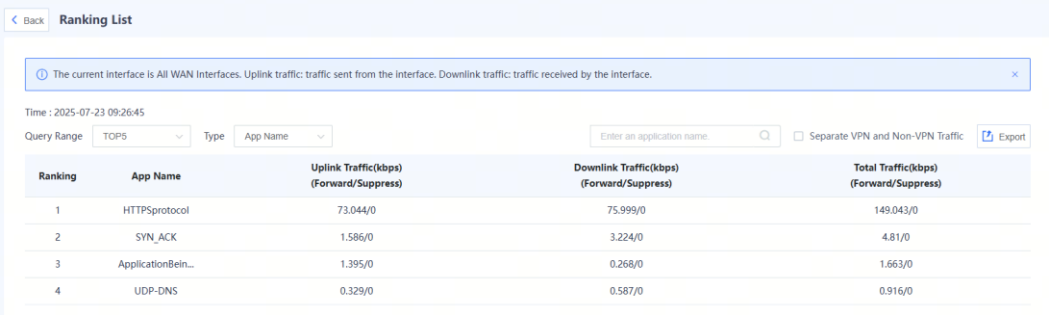
Note

- You can move the cursor over the horizontal coordinate to view traffic trends in different periods of time.

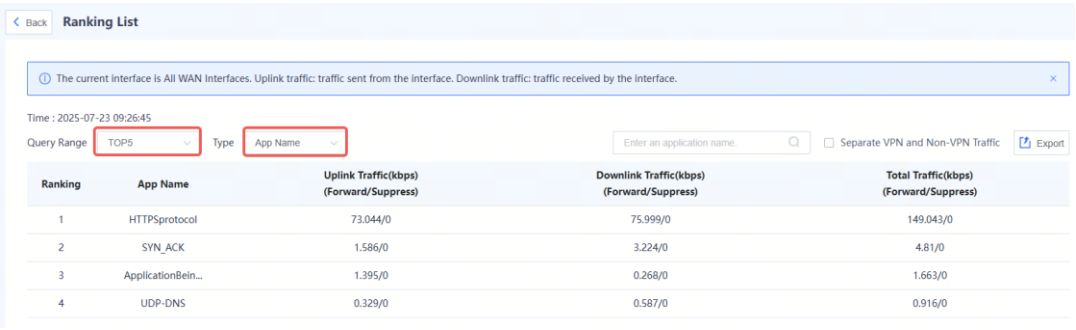


- If no hard disk is installed on the device, traffic data can be viewed only in the last 5 minutes.





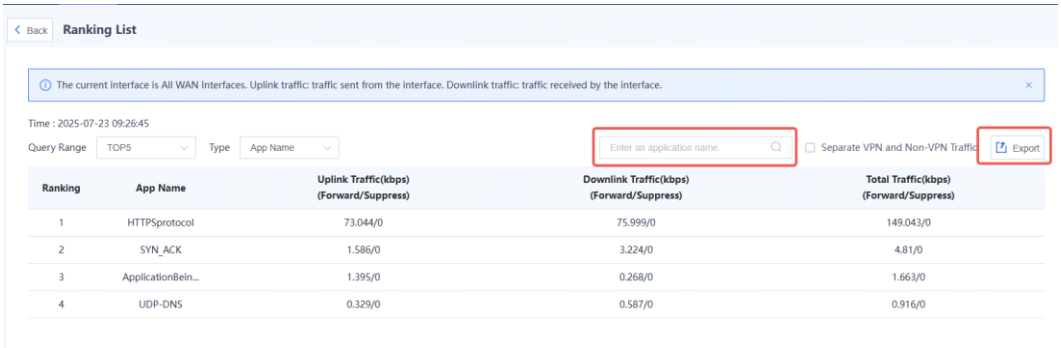
On the **Ranking List** page, you can set the ranking scope and statistics dimensions (based on the source IP address, application name, or username) for traffic data.



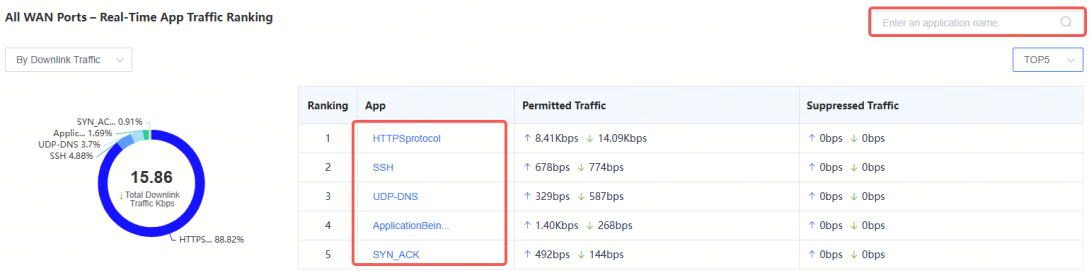
If you select **Separate VPN and Non-VPN Traffic**, VPN traffic statistics and non-VPN traffic statistics are collected separately.



Enter the application name, source IP address, or username in the search box to query traffic details of a specified object. Click **Export** to export the ranking list to the local PC.

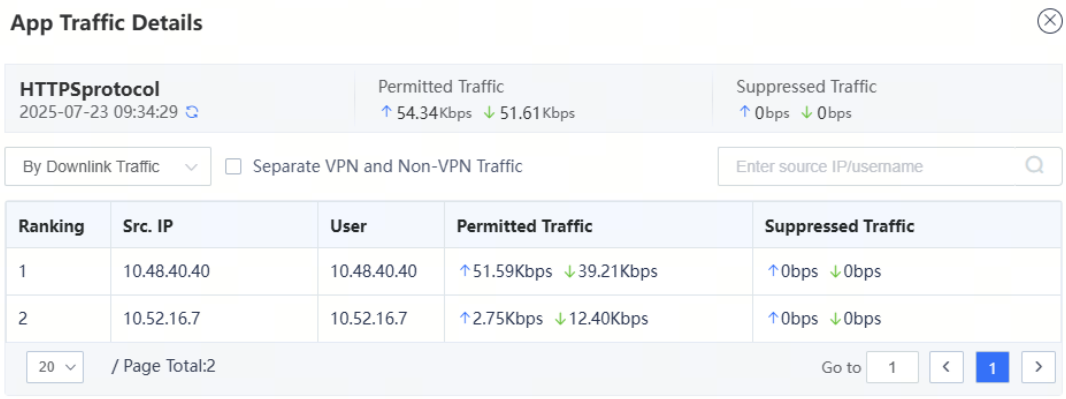


- App Traffic Ranking: This function visualizes real-time traffic data by application, helping administrators understand traffic usage and allocate bandwidth resources appropriately. You can collect statistics based on uplink, downlink, or total traffic, and query top 50 applications by traffic and their traffic data.

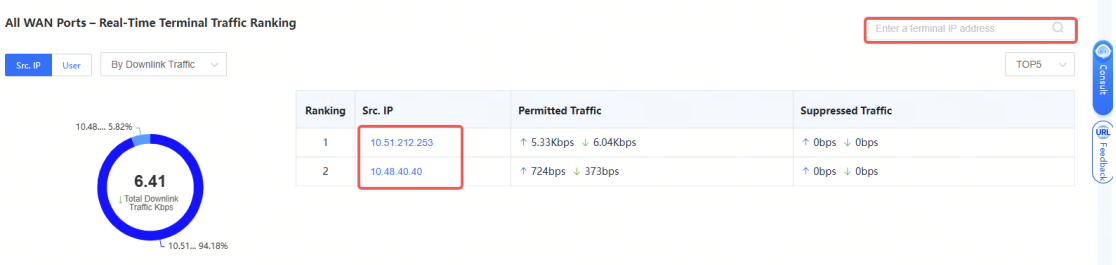


Click an application name in the **Real-Time App Traffic Ranking** section, or enter an application name in the search box to view traffic details snapshot of the application, which displays detailed source IP address/user information of the current application.

Click  to obtain the latest traffic snapshot. If you select **Separate VPN and Non-VPN Traffic**, VPN traffic statistics and non-VPN traffic statistics are collected separately.

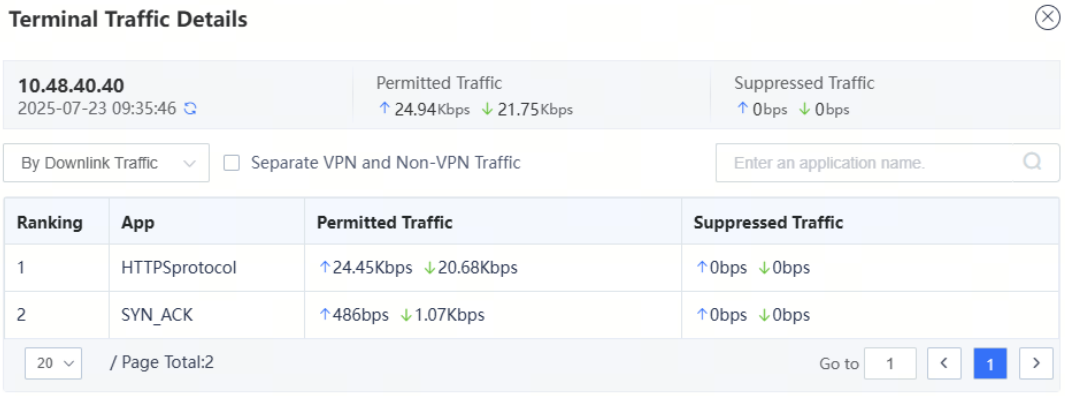


- Real-Time Terminal Traffic Ranking: This function visualizes real-time traffic data of a line based on the source IP address or username, helping administrators understand traffic usage and allocate bandwidth resources appropriately. You can query top 50 source IP addresses/users by uplink traffic, downlink traffic, or total traffic, and view traffic details of the source IP addresses/users.



Click a source IP address or user in the **Real-Time Terminal Traffic Ranking** section, or enter a terminal IP address in the search box to view terminal traffic snapshots and detailed application information of the terminal.

Click to obtain the latest traffic snapshot. If you select **Separate VPN and Non-VPN Traffic**, VPN traffic statistics and non-VPN traffic statistics are collected separately.



3. Traffic Statistics

Application Scenario

Enable this function to display the distribution of historical uplink and downlink traffic on the device.

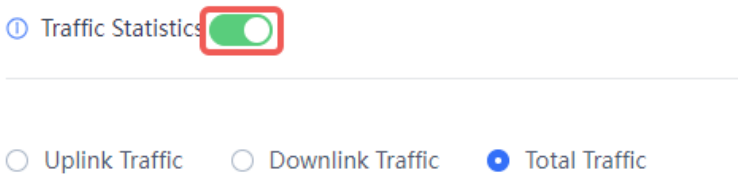
Precautions

- If no hard disk is installed, only traffic statistics in the last 1 hour can be displayed. If a hard disk is installed, you can specify a time range for querying the traffic statistics of the device.

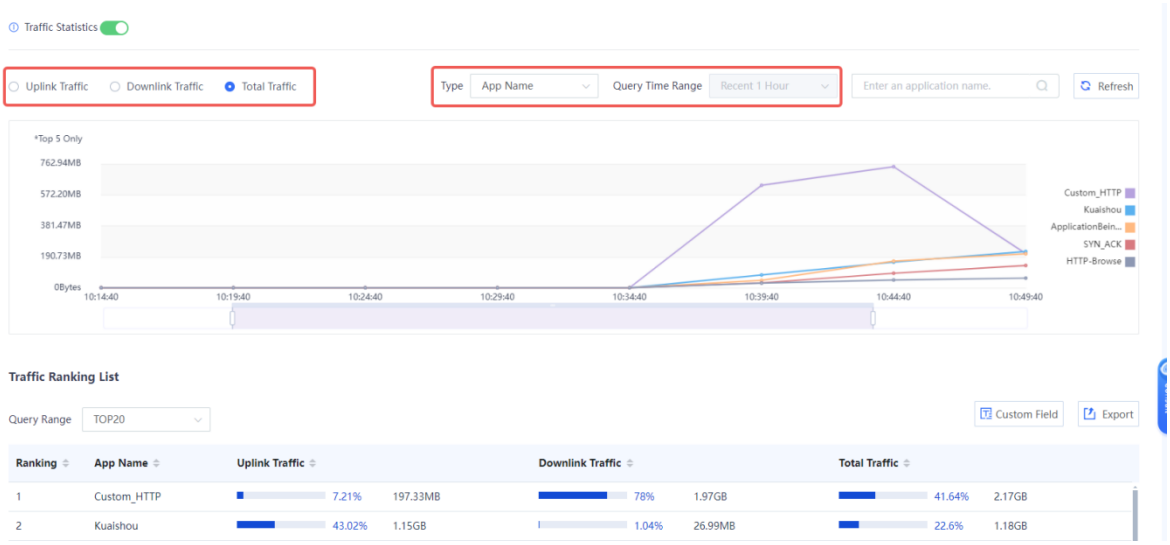
Procedure

(1) Choose **O&M** > **Network** > **Traffic** > **Traffic Statistics**.

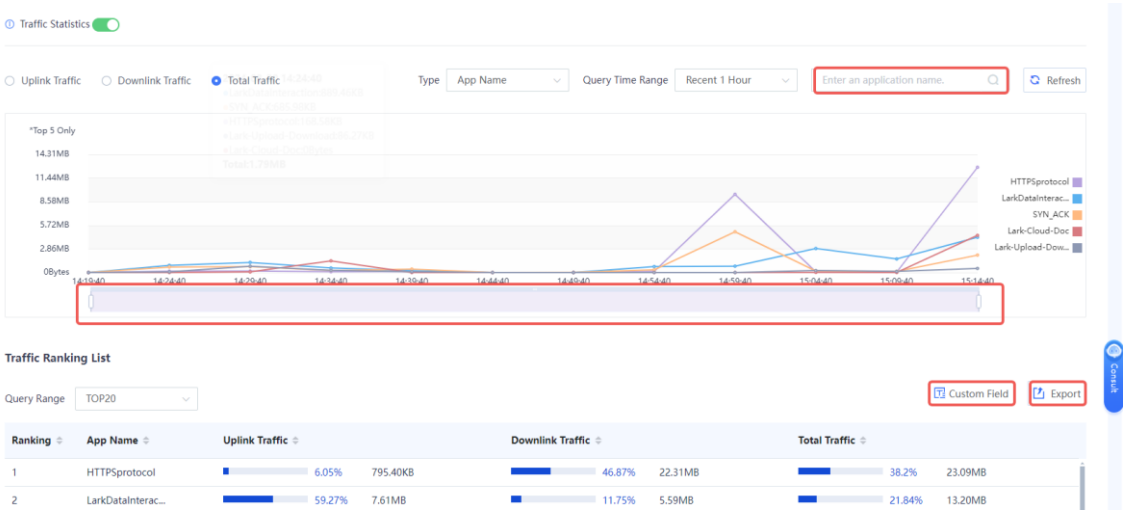
(2) Toggle on to enable traffic statistics.



(3) Set search criteria to view information about specific traffic.



Follow-up Procedure



- Enter an application name, source IP address, or username in the search box to query the traffic details about a specified object.
- On the device, you can change the horizontal coordinate of a traffic chart to view the traffic trend in different periods of time.
- Click **Export** to export the traffic ranking list and save it locally.
- Click **Custom Field** and set the fields to be displayed on the page.

8.4.2 Session Monitoring

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.

2. Real-Time Session

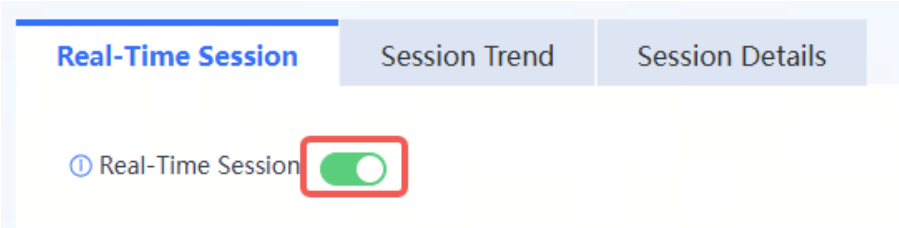
Application Scenario

The real-time session function is used to display real-time session data of a line. The device collects real-time session information and performs analysis based on the line, application, and terminal dimensions. It helps administrators quickly understand the session usage and manage egress lines based on visual statistical graphs.

Procedure

(1) Choose **O&M** > **Network** > **Session** > **Real-Time Session**.

(2) Toggle on to enable the real-time session statistics collection function.



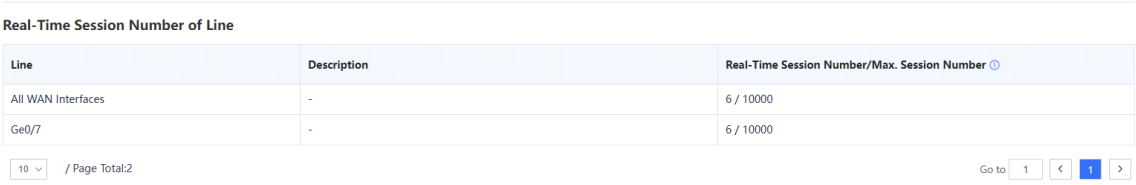
Note

The real-time session function records analysis information only for sessions established after this function is enabled. Sessions established before this function is enabled are not analyzed.

Follow-up Procedure

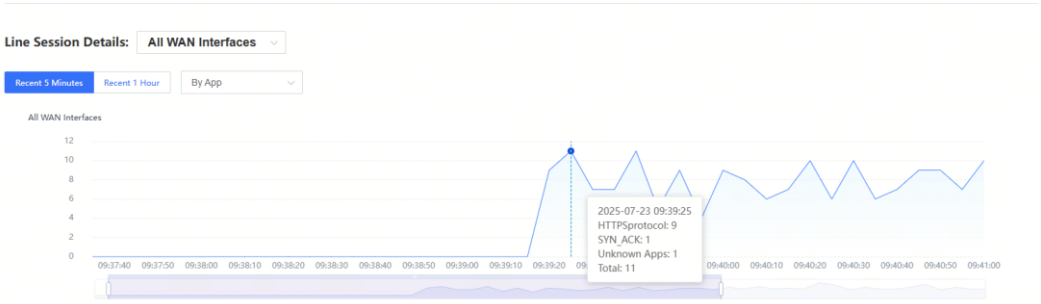
The **Real-Time Session** page displays the following information:

- Real-Time Session Number of Line: displays the maximum number of uplink/downlink sessions supported and the number of real-time sessions of each egress line.



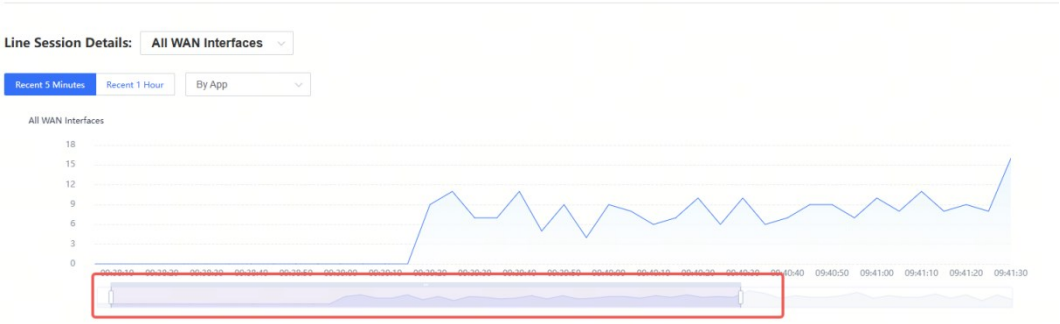
- Line Session Details: Select the port in the upper left drop-down list to specify the port for viewing details. By default, the statistics of all WAN ports are collected.
  - Real-time session trend: shows the real-time session change trend in the last 5 minutes by source IP address, application, or user. If no hard disk is installed on the device, you can view the data in the last 5 minutes and last 1 hour. If a hard disk is installed on the device, you can view the data in the last 24 hours and last 7 days.

    Hover the cursor over a data point to display the detailed data at the corresponding time point.

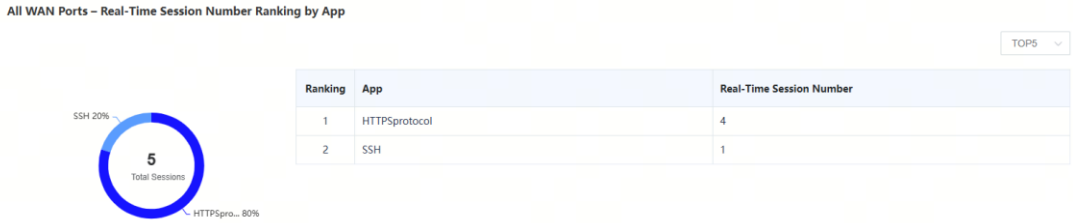


Note

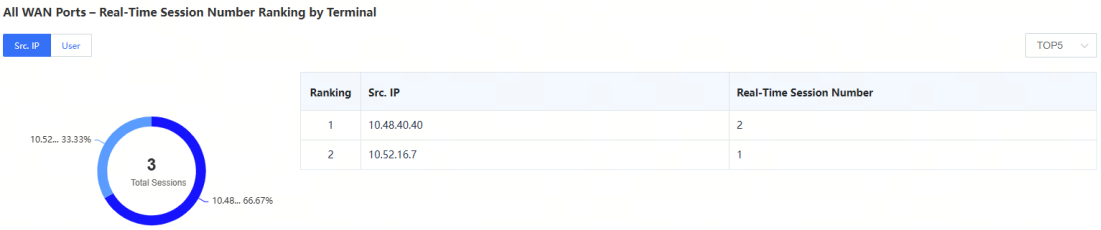
You can hover the cursor over the horizontal coordinate to view session data in different time ranges.



- Real-Time Session Number Ranking by App: This function visualizes real-time session rankings by application, helping administrators understand the distribution of sessions and adjust session control policies. You can query top 50 applications by real-time session numbers and their session data.



- Real-Time Session Number Ranking by Terminal: Based on the source IP address or username, this function visualizes real-time session ranking by line to help administrators understand the distribution of sessions and adjust session control policies. You can query top 50 source IP addresses/users and their session data based on the number of sessions.



3. Session Change Trend

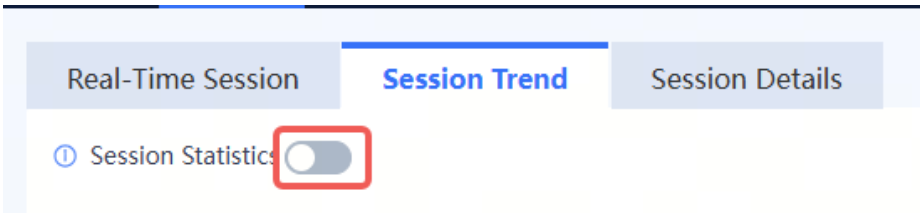
Application Scenario

The session change trend function supports real-time monitoring and visualization of the changes in new sessions and concurrent sessions (including average and peak values of new session rates and numbers of concurrent sessions) within a specified time period.

Procedure

(1) Choose **O&M** > **Network** > **Session** > **Session Trend**.

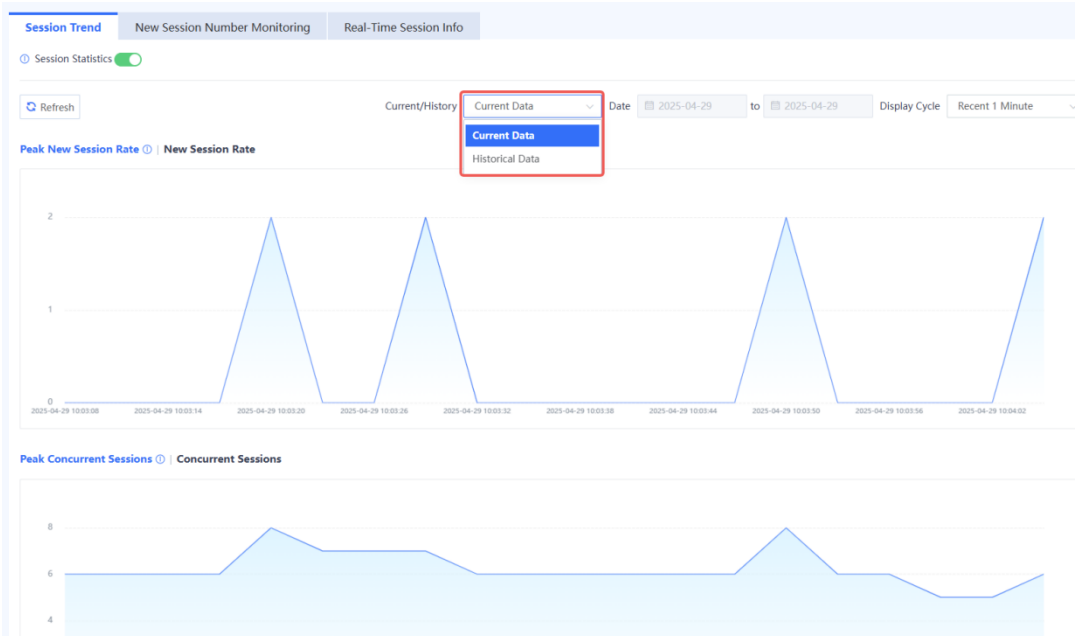
(2) Toggle on **Session Statistics**.



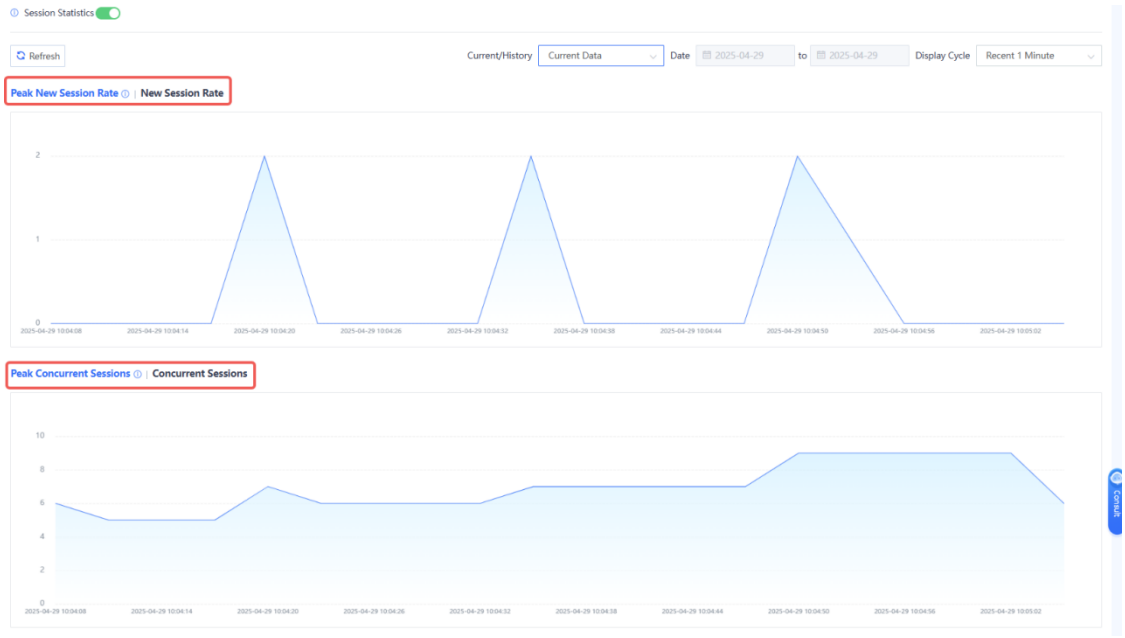
(3) In the dialog box that is displayed, click **OK**.

(4) 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.



(5) Click the link in the upper left corner of a chart to display peak or average statistics on sessions.



4. Session Detalis

Application Scenario

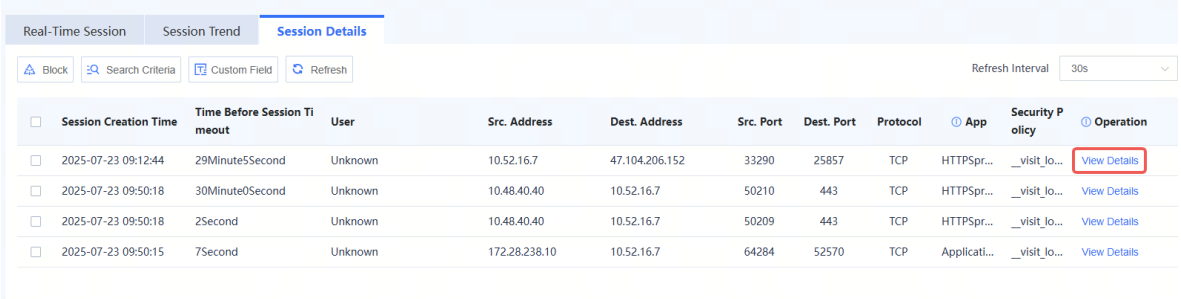
The session details function is used to collect and display the current number of sessions. You can block a session based on service needs. After a session is blocked, the firewall discards subsequent packets transmitted over this session and the session is no longer displayed on the page. In addition, the device can block users or terminals based on session details.

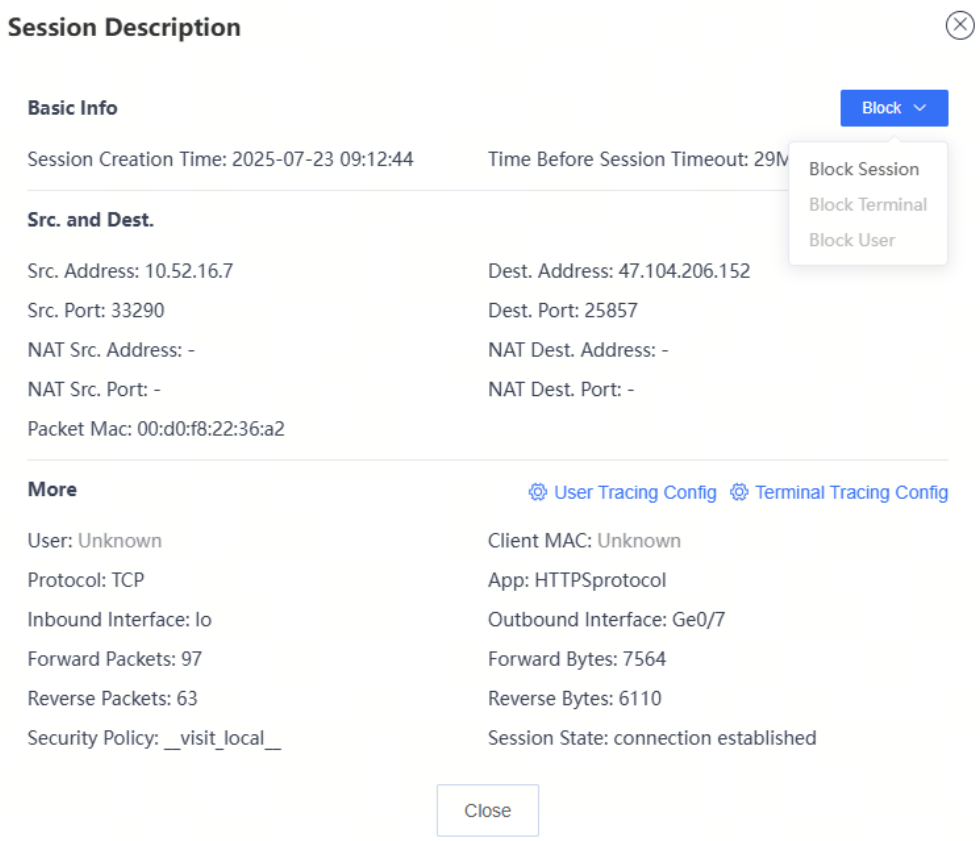
Procedure

(1) Choose **O&M** > **Network** > **Session** > **Session Details**.

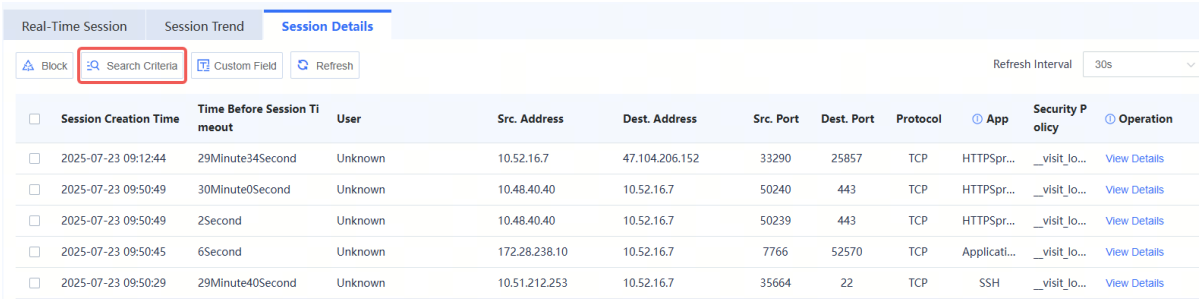
(2) Select the desired session and click **View Details** to view the session creation time, hit security policy, number of forward packets, and number of reverse packets.

On the **Session Description** page, you can block sessions, users, or terminals as required. When the username or terminal MAC address is unknown, **Block User** and **Block Terminal** buttons are unavailable. You can configure real-name user information reception and terminal MAC address identification to obtain the username and terminal's MAC address. For details on how to configure real-name user information reception and terminal MAC address identification, see 7.3.1 Identity System Association and 7.3.2 Network Device Association.

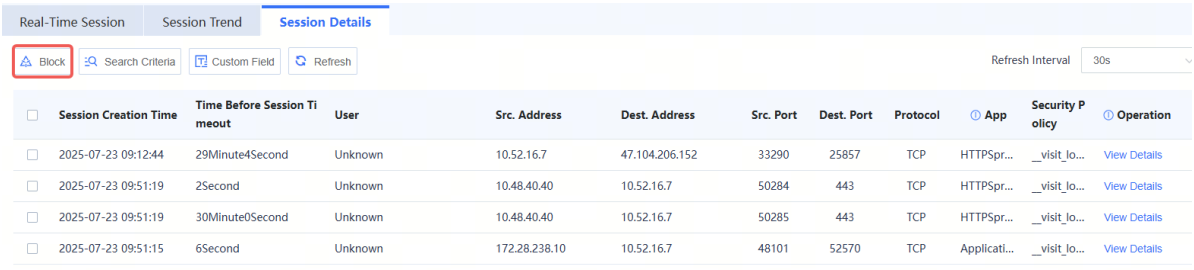




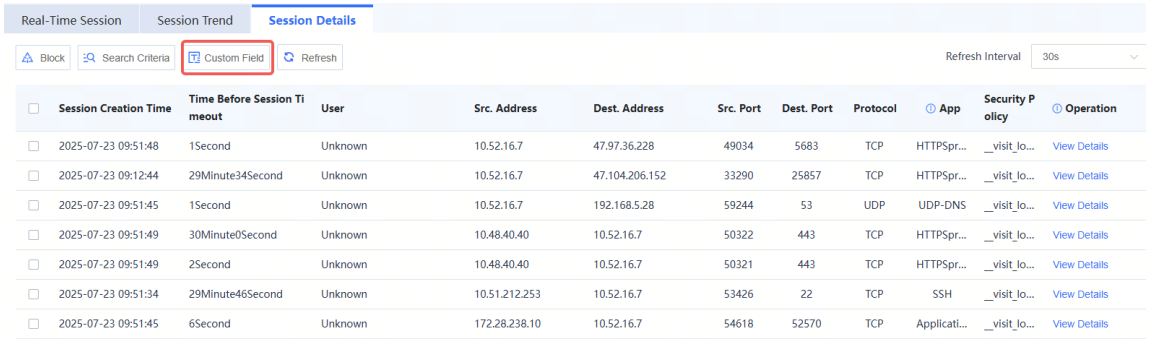
(3) (Optional) Click **Search Criteria** to set the criteria for filtering sessions.



(4) (Optional) Select one or more sessions and click **Block** to block the selected sessions.



(5) (Optional) Click **Custom Field** to set the session fields to be displayed on the page.



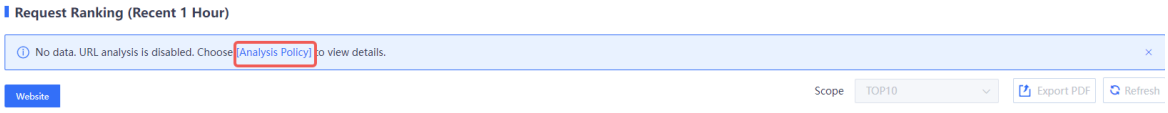
Session Creation Time	Time Before Session Timeout	User	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Security Policy	Operation
2025-07-23 09:51:48	1Second	Unknown	10.52.16.7	47.97.36.228	49034	5683	TCP	HTTPSpr...	_visit_lo...	View Details
2025-07-23 09:12:44	29Minute34Second	Unknown	10.52.16.7	47.104.206.152	33290	25857	TCP	HTTPSpr...	_visit_lo...	View Details
2025-07-23 09:51:45	1Second	Unknown	10.52.16.7	192.168.5.28	59244	53	UDP	UDP-DNS	_visit_lo...	View Details
2025-07-23 09:51:49	30Minute0Second	Unknown	10.48.40.40	10.52.16.7	50322	443	TCP	HTTPSpr...	_visit_lo...	View Details
2025-07-23 09:51:49	2Second	Unknown	10.48.40.40	10.52.16.7	50321	443	TCP	HTTPSpr...	_visit_lo...	View Details
2025-07-23 09:51:34	29Minute46Second	Unknown	10.51.212.253	10.52.16.7	53426	22	TCP	SSH	_visit_lo...	View Details
2025-07-23 09:51:45	6Second	Unknown	172.28.238.10	10.52.16.7	54618	52570	TCP	Applicati...	_visit_lo...	View Details

8.4.3 URL Ranking

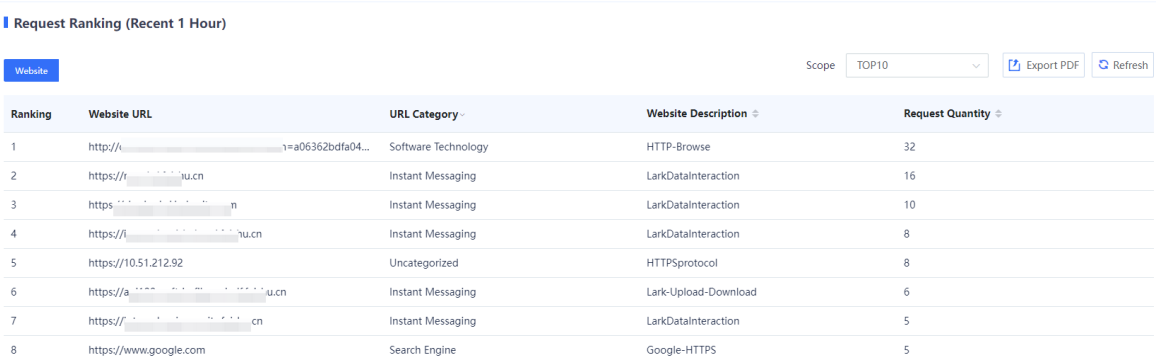
Procedure

(1) Choose **O&M** > **Network** >**URL Ranking**.

URL audit is disabled by default. URL audit data is displayed only after URL audit is enabled.



(2) The system displays top website requests in the last 1 hour.



Ranking	Website URL	URL Category	Website Description	Request Quantity
1	http://...=a06362bdfa04...	Software Technology	HTTP-Browse	32
2	https://...u.cn	Instant Messaging	LarkDataInteraction	16
3	https...n	Instant Messaging	LarkDataInteraction	10
4	https://...u.cn	Instant Messaging	LarkDataInteraction	8
5	https://10.51.212.92	Uncategorized	HTTPSprotocol	8
6	https://a...u.cn	Instant Messaging	Lark-Upload-Download	6
7	https://...cn	Instant Messaging	LarkDataInteraction	5
8	https://www.google.com	Search Engine	Google-HTTPS	5

Follow-up Procedure

- You can set **Scope** to view traffic data in a specified range.
- Click **Export PDF** to export website request statistics collected in nearly one hour to a PDF file on the local device for convenient reading and query later.
- Click **Refresh** to view the latest request ranking.

8.5 Device Hardware Monitoring

Application Scenario

You can perform this operation to monitor the CPU usage, memory usage, and hard disk usage of the firewall and process exceptions in a timely manner.

You can set the display cycle to recent 1 hour, recent 24 hours, or recent 7 days. The system displays historical data about the CPU usage, memory usage, and hard disk usage based on the configured display cycle.

Procedure

(1) Choose **O&M** > **Device** > **Device Hardware**.

(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.

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

Note

The hard disk usage is displayed only when a hard disk is installed on the device.

The usage of the built-in storage (eMMC) is displayed only for RG-CF10S, RG-CF10S-LTE, and RG-CF30XS.



Follow-up Procedure

Item	Description
CPU Usage	In normal cases, the CPU usage should be lower than 80%. If the CPU usage is too high for a long time, check the device and analyze the causes. The possible causes for high CPU usage are as follows: App protection or DDoS protection is enabled. Too many connections are created, many of which are initiated by attackers.
Memory Usage	In normal cases, the memory usage should be lower than 80%. If the memory usage is too high for a long time, check the device and analyze the causes.
Hard Disk Usage	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.
Built-in Storage (eMMC)	In normal cases, the usage of the built-in storage (eMMC) should be lower than 90%. If the remaining eMMC space is too small for a long time, check the device and clear the eMMC space.

8.6 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.

8.6.1 Diagnostic Center

1. Network Connectivity Diagnosis

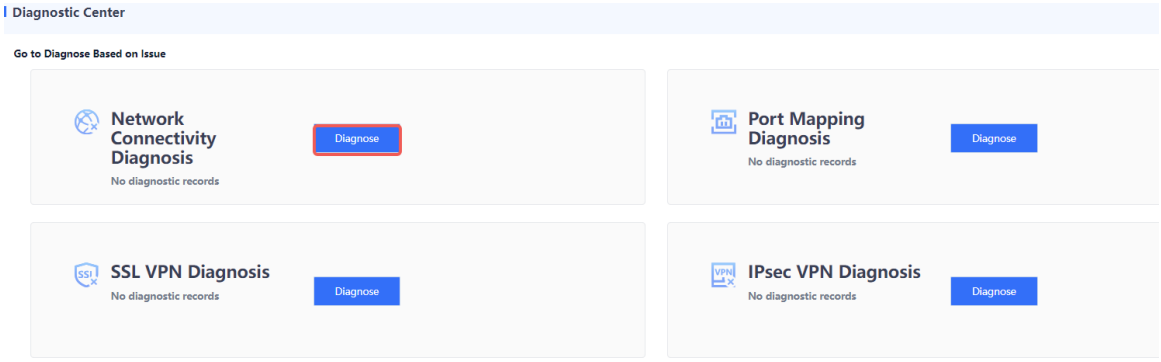
Application Scenario

The network connectivity 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.

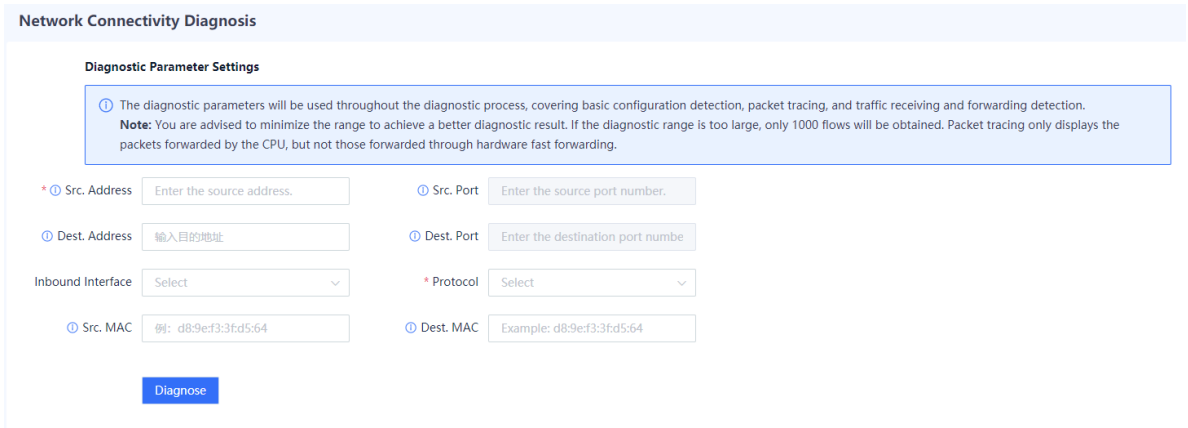
Procedure

(1) Choose **O&M** > **Fault Diagnosis** > **Diagnostic Center**.

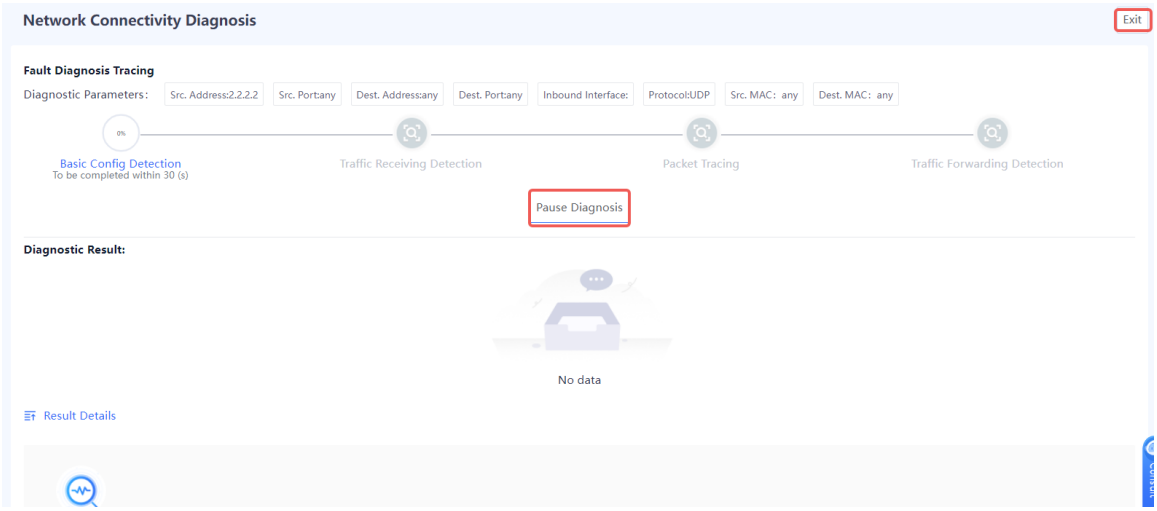
(2) Click **Diagnose**.



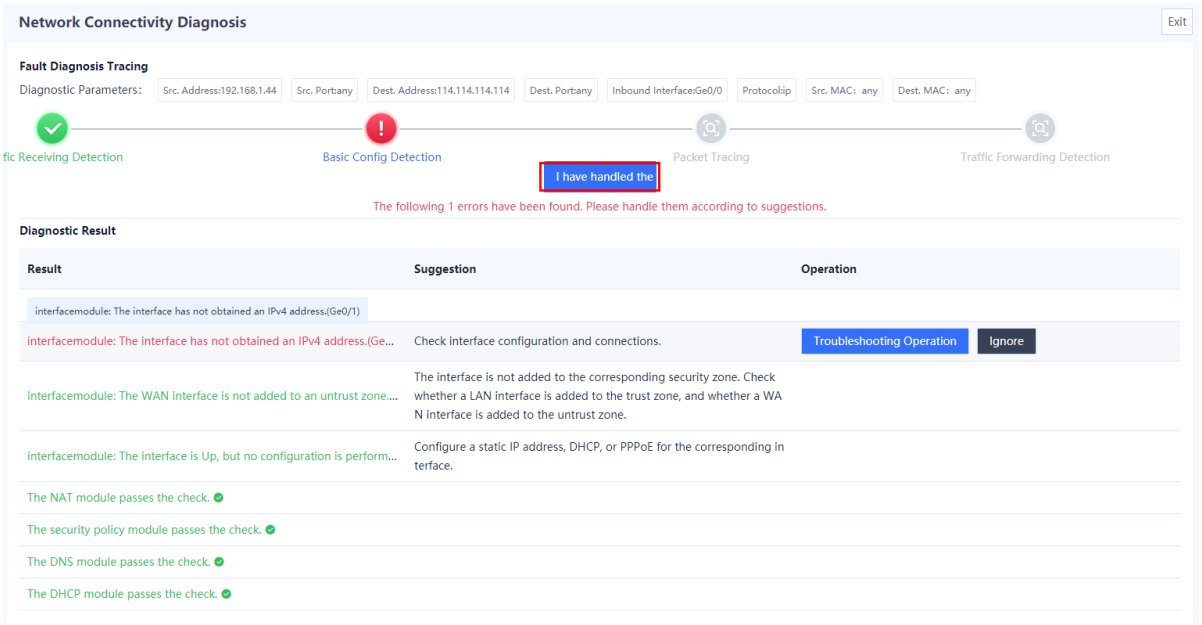
(3) Enter the source/destination IP address, source/destination port, source/destination MAC address, inbound interface, and protocol, and click **Diagnose**. The firewall checks the network connectivity between the specified source and destination IP addresses.



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

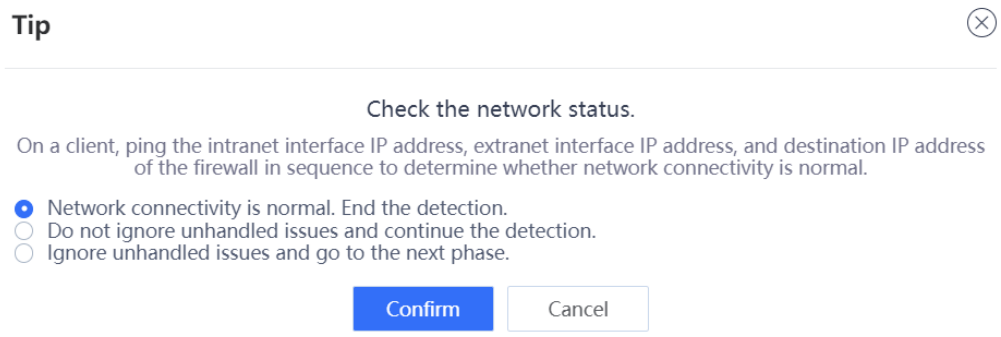


(5) After the diagnosis is complete, the diagnostic result and diagnostic details are displayed in the lower part of the page. After you troubleshoot the fault based on the diagnostic details, click **I have handled the problem**.



(6) Click the content in the displayed dialog box to end or continue the detection.

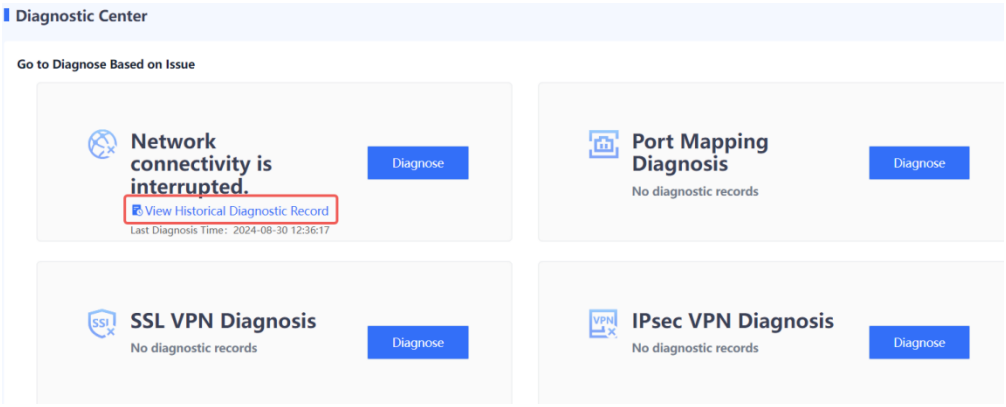
- Click **Network connectivity is normal. End the detection.** to end detection and exit diagnostics.
- Click **Do not ignore unhandled issues and continue the detection.** to restart detection in this phase.
- Click **Ignore unhandled issues and go to the next phase.** to skip detection in this phase and enter the next phase.



(7) Repeat steps 5 and 6 until all the items are checked.

Follow-up Procedure

Click **View Historical Diagnostic Record** to view and download historical diagnostic records.



2. Port Mapping Exception Diagnostics

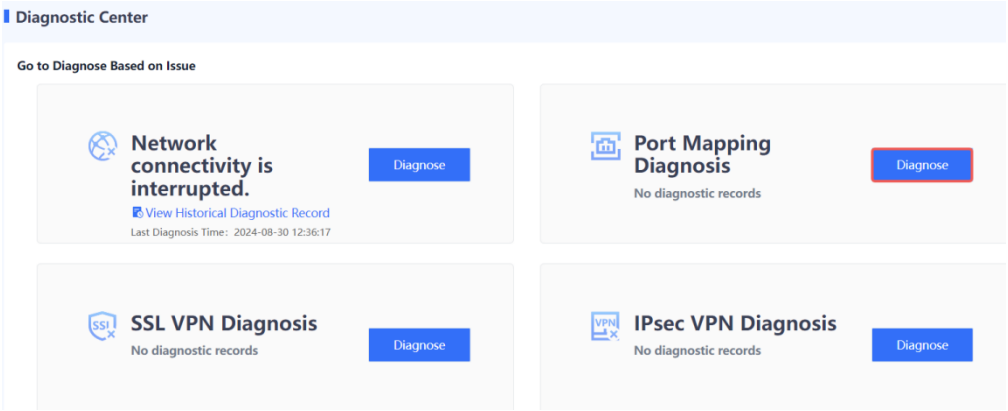
Application Scenario

When port mapping takes ineffective or the destination address fails to be translated using NAT, you can use the port mapping exception diagnosis function to locate the fault with one click.

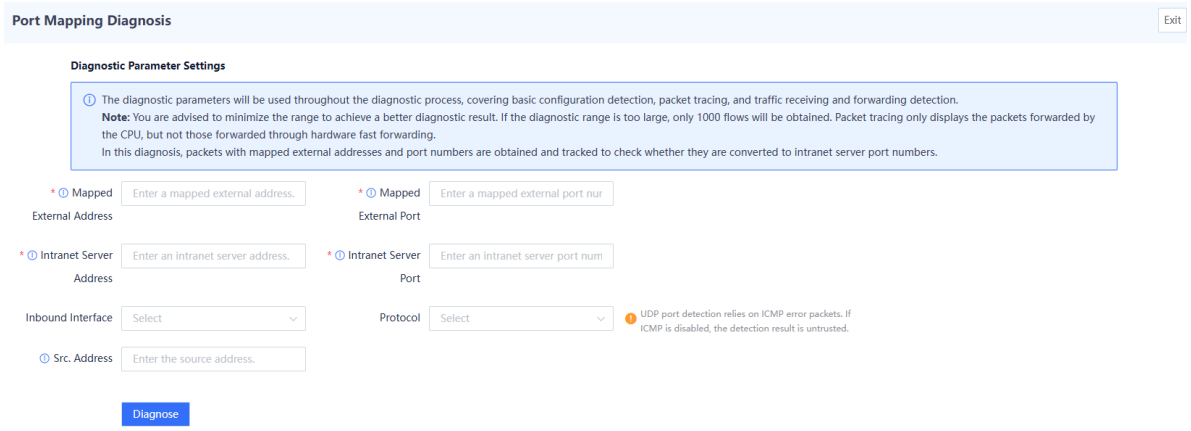
Procedure

(1) Choose **O&M** > **Fault Diagnosis** > **Diagnostic Center**.

(2) Click **Diagnose**.



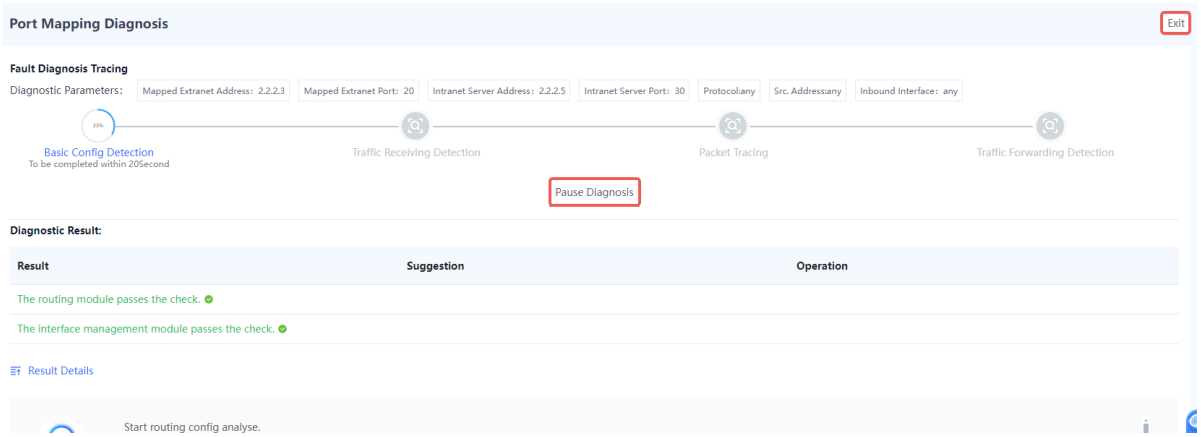
(3) Set diagnosis parameters and click **Diagnose**. Then the device will check the port mapping between the intranet and external network.



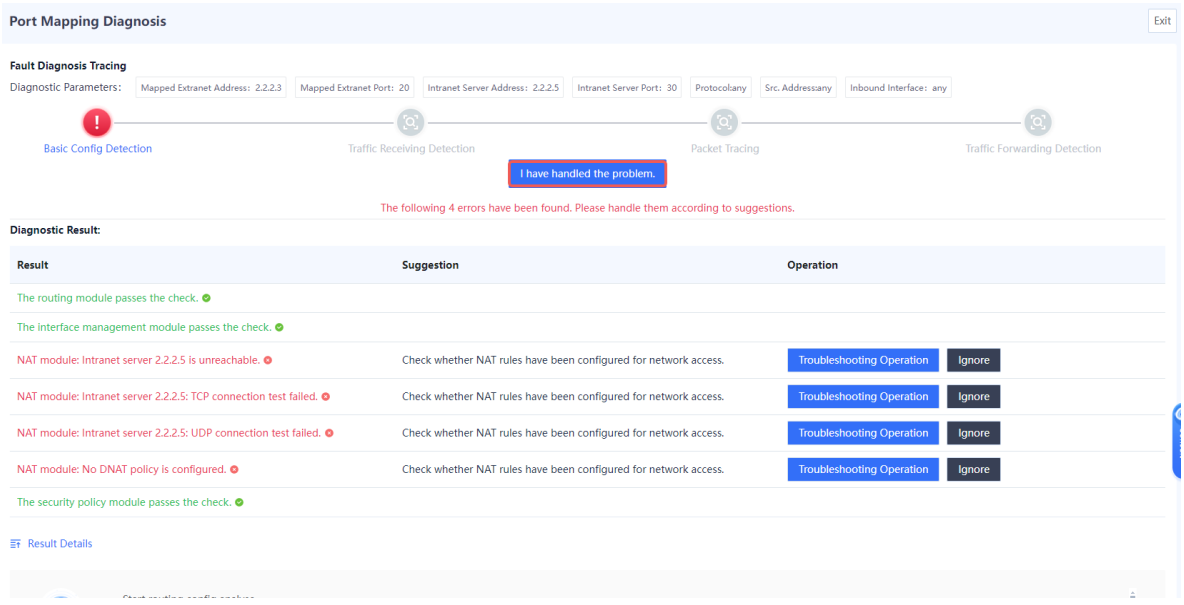
Item	Description	Remarks
Mapped External Address	External IP address for port mapping.	Only a single IPv4 address is supported. [Example] 192.168.1.1
Mapped External Port	External port for mapping.	Only a single interface is supported. [Example] 80
Intranet Server Address	IP address of the internal server for port mapping.	Only a single IPv4 address is supported. [Example] 192.168.1.2
Intranet Server Port	Port of the internal server for mapping.	Only a single interface is supported. [Example] 81
Inbound Interface	Inbound interface of traffic from an external network to an intranet server.	Select a value from the drop-down list box.
Protocol	Protocol type used for traffic access to the internal network server, which can be TCP or UDP.	Select a value from the drop-down list box. [Example] TCP

Item	Description	Remarks
Src. Address	Source address of traffic destined for the intranet server.	Only a single IPv4 address is supported. [Example] 192.168.1.3

(4) (Optional) You can end the diagnosis task at any time during detection.



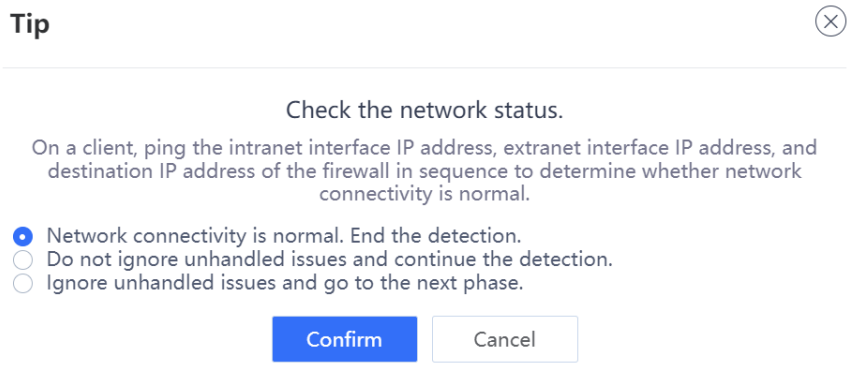
(5) After diagnosis is complete, the diagnosis results and details will be displayed below. After troubleshooting the fault according to the diagnosis details, click **I have handled the problem**.



(6) Click the content in the displayed dialog box to end or continue detection.

- Click **Network connectivity is normal. End the detection.** to end detection and exit diagnostics.
- Click **Do not ignore unhandled issues and continue the detection.** to restart detection in this phase.
- Click **Ignore unhandled issues and go to the next phase.** to skip detection in this phase and enter the

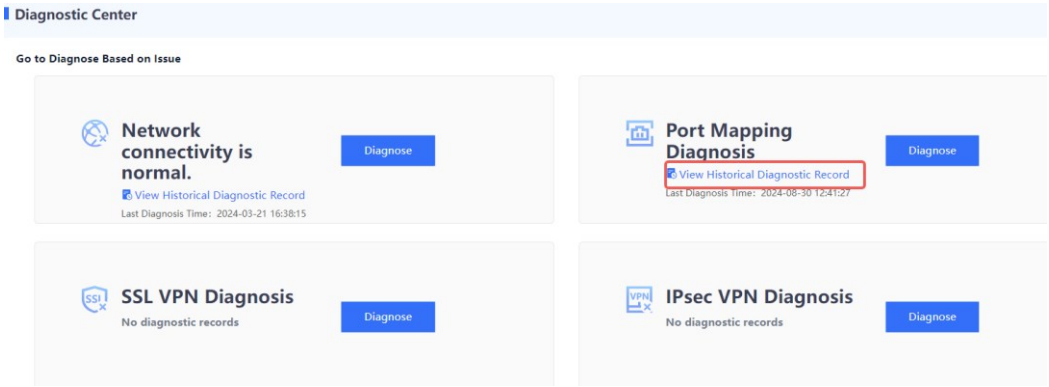
next phase.



(7) Repeat steps (5) and (6) until all items are checked.

Follow-up Procedure

- Click **View Historical Diagnostic Record** to view and download historical diagnosis information.



3. IPsec VPN Diagnosis

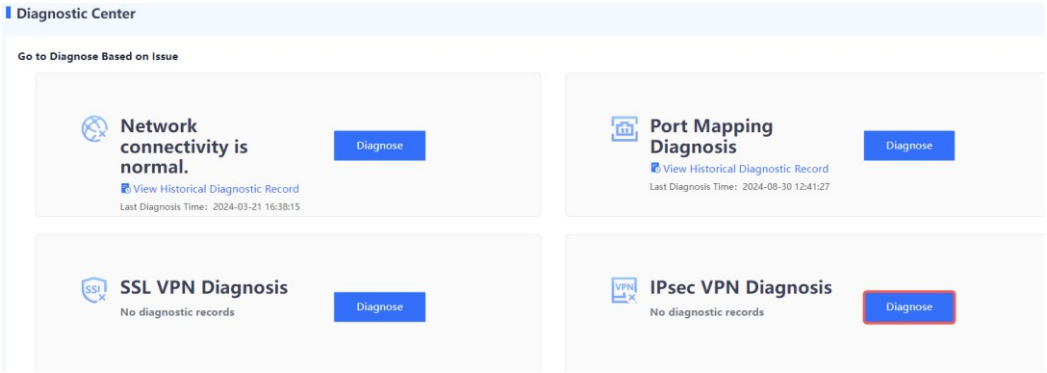
Application Scenario

When an IPsec VPN tunnel is abnormal (for example, the tunnel cannot be established or data forwarding fails), you can use the IPsec VPN diagnosis tool to perform troubleshooting and locate the network issue with one click.

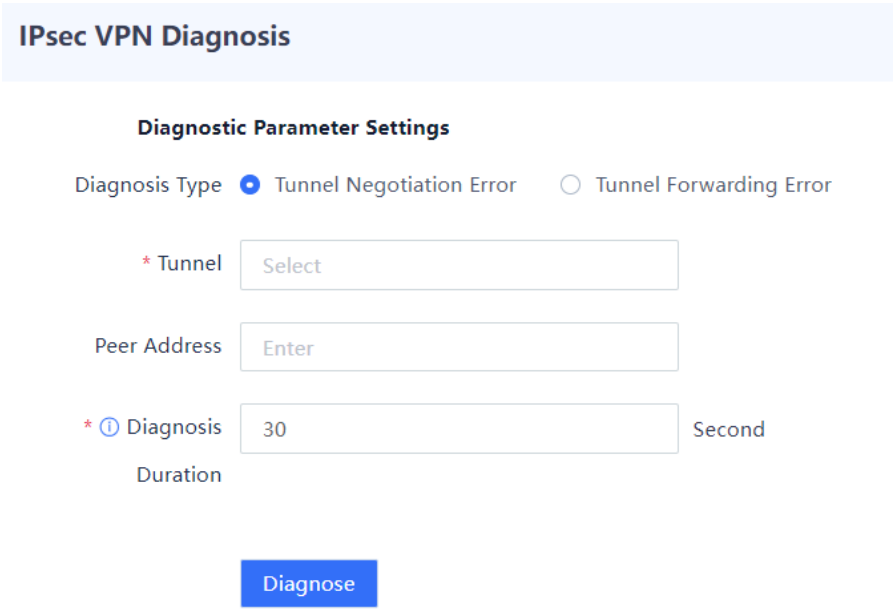
Procedure

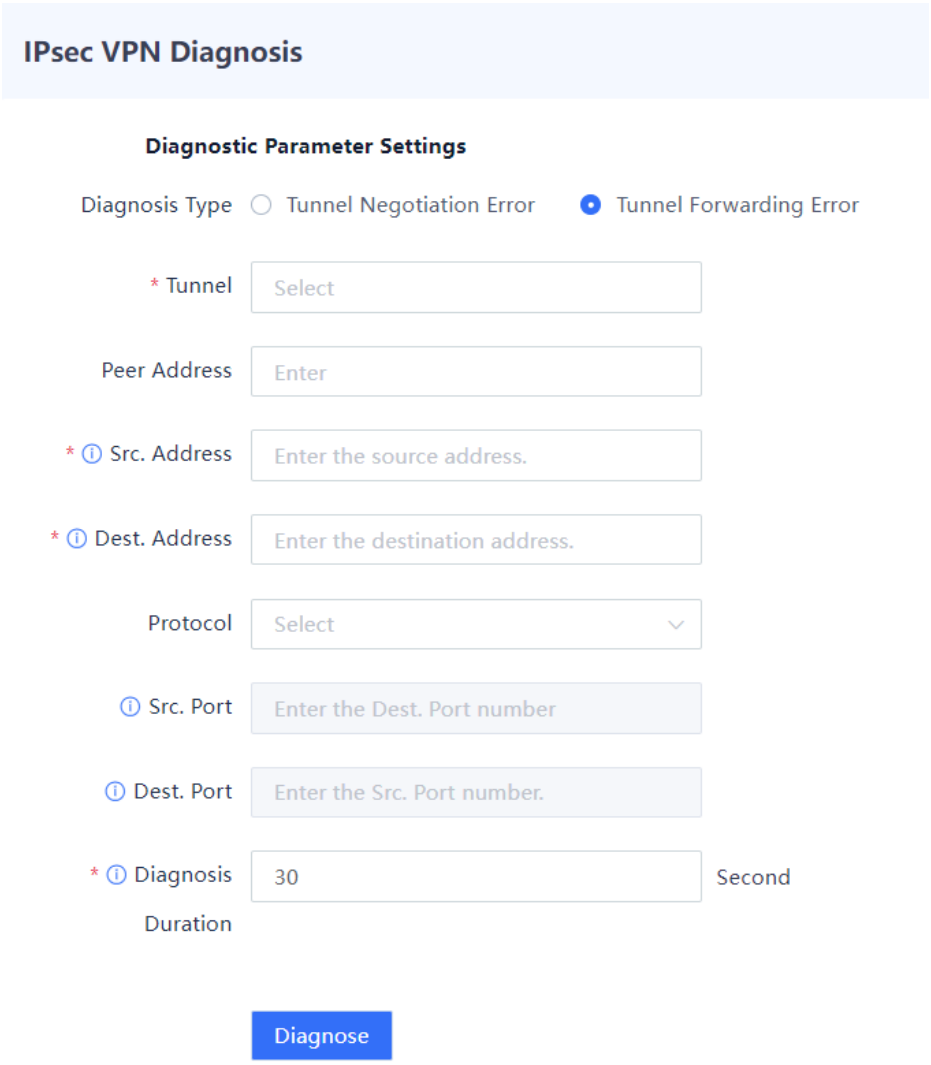
(1) Choose **O&M** > **Fault Diagnosis** > **Diagnostic Center**.

(2) Click **Diagnose** next to IPsec VPN Diagnosis.



(3) Set diagnostic parameters and click **Diagnose**. The firewall checks tunnel connectivity.

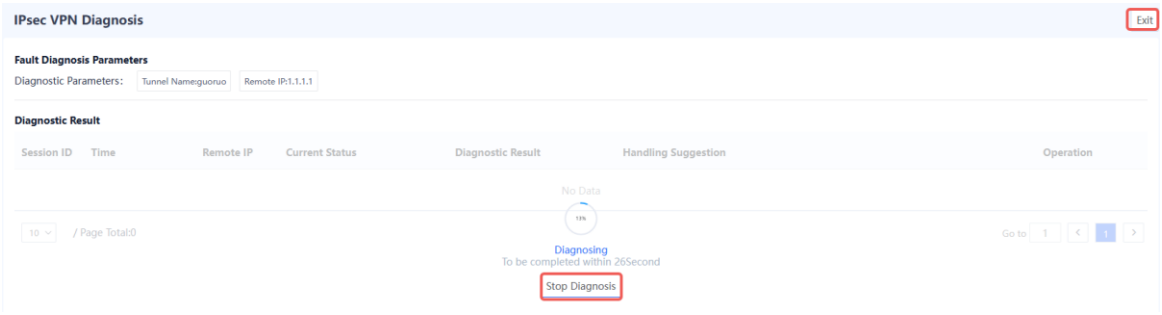




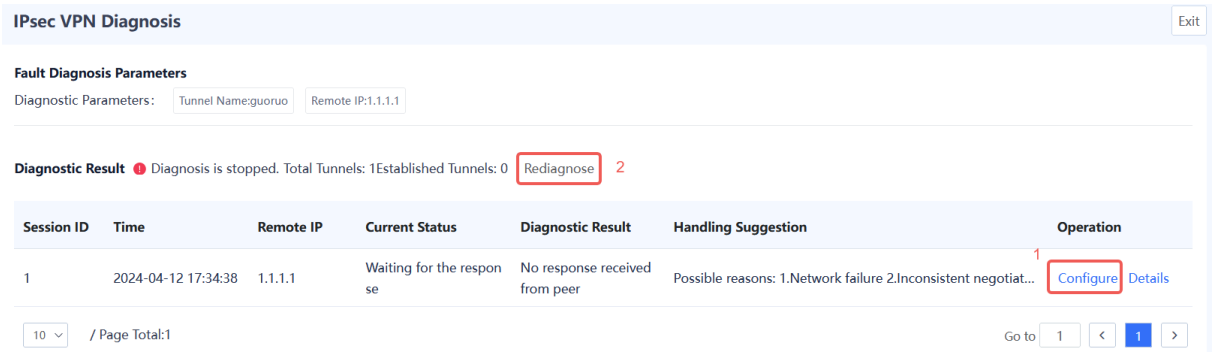
Item	Description	Remarks
Tunnel Negotiation Error		
Tunnel	Name of the tunnel to be diagnosed.	Select an existing IPsec VPN tunnel from the drop-down list.
Peer Address	Remote IP address of the IPsec VPN tunnel.	If the tunnel is in site-to-site mode, the value is automatically set after you select the tunnel. If the tunnel is in hub-and-spoke mode, you need to enter the remote IP address.
Diagnosis Duration	Tunnel diagnosis duration. The diagnosis automatically stops when the duration expires.	The default value is 30 seconds. [Example] 30

Item	Description	Remarks
Tunnel Forwarding Error		
Tunnel	Name of the tunnel to be diagnosed.	Select an existing IPsec VPN tunnel from the drop-down list.
Peer Address	Remote IP address of the IPsec VPN tunnel.	If the tunnel is in site-to-site mode, the value is automatically set after you select the tunnel. If the tunnel is in hub-and-spoke mode, you need to enter the remote IP address.
Src. Address	Source address of interesting traffic.	Only one IP address is supported. [Example 1] 192.168.1.1 [Example 2] 1234::100
Dest. Address	Destination address of interesting traffic.	Only one IP address is supported. [Example 1] 192.168.1.2 [Example 2] 1234::101
Protocol	Protocol of interesting traffic.	Select a value from the drop-down list.
Src. Port	Source port of interesting traffic. This parameter is optional when the protocol is TCP or UDP.	Only one port is supported. [Example] 81
Dest. Port	Destination port of interesting traffic. This parameter is optional when the protocol is TCP or UDP.	Only one port is supported. [Example] 80
Diagnosis Duration	Tunnel diagnosis duration. The diagnosis automatically stops when the duration expires.	The default value is 30 seconds. [Example] 30

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



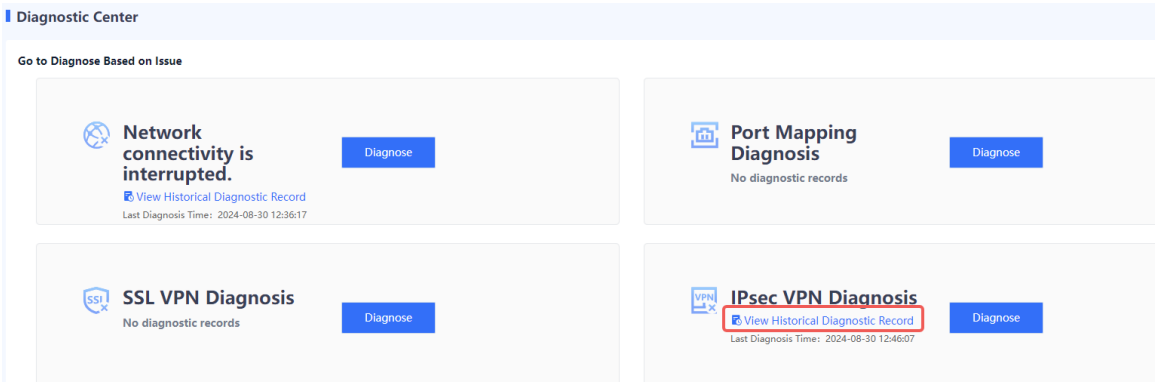
(5) After the diagnosis is complete, the diagnosis result, diagnosis details, and handling suggestions are displayed in the lower part of the page. Click **Configure** in the **Operation** column to rectify the fault based on the diagnosis details and handling suggestions, and then click **Rediagnose**.



(6) Repeat step 5 until all the items pass the check.

Follow-up Procedure

Click **View Historical Diagnostic Record** to view and download historical diagnostic records.



4. SSL VPN Fault Diagnosis

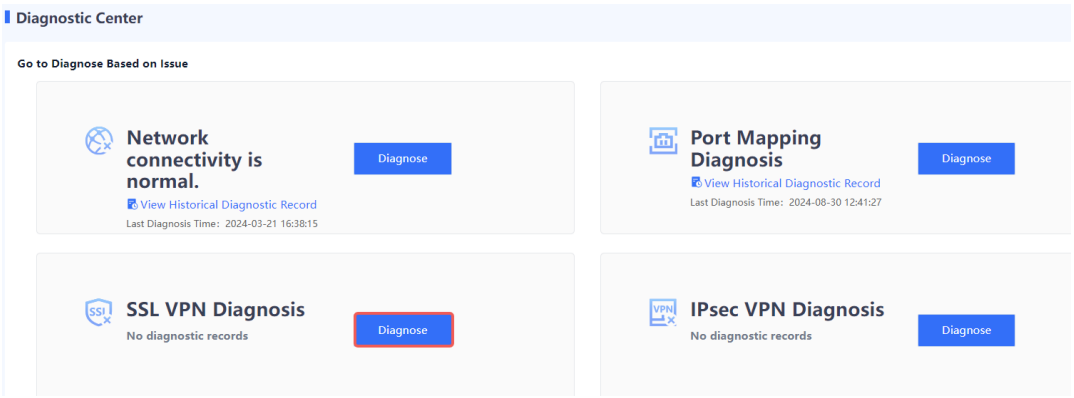
Application Scenario

When an SSL VPN tunnel is abnormal (for example, the user fails to log in to the gateway or access resources), you can use the SSL VPN diagnosis tool to perform troubleshooting and locate the network issue with one click.

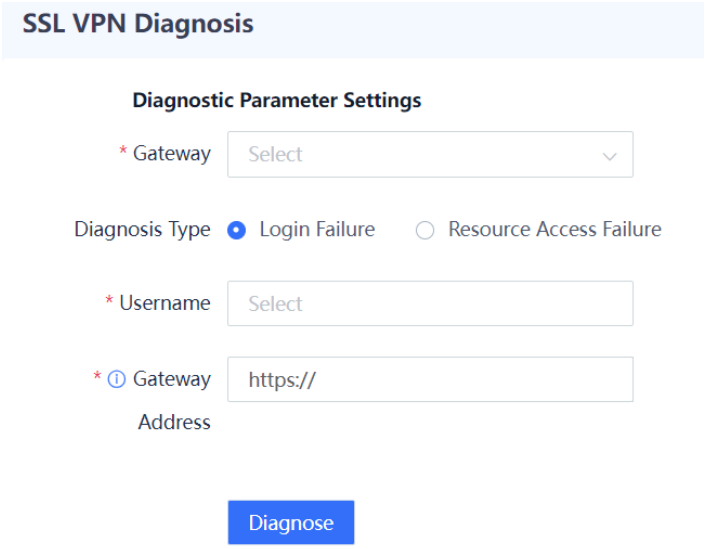
Procedure

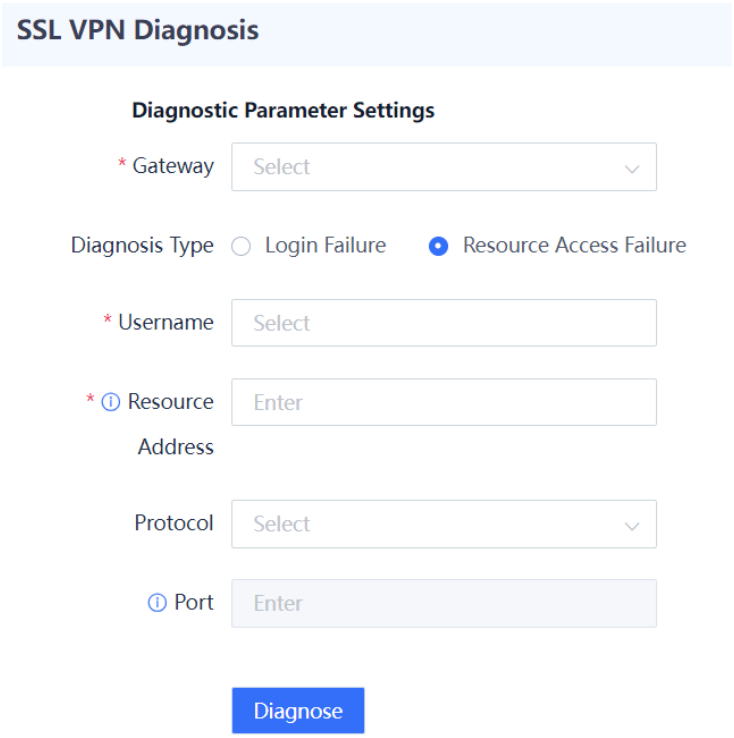
(1) Choose **O&M** > **Fault Diagnosis** > **Diagnostic Center**.

(2) Click **Diagnose** next to SSL VPN Diagnosis.



(3) Set diagnostic parameters and click **Diagnose**. The firewall checks tunnel connectivity.

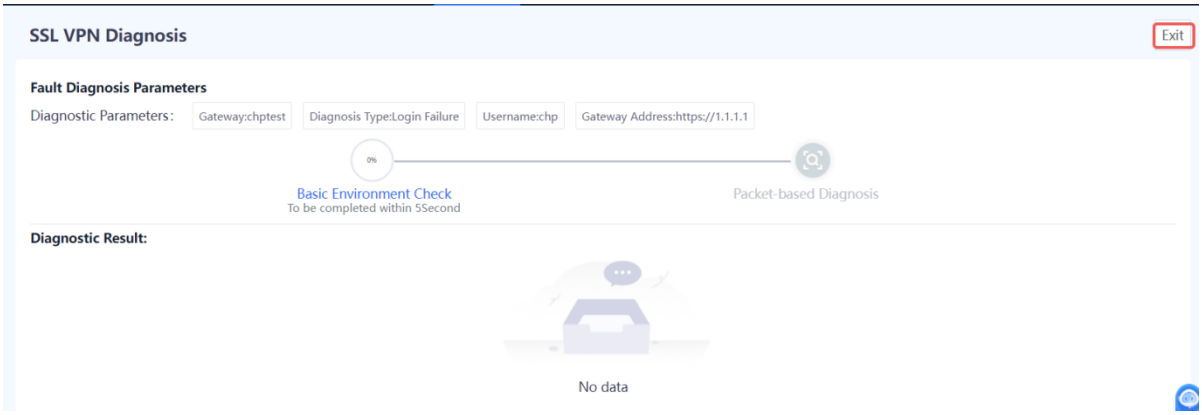




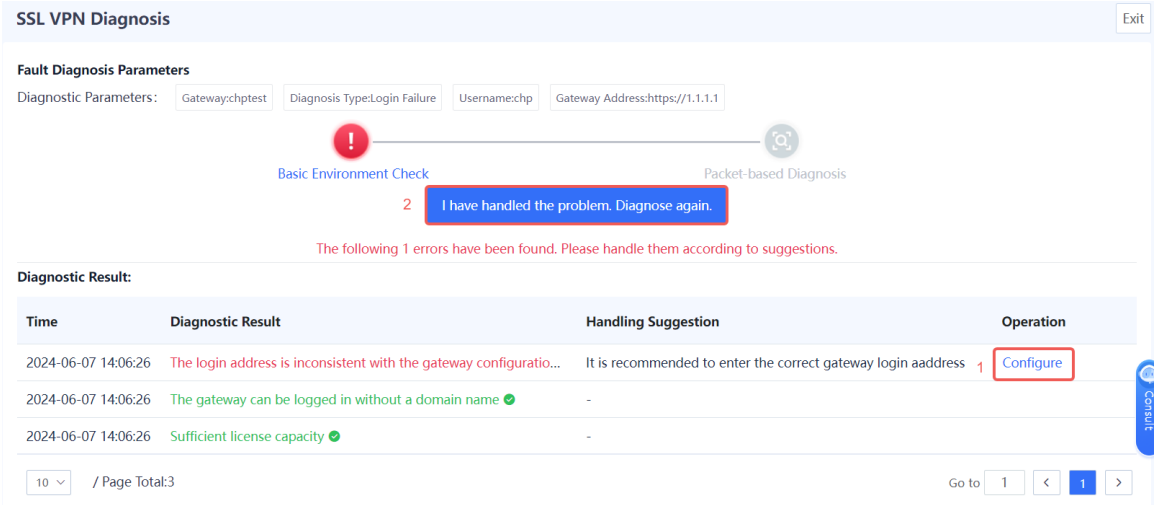
Item	Description	Remarks
Login Failure		
Gateway	Name of the gateway to be diagnosed.	Select an SSL VPN gateway from the drop-down list.
Username	Name of the user who fails to log in to the SSL VPN gateway.	Enter an existing user or select a user from the drop-down list.
Gateway Address	Address of the gateway to be diagnosed.	[Example] https://192.168.1.1:8443
Resource Access Failure		
Gateway	Name of the gateway to be diagnosed.	Select an SSL VPN gateway from the drop-down list.
Username	Name of the user who fails to access SSL VPN gateway resources.	Enter an existing user or select a user from the drop-down list.
Resource Address	IP address of the SSL VPN gateway that fails to be accessed.	[Example] 192.168.1.1

Item	Description	Remarks
Protocol	Protocol of the resource IP address that fails to be accessed.	Select a protocol from the drop-down list. [Example] TCP
Port	Protocol port number of the resource IP address that fails to be accessed.	This parameter can be configured only when the protocol is TCP or UDP.

(4) (Optional) During the diagnosis, you can exit the diagnostic task at any time if required.



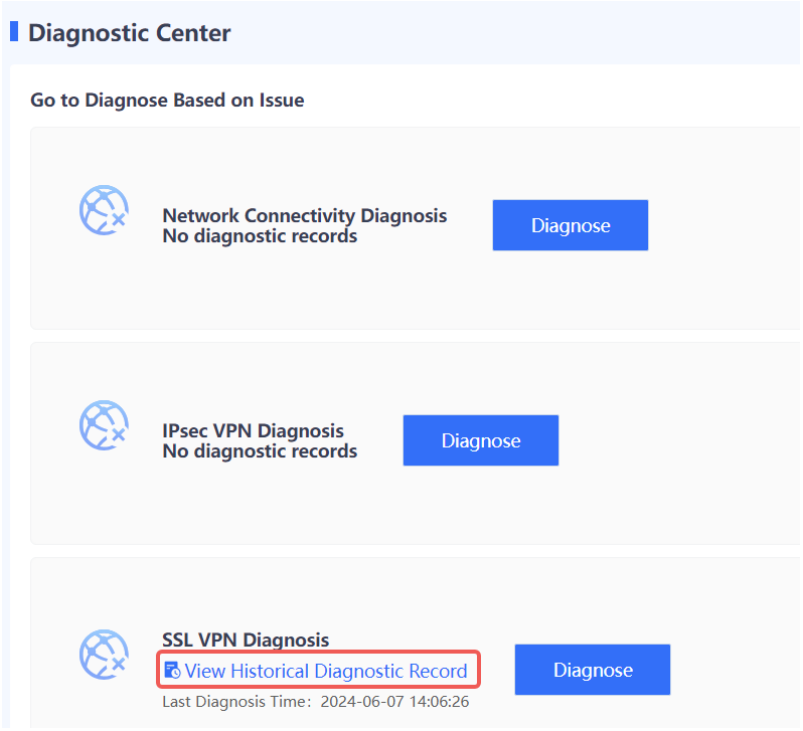
(5) After the diagnosis is complete, the diagnosis result, diagnosis details, and handling suggestions are displayed in the lower part of the page. Click **Configure** in the **Operation** column to rectify the fault based on the diagnosis details and handling suggestions, and then click **I have handled the problem. Diagnose again.**



(6) Repeat step 5 until all the items pass the check.

Follow-up Procedure

Click **View Historical Diagnostic Record** to view and download historical diagnostic records.



8.6.2 Device Self-Test

1. Device Self-Test

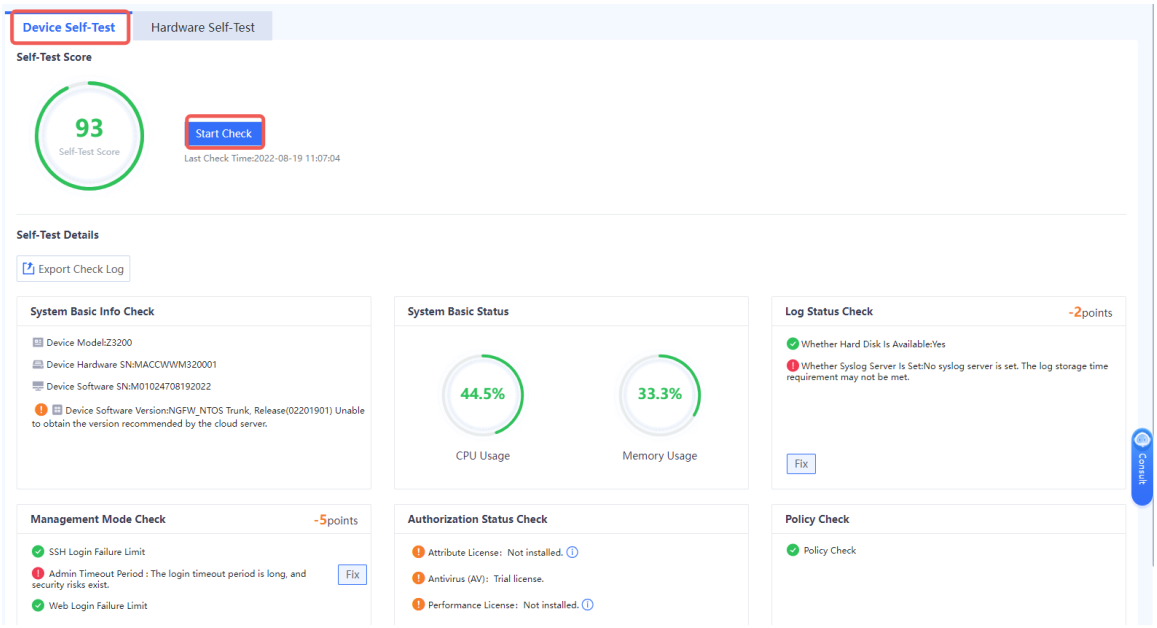
Application Scenario

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

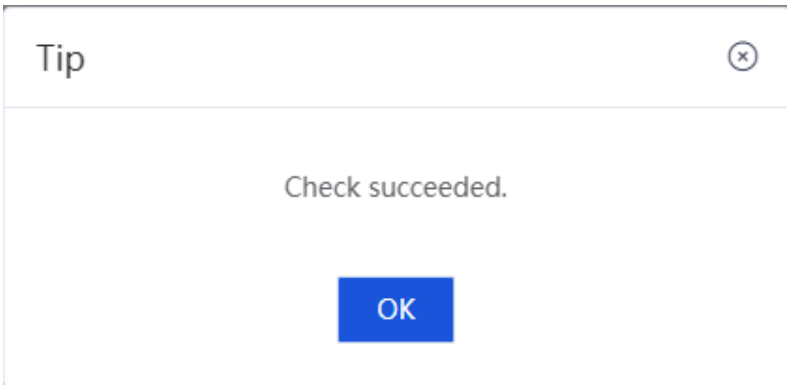
Procedure

(1) Choose **O&M** > **Fault Diagnosis** > **Device Self-Test** > **Device Self-Test**. The **Device Self-Test** page is displayed.

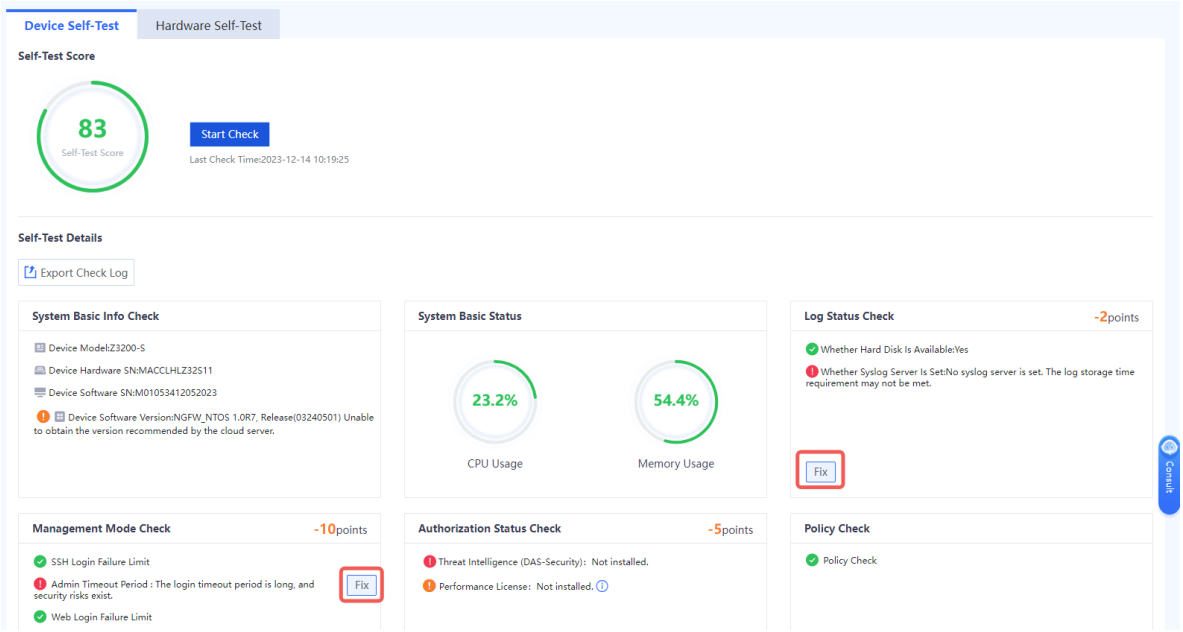
(2) Click **Start Check** to start device self-test.



(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.



2. Hardware Self-Test

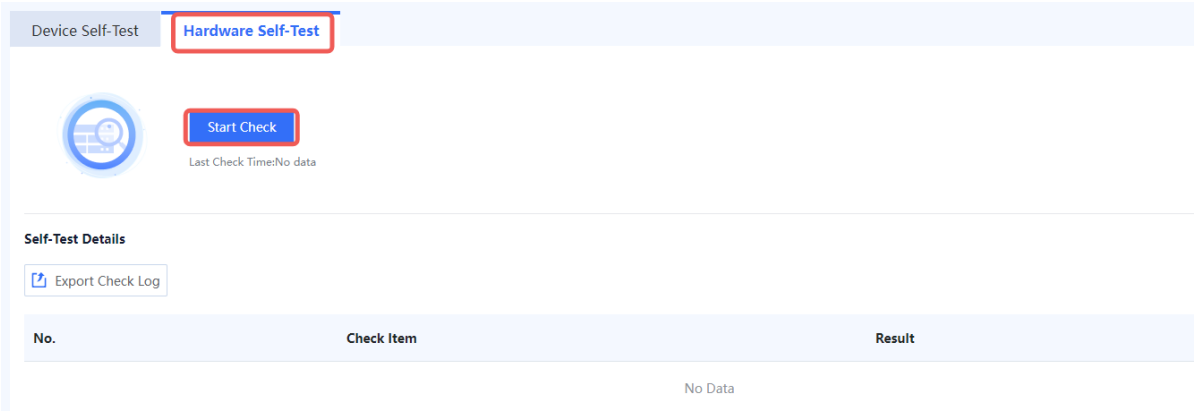
Application Scenario

The hardware self-test function can detect whether the hardware status of the device, including the temperature, hard disk, power supply, and voltage, is normal.

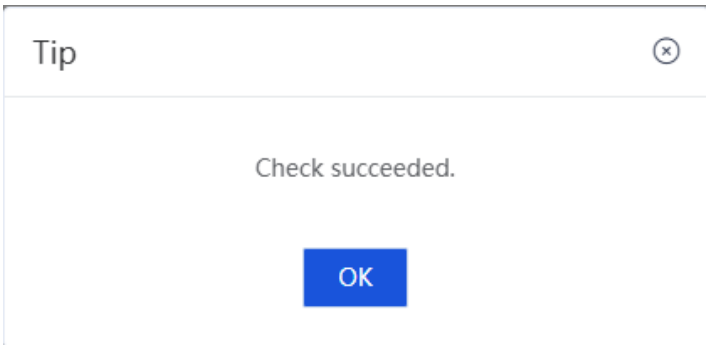
Procedure

(1) Choose **O&M** > **Fault Diagnosis** > **Device Self-Test** > **Hardware Self-Test** and click the Hardware Self-Test tab.

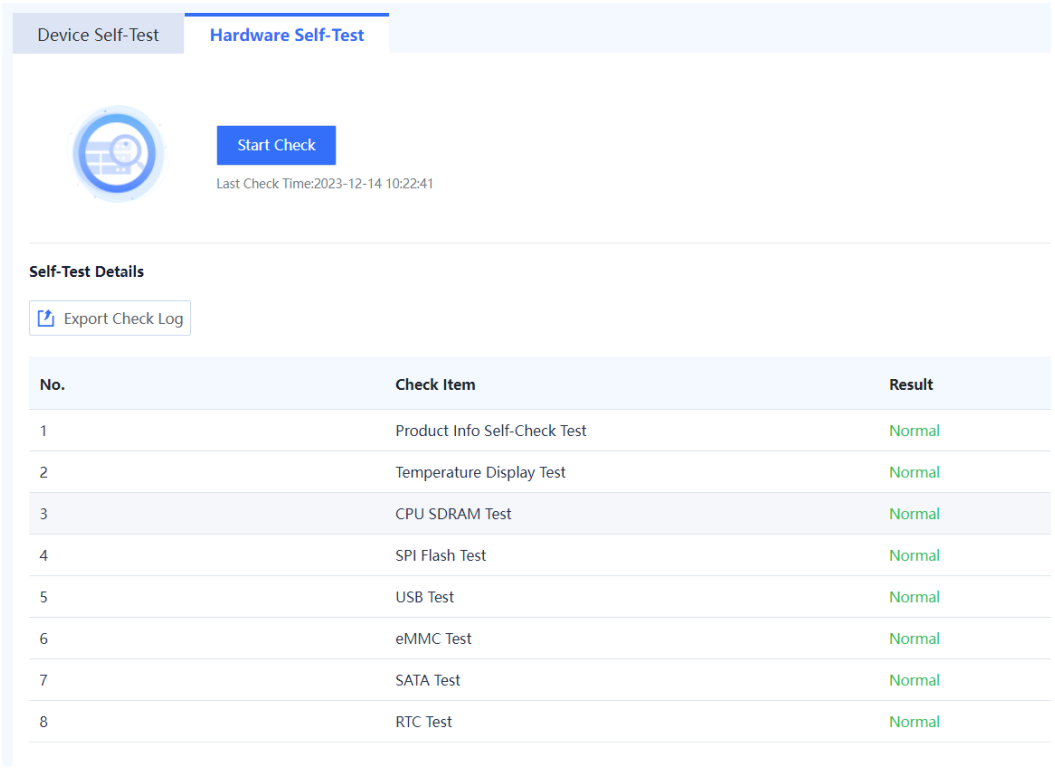
(2) Click **Start Check**. The device performs a self-test



(3) After the self-test is complete, a dialog box is displayed. Click **OK**.



(4) If any item is abnormal, contact Ruijie Networks technical support.



No.	Check Item	Result
1	Product Info Self-Check Test	Normal
2	Temperature Display Test	Normal
3	CPU SDRAM Test	Normal
4	SPI Flash Test	Normal
5	USB Test	Normal
6	eMMC Test	Normal
7	SATA Test	Normal
8	RTC Test	Normal

8.6.3 Ping

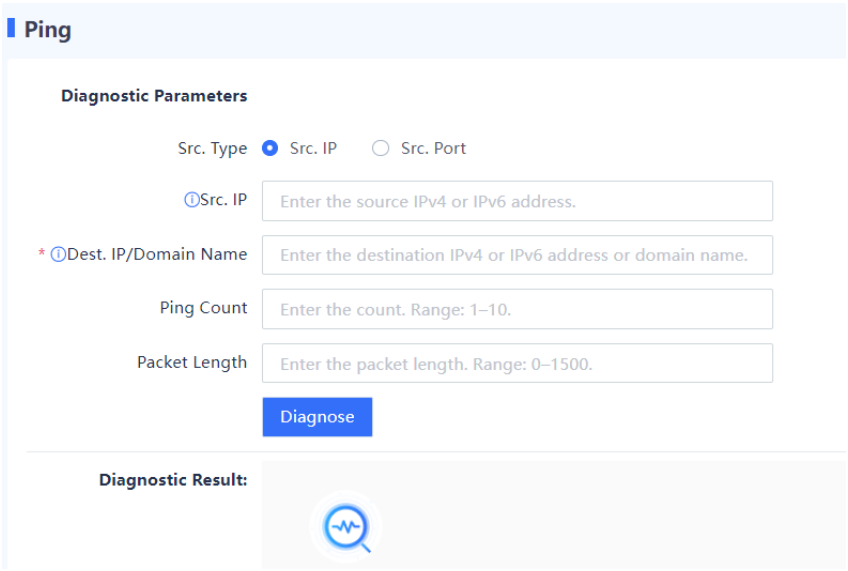
Application Scenario

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 **O&M** > **Fault Diagnosis** > **Ping**.

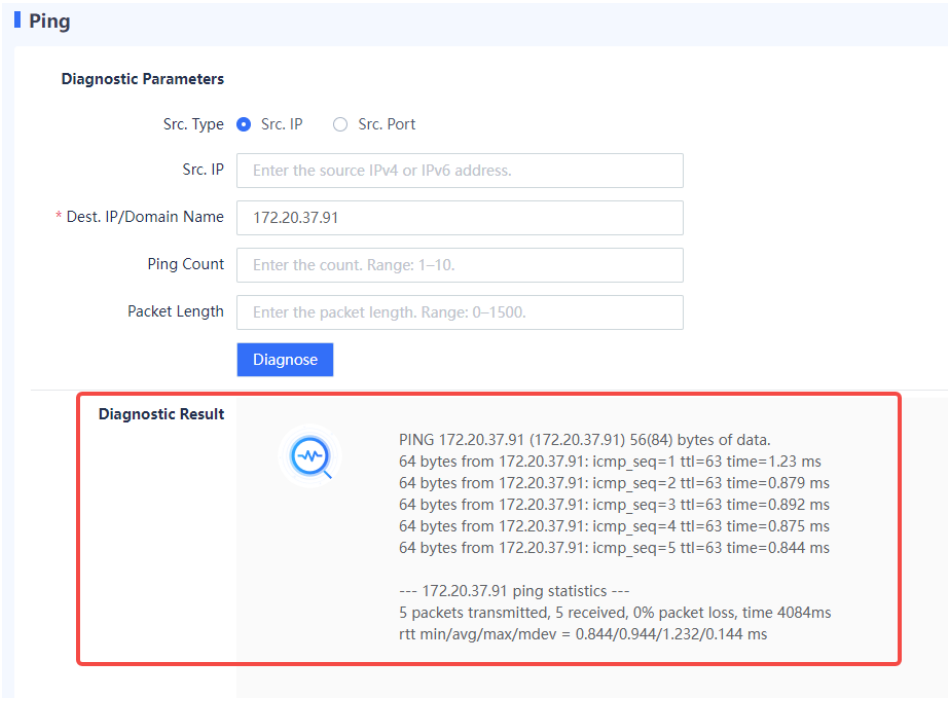


(2) Configure the diagnosis parameters, such as the source IP address, destination IP address, and domain name.

(3) Click **Diagnose**.

Follow-up Procedure

The diagnostic result is displayed in the lower part of the page.



8.6.4 Tracert

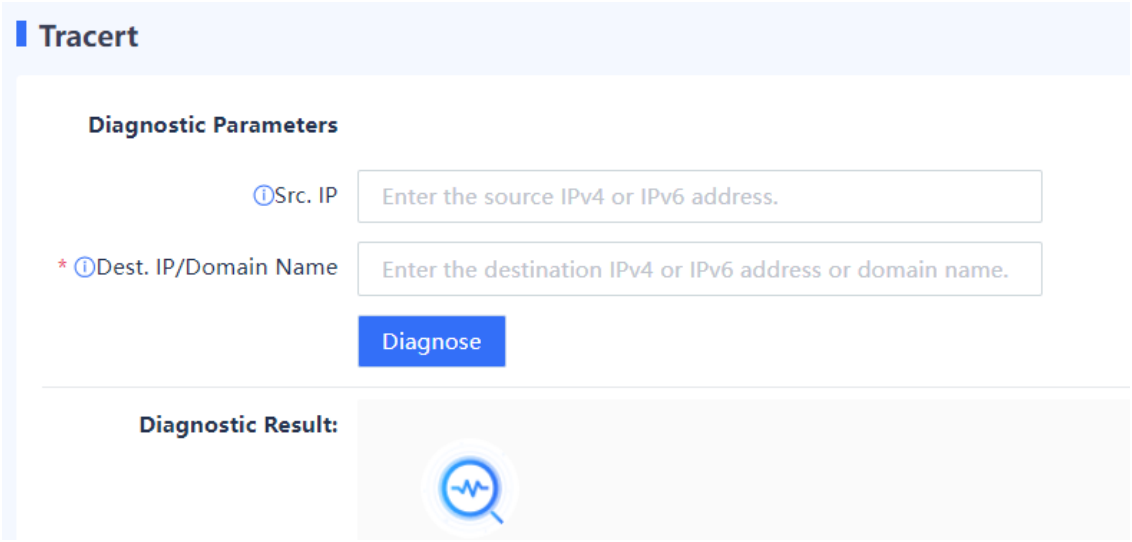
Application Scenario

You can locate a network fault using tracert.

Procedure

(1) Access the **Tracert** page.

Choose **O&M** > **Fault Diagnosis** > **Tracert**.

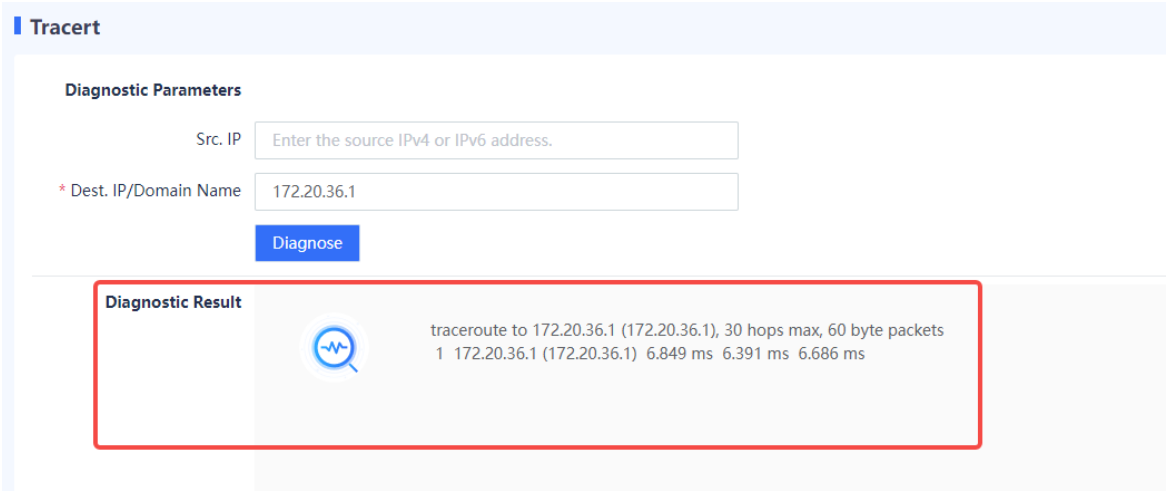


(2) Configure the diagnosis parameters, such as the source IP address, destination IP address, and domain name.

(3) Click **Diagnose**.

Follow-up Procedure

The diagnostic result is displayed in the lower part of the page.



8.6.5 Packet Obtaining Tool

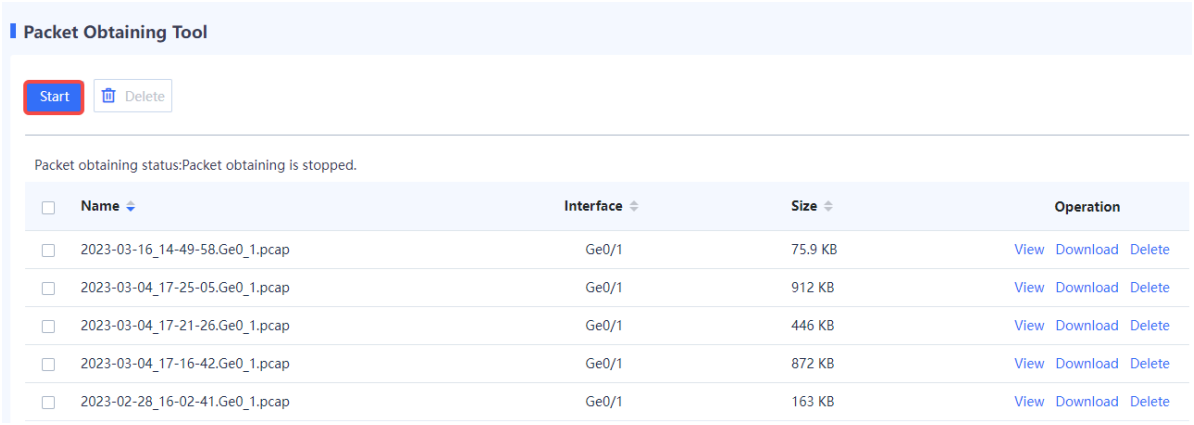
Application Scenario

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.

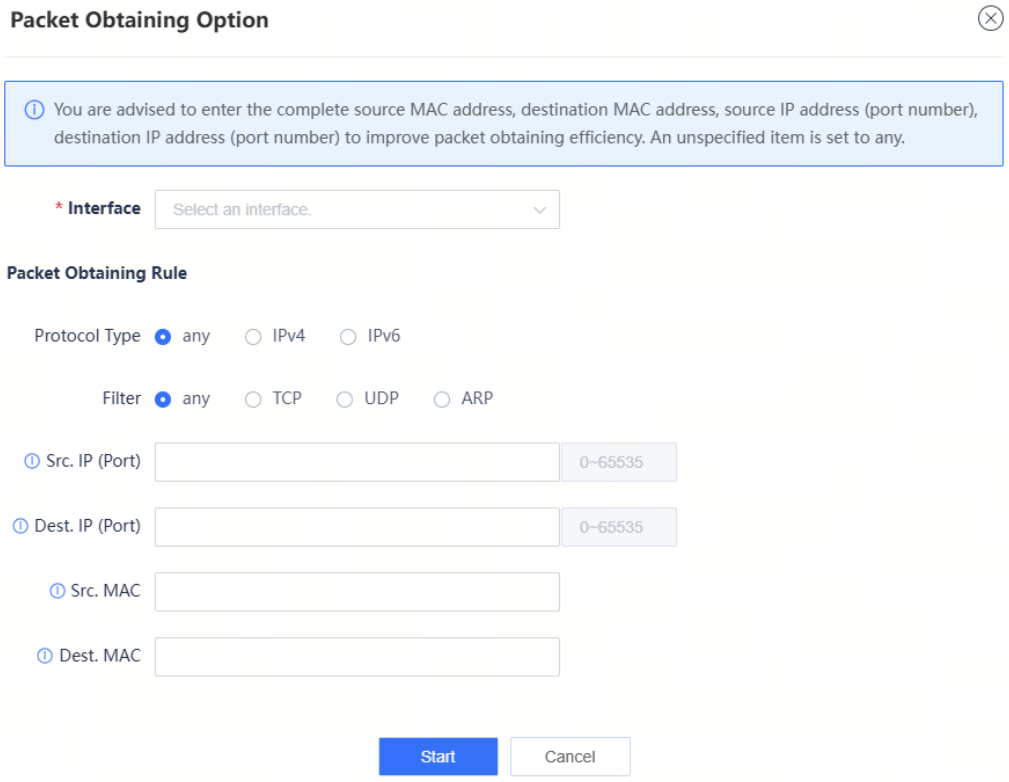
Procedure

(1) Access the **Packet Obtaining Tool** page.

Choose **O&M** > **Fault Diagnosis** > **Packet Obtaining Tool**.



(2) Click **Start**, select the interface where packets need to be obtained, and then set the packet obtaining rule. Currently, you can filter the information based on the protocol type, IP address, port number, and MAC address.



Item	Description
Interface	Interface from which packets are obtained. You can configure a maximum of four interfaces.
Protocol Type	Protocol type of packets to be obtained. You can configure this parameter to obtain only IPv4 or IPv6 packets.

Item	Description
Filter	● **any**: Does not limit the packet type to be obtained. ● **TCP**: Obtains TCP packets. ● **UDP**: Obtains UDP packets. ● **ARP**: Obtains ARP packets. This option is available only when **Protocol Type** is set to **IPv6**.
Src. IP (Port)	Source IP address of the packets to be obtained. When you configure the device to obtain TCP or UDP packets, you can specify a port number. This option is not supported when the device obtains ARP packets.
Dest. IP (Port)	Destination IP address of the packets to be obtained. When you configure the device to obtain TCP or UDP packets, you can specify a port number. This option is not supported when the device obtains ARP packets.
Src. MAC	Source MAC address of the packets to be obtained.
Dest. MAC	Destination MAC address of the packets to be obtained.

(3) Click **Start**.

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.

8.6.6 One-Click Fault Information Collection

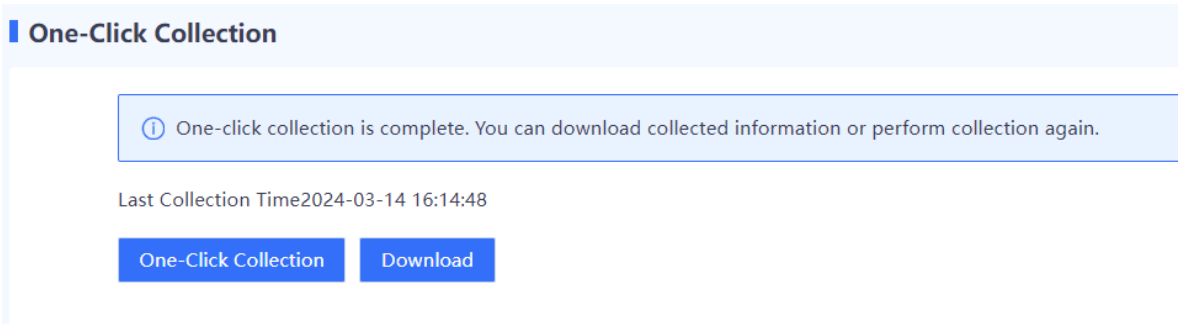
Application Scenario

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 **O&M** > **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.

8.7 Report

8.7.1 Generating and Viewing Reports

Application Scenario

You can configure a report task to enable the device to automatically generate visualized and multi-dimensional traffic reports and security reports at specified intervals. These reports help administrators implement refined network management and proactive threat defense. The device can generate daily reports, weekly reports, and monthly reports to meet the requirements in different scenarios such as quick inspection and operation analysis.

Table 8-1 The following table describes the report types.

Report Type	Report Content
Traffic report	Summarizes traffic data from dimensions such as the line, application, user, source IP address, and session and displays traffic trends and top rankings to provide data support for network optimization, bandwidth management, and user behavior analysis.
Security report	Integrates security module data including antivirus protection, intrusion prevention, web app protection, threat intelligence, DDoS protection, and AI-based Threat Detection. Extracts key information such as top attack types, top attackers and victim hosts, attack interception information, and attack trends. The information helps administrators understand the security threat trends, identify security risks in advance, and proactively defend against threats.

Note

RG-CF10S and RG-CF10S-LTE do not support the report function.

Prerequisites

- The local report function is supported only when a hard disk is installed on the device.

  Note

  If no hard disk is installed on the device, enable UX Improvement Plan and subscribe and view reports on MACC or Ruijie Security Cloud Platform.

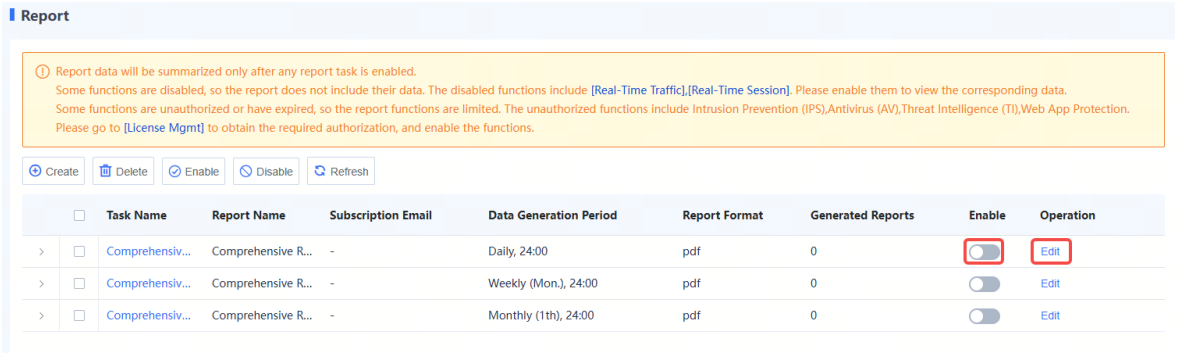
- Enable security service functions such as antivirus protection, intrusion prevention, threat intelligence, web app protection, DDoS protection, and AI-based Threat Detection, so that security reports can obtain and analyze the corresponding service statistics. If related functions are disabled or not licensed, or the license has expired, the corresponding statistical information will not be displayed in security reports.
- Enable traffic statistics collection functions such as real- time traffic, traffic statistics collection, and

real- time sessions, so that traffic reports can obtain and analyze the corresponding statistics. If related functions are disabled, the corresponding statistical information will not be displayed in traffic reports.

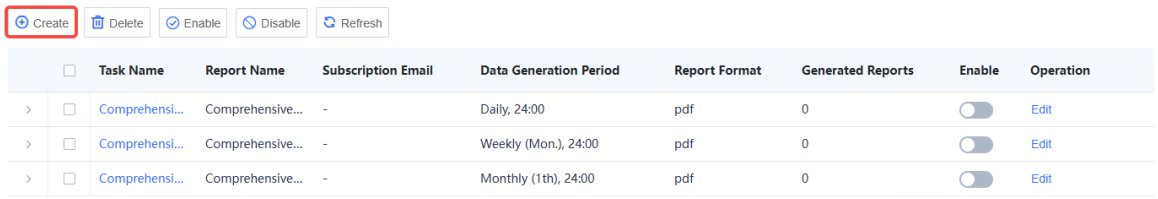
Procedure

(2) Choose **O&M** > **Report**.

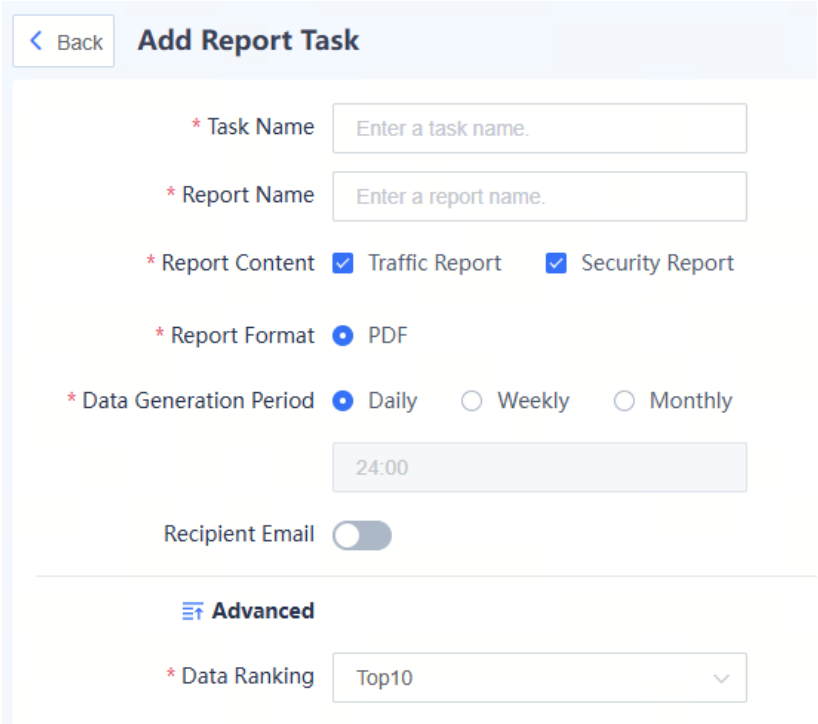
The system predefines three report tasks: comprehensive report (daily), comprehensive report (weekly), and comprehensive report (monthly). Toggle on to enable a report task and click **Edit** to modify the report task configuration. You cannot delete predefined report tasks or modify the data generation period for reports.



(3) Click **Create** to create a report task.



(4) Configure relevant parameters for a report task.

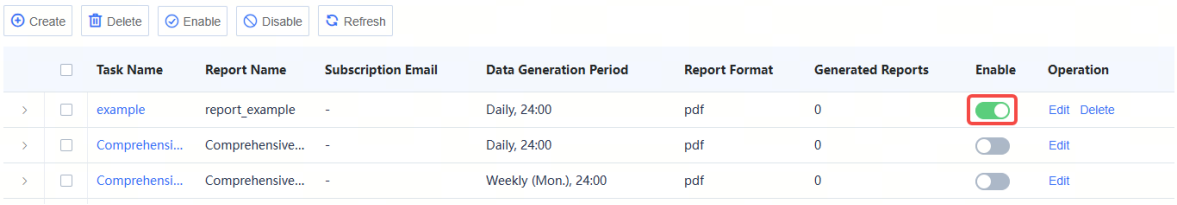


Item	Description	Remarks
Task Name	Name of the report task.	[Example] test_report
Report Name	Name of the report. The name is displayed on the cover of a report file.	[Example] Enterprise A traffic monthly report
Report Content	Content in the report. ● **Traffic Report**: Displays traffic data and trends of the device within a period of time, including traffic overview, line traffic, application traffic, user traffic, source IP traffic, online users, and number of sessions. ● **Security Report**: Displays security threat statistics and trends of the device within a period of time, including risk overview, antivirus protection analysis, intrusion prevention analysis, threat intelligence analysis, DDoS protection analysis, attack source and destination statistics, and encrypted traffic detection statistics.	[Example] Traffic Report and Security Report
Report Format	Format of the generated report file. Currently, the file format can only be PDF.	[Example] PDF

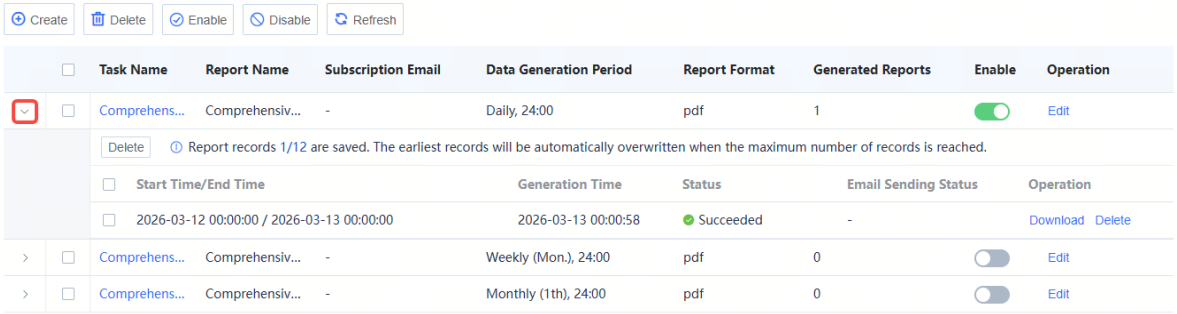
Item	Description	Remarks
Data Generation Period	Period for report generation. ● **Daily**: The device generates a report for the current day at 24:00 every day. ● **Weekly**: The device generates a report for the previous week at the specified time every week. For example, if you configure the device to generate a report at 24:00 of Monday (00:00 of Tuesday) every week, the statistical period of a weekly report is 00:00 of Tuesday of last week to 00:00 of Tuesday of the current week. ● **Monthly**: The device generates a report for the previous month at the specified time every month. For example, if you configure the device to generate a report at 24:00 on the first day of every month (00:00 on the second day of every month), the statistical period of a monthly report is 00:00 on the second day of last month to 00:00 on the second day of the current month. If the selected date does not exist for a month (such as February 30 or February 31), a reported is generated at 24:00 on the last day of the month.	[Example] Weekly
Recipient Email	Enables the device to automatically send the generated report to the specified email address. After you enable this function, you must specify an email address for receiving reports. Caution: To use the report pushing by email function, the device must be able to normally access Ruijie Security Cloud Platform (https://secloud1.ruijie.com.cn).	After you toggle on **Recipient Email**, you must specify an email address for receiving reports. Enter one email address in each line. You can configure a maximum of five email addresses. [Example] Enable example@ruijie.com.cn
Advanced		
Data Ranking	Number of data entries in the data ranking of the report. The device can display top 5, top 10, or top 50 data rankings.	[Example] Top10

(5) Click **Confirm**.

(6) Ensure that the report task is enabled. After that, the system starts summarizing report data and generating reports.



Follow-up Procedure



- Click the arrow in front of a report task to view generation records of the report and download the report file.

  Note

  - The device can store a maximum of 12 report records (files) for each report task. After the number reaches the limit, the device automatically overrides the earliest records.
  - Find a report record and click **Download** to download the report file.
  - Find a report record and click **Delete** to delete the report record and the corresponding report file.

- Toggle on or off the Enable switch to enable or disable a report task. After you disable a report task, the corresponding report file will not be deleted.
- Click **Delete** to delete the report task. After you delete a report task, all the generated tasks of this task are deleted too. Exercise caution when performing this operation.

9 Ruijie Cloud Connection

9.1 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.

9.2 Connecting to Ruijie Cloud

9.2.1 Starting Ruijie Cloud

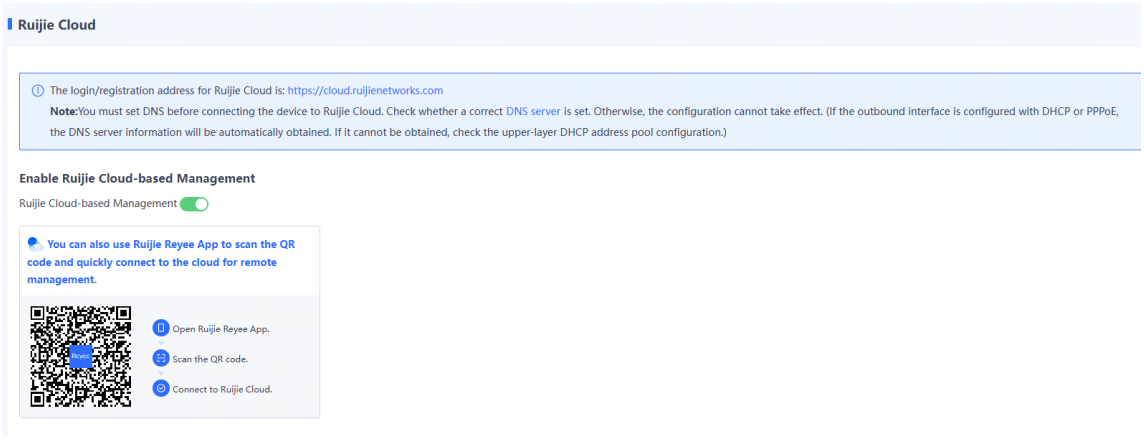
Application Scenario

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**.

(2) Toggle on **Ruijie Cloud-based Management** (enabled by default). Then you can manage the firewall on Ruijie Cloud.



9.2.2 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.

You can register a Ruijie Cloud account at https://cloud.ruijienetworks.com and bind devices on the platform.

9.3 Operations on Ruijie Cloud

9.3.1 Viewing Device Information

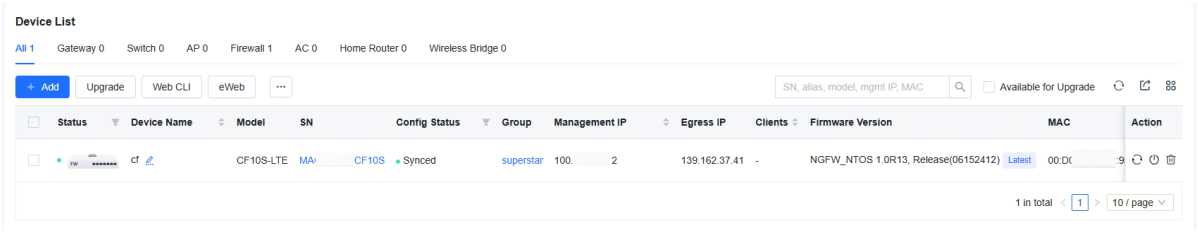
Application Scenario

After enabling Ruijie Cloud, enter the address of Ruijie Cloud (https://cloud.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

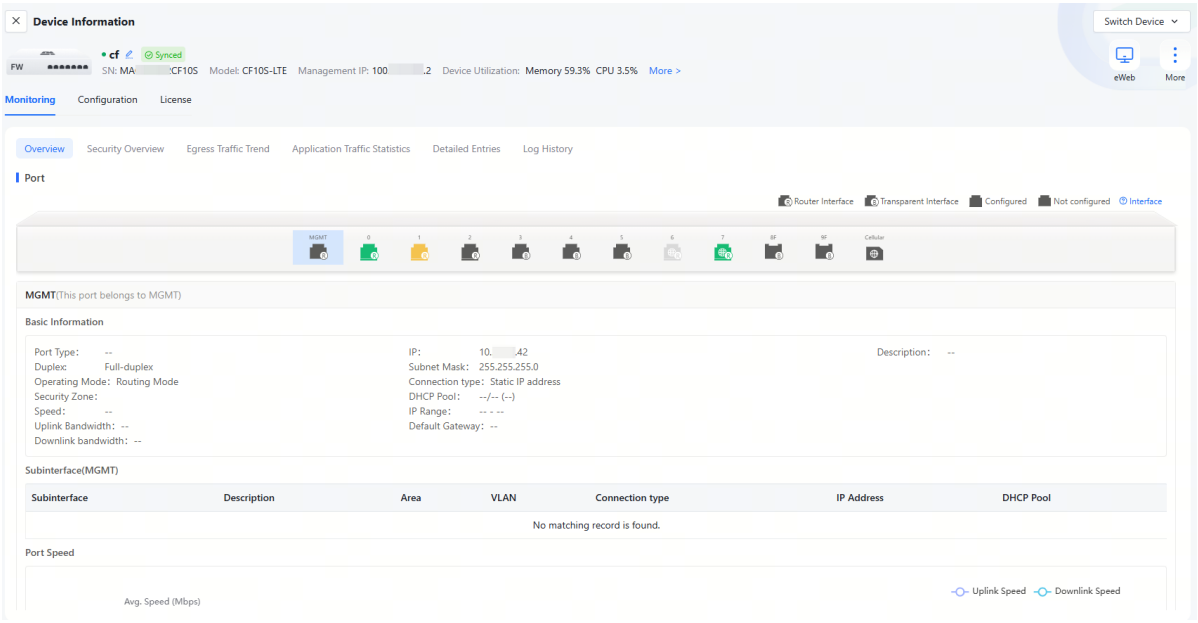
(1) Choose **Project** > **Devices** to access the page of device list.

(2) View device 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.



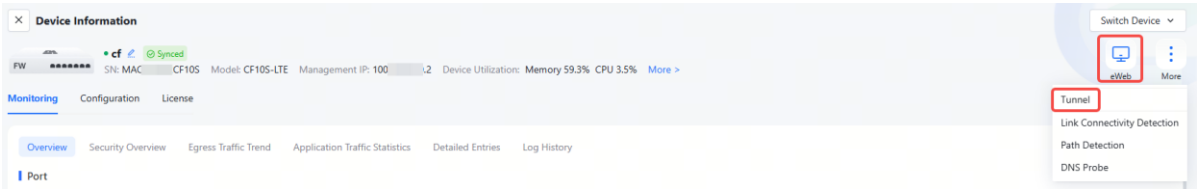
You can click the titles one by one to manage devices.

- **Monitoring**: Supports different modules, including **Overview**, **Security Overview**, **Egress Traffic Trend**, **Detailed Entries**, and **Log History**.
- **Configuration**: Supports different modules, including **Interface**, **Routing**, **Configuration Backup**, **Security Policy**, and **Threat Intelligence**.
- **License**: Allows you to check the license activation and information.

9.3.2 Managing Tunnels

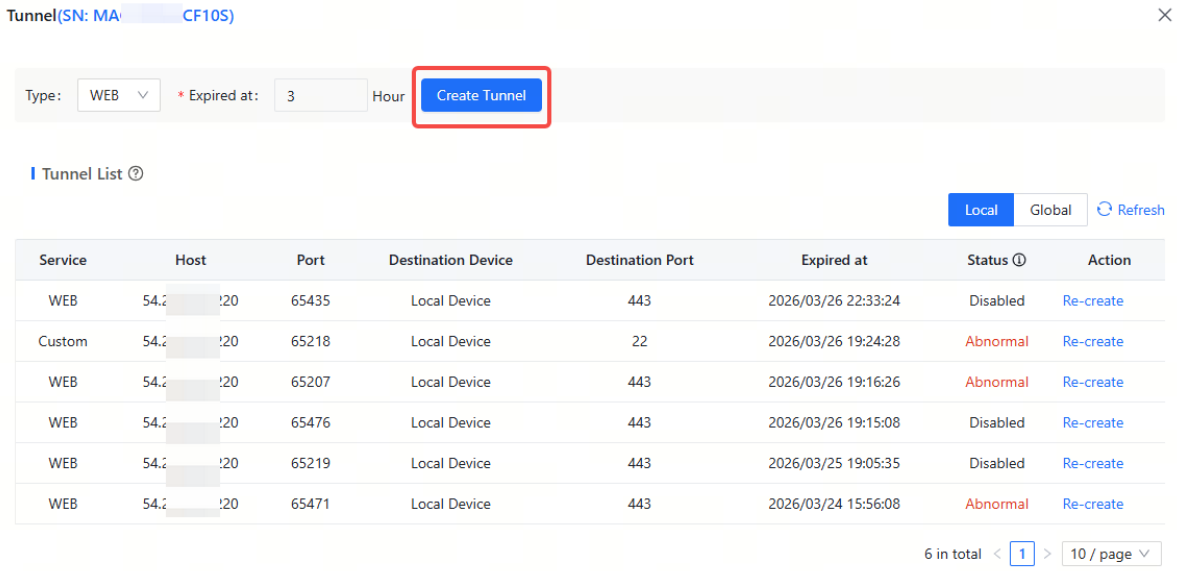
(1) Click **More** and select **Tunnel** from the drop-down list, or click **eWeb** to access the device's eWeb.

Figure 9-1 Tunnel Management



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

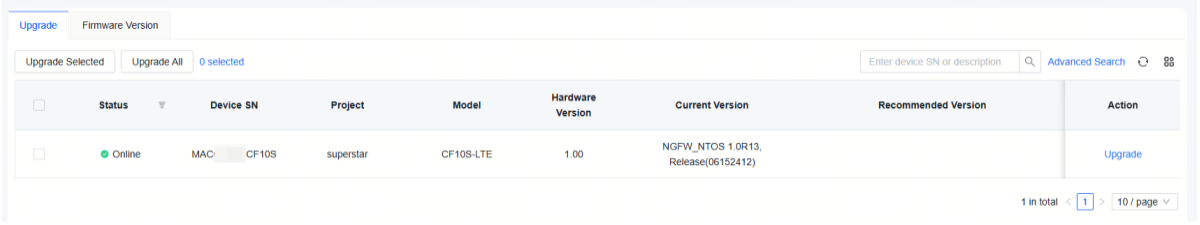
Figure 9-2 Creating a Tunnel



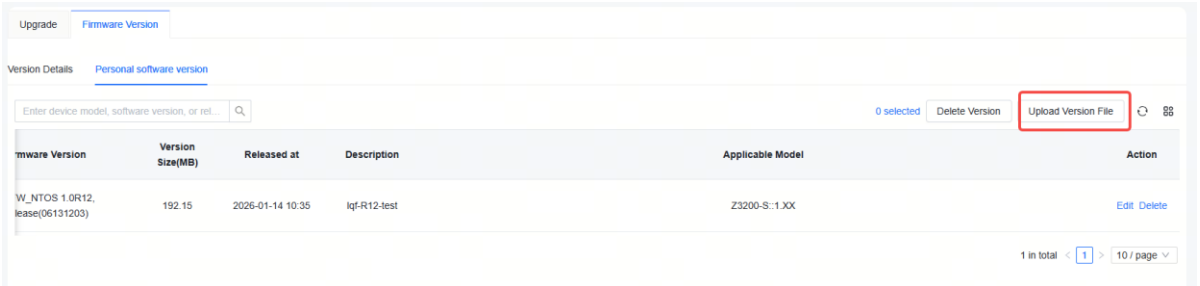
9.3.3 Upgrading Device Software

(1) Choose **Project** > **Upgrade** > **Upgrade**..

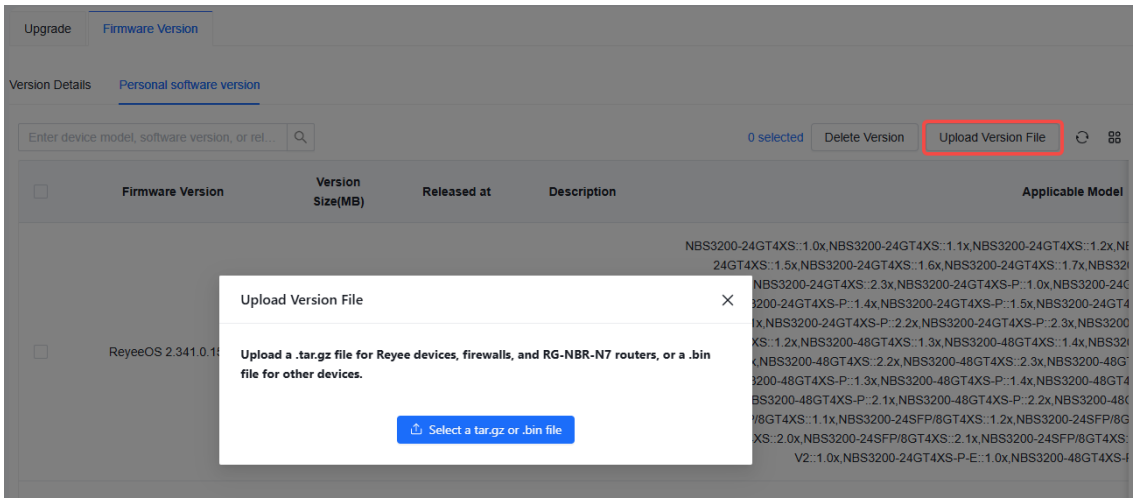
(2) Find the device to be upgraded in the device list, and click **Upgrade** in the **Action** column.



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



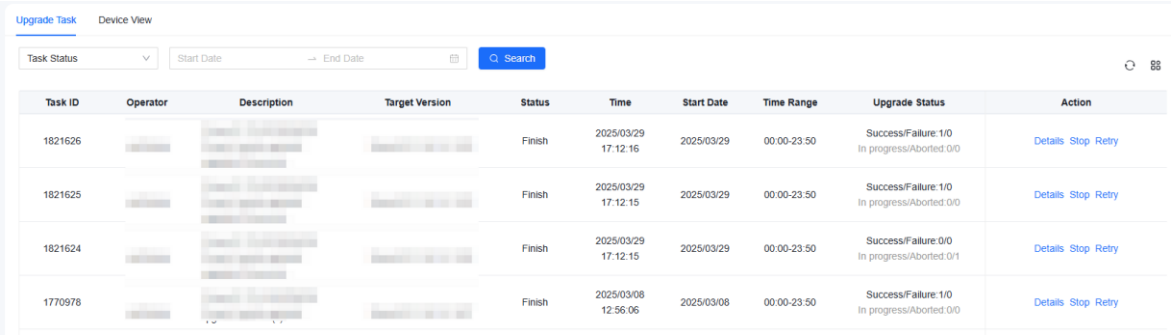
To perform a local upgrade, choose **Project** > **Upgrade** > **Firmware Version** > **Personal software version** and click **Upload Version File** to upload the upgrade package file.



(4) 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.

(5) When the upgrade is completed, choose **Project** > **Logs & Alarms** > **Upgrade Log** to view the upgrade result.



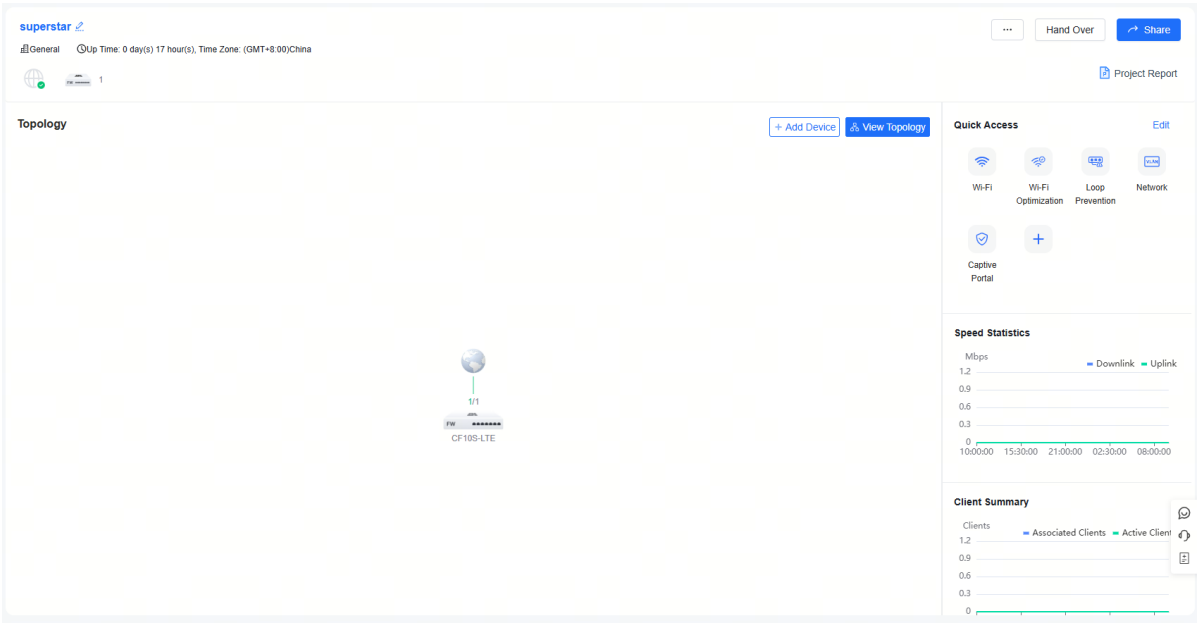
9.3.4 Viewing Network Topology

The relationships between the firewall and other network devices can be discovered on Ruijie Cloud and the topology is generated.

Caution

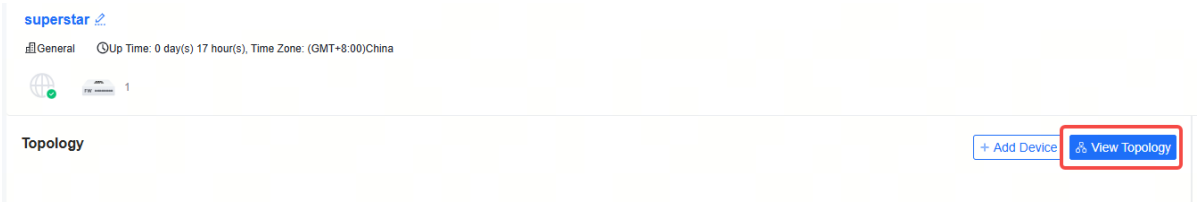
- When there are multiple default routes on the firewall, or when bridge interfaces and routing interfaces are mixedly used, you will find that the topology on Ruijie Cloud is abnormal.
- When the firewall is in transparent mode, port 0/MGMT does not need to be connected separately.

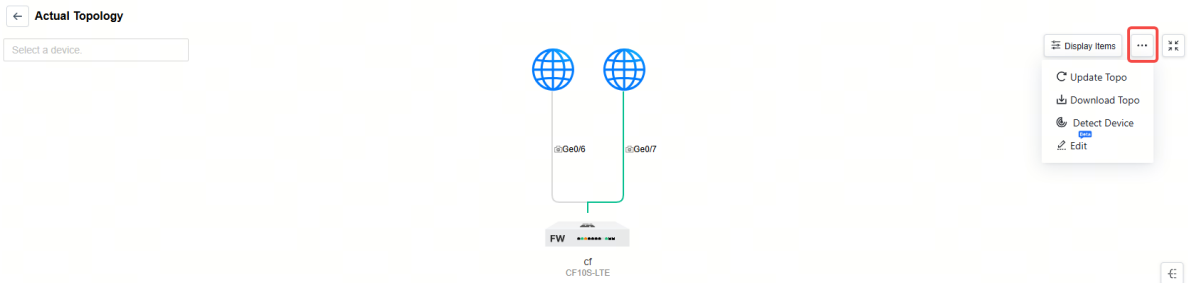
(1) Choose **Project** > **Workspace** to view the topology of the firewall and other network devices.



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 **Edit**.





10 FAQs

10.1 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://10.20.30.42) 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://10.20.30.42 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.

  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.

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

Possible Causes

The SSH port number is incorrect.

Solution

(1) Check the network connection.

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

Figure 10-1 Modifying the SSH Port Number

