



Ruijie RG-WALL 1600-Z-S Series Cloud-Managed Firewalls

Cookbook

Copyright

Copyright © 2024 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  trademarks are owned by Ruijie Networks.

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

Disclaimer

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

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

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Intended Audience

This document is intended for:

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

Technical Support

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


Conventions


1. GUI Symbols


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

2. Signs

The signs used in this document are described as follows:


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

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

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

 Note

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

 Specification

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

3. Note

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

Contents

Preface	I
1 Product Overview	1
1.1 Overview	1
1.2 Product Characteristics.....	1
1.3 Hardware Description	2
1.3.1 RG-WALL 1600-Z3200-S Panels.....	2
1.3.2 RG-WALL 1600-Z5100-S Panels.....	4
1.4 Specifications.....	6
1.4.1 RG-WALL 1600-Z3200-S Specifications	6
1.4.2 RG-WALL 1600-Z5100-S Specifications	7
2 Device Management	9
2.1 Logging In to the Device	9
2.1.1 Logging In to the Device from the Web	9
2.1.2 Logging In to the Device from the Console	15
2.1.3 Logging In to the Device Using SSH	19
2.2 Modifying the Web Login Configuration	22
2.3 Account Permission Settings.....	24
2.3.1 Administrator Permission Overview	24
2.3.2 Enabling Default Accounts.....	24
2.3.3 Creating an Administrator	25
2.3.4 Changing the Password.....	30
2.4 Configuration Backup and Restoration.....	33
2.4.1 Exporting the Configuration	33

2.4.2 Importing the Configuration	34
2.5 Defaults Restoration	35
2.5.1 Web-based One-Click Restoration	36
2.5.2 Restoration by Pressing the Reset Button.....	36
2.6 Password Restoration.....	37
2.7 SNMP Management	40
2.7.1 Overview	40
2.7.2 Configuring SNMP	41
3 License Activation.....	45
3.1 Authorization Service Overview.....	45
3.2 Ruijie Secure Cloud Platform.....	45
3.2.1 Overview	45
3.2.2 Operations on Ruijie Secure Cloud Platform.....	46
3.2.3 License Activation Methods	64
3.3 Precautions for License Activation	67
4 Configuring the Syslog Server	69
5 Signature Library Upgrade.....	71
5.1 Configuring Automatic Upgrade	71
5.2 Local Manual Upgrade.....	72
5.3 Online Automatic Upgrade.....	73
6 Version Upgrade.....	75
6.1 Overview	75
6.2 Upgrade Operations	76
6.2.1 Offline Upgrade	76

6.2.2 Online Upgrade	77
6.2.3 Version Rollback	77
7 Configuration Examples for Typical Scenarios	79
7.1 Integrated Deployment on Ruijie Cloud.....	79
7.1.1 Firewall Deployment (Routing Mode)	79
7.1.2 NBR Deployment (Transparent Mode)	84
7.1.3 Deployment Using Ruijie Cloud App (Routing Mode).....	89
7.1.4 Deployment Using Ruijie Cloud App (Transparent Mode).....	98
7.2 Transparent Mode.....	107
7.2.1 Preparations.....	107
7.2.2 Deployment in Transparent Mode (Quick Deployment)	108
7.2.3 Out-of-Band Management in Transparent Mode (Custom Deployment)	112
7.2.4 Multi-bridge Deployment Mode.....	118
7.2.5 Precautions for Deploying Transparent Bridge Mode	125
7.2.6 Configuring a Bridge Interface	125
7.3 Routing Mode.....	129
7.3.1 Preparations.....	129
7.3.2 Single-Line Onboarding (Quick Deployment).....	130
7.3.3 Single-Line Onboarding (Custom Deployment).....	134
7.4 Off-Path Mode.....	157
7.4.1 Preparations.....	157
7.4.2 Deployment in Off-Path Mode (Quick Deployment)	158
7.4.3 Configuring an Off-Path Interface (Custom Deployment)	161
7.4.4 Precautions for Deploying Off-Path Mode	164

8 Common Operations	165
8.1 NAT Policy	165
8.1.1 NAT Technology	165
8.1.2 Application Scenario	168
8.1.3 Configuring Destination Address Translation (One-to-One Port Mapping)	169
8.1.4 Configuring Bidirectional Address Translation (Allowing Intranet PCs to Access the Map Server by Using a Public Network Address).....	173
8.1.5 Configuration Example of Static NAT-PT Networking	178
8.1.6 Configuration Example of Dynamic NAT-PT Networking	185
8.1.7 Configuration Example of Stateless NAT64 Networking	192
8.1.8 Configuration Example of Static NAT64 Networking	199
8.1.9 Configuration Example of Dynamic NAT64 Networking	205
8.1.10 Configuration Example of NAT66-Source NPTv6 Networking	211
8.1.11 Configuration Example of NAT66-Destination NPTv6 Networking.....	216
8.2 Port Mapping Policy	221
8.2.1 Overview	221
8.2.2 Configuring a Port Mapping Policy	221
8.3 Security Defense.....	224
8.3.1 Principle and Application Scenario	224
8.3.2 DoS/DDoS Attack Defense	228
8.3.3 Intrusion Prevention	234
8.3.4 Virus Protection.....	238
8.3.5 ARP Attack Defense.....	240
8.3.6 Local Defense	243
8.3.7 Session Suppression	247

8.3.8 Threat Intelligence	254
8.4 Content Identification Library	264
8.4.1 Configuring a Keyword Set	264
8.4.2 URL Category	265
8.5 URL Filtering	268
8.5.1 Custom URL Filtering Template	268
8.5.2 Predefined URL Filtering Template	270
8.5.3 Configuration Examples of Blocking Websites	272
8.6 Keyword Filtering	283
8.7 Behavior Analysis	285
8.8 Configuring HTTP Packet Resolution	291
8.9 Configuring SSL Proxy Policies	291
8.9.1 Overview	291
8.9.2 Configuring an SSL Proxy Template	292
8.9.3 Importing Certificate	293
8.9.4 Configuring an SSL Proxy Policy	297
8.9.5 Allowlist	301
8.10 Port Scan	303
8.11 Traffic Learning	308
8.12 Security Policy	312
8.12.1 Overview	312
8.12.2 Configuring Security Policy (Using Wizard)	314
8.12.3 Configuring Security Policy (Manual)	323
8.12.4 Adjusting Policy Order	328

8.12.5 Optimizing Policy	329
8.12.6 Policy Lifecycle Management	330
8.12.7 Simulation Run.....	331
8.12.8 Importing Security Policies in a Batch	333
8.12.9 Exporting Security Policies	335
8.12.10 Enabling Basic Protocol Packet Control.....	336
8.12.11 Configuration Examples of DHCP + Security Policies.....	337
8.13 Traffic Control Policy.....	347
8.13.1 Overview	347
8.13.2 Configuring Traffic Control Policies.....	347
8.14 DHCP Management.....	353
8.14.1 Overview	353
8.14.2 Configuring a DHCP Server.....	354
8.14.3 Address Management List	359
8.15 Blocklist and Allowlist.....	360
8.15.1 Overview	360
8.15.2 Precautions	360
8.15.3 Creating an IPv4 Allowlist	361
8.15.4 Creating an IPv6 Allowlist	363
8.15.5 Creating an IPv4 Blocklist.....	364
8.15.6 Creating an IPv6 Blocklist.....	366
8.15.7 Creating a Temporary IPv4 Blocklist.....	367
8.15.8 Creating a Temporary IPv6 Blocklist.....	368
8.16 Security Rule Base Management	370

8.17 Connecting to Ruijie Cloud	371
8.17.1 Overview	371
8.17.2 Connecting to Ruijie Cloud	371
8.17.3 Operations on Ruijie Cloud.....	372
8.18 DNS Server.....	377
8.18.1 Configuring DNS	377
8.18.2 Configuring DNS Transparent Proxy	378
8.18.3 Configuring DDNS	386
8.19 Intelligent Routing	388
8.20 Address Library Routing (ISP-based Routing).....	393
8.20.1 Overview	393
8.20.2 Configuring an ISP Address Library	393
8.20.3 Configuring ISP Routing	398
8.20.4 Viewing the Routing Table of Address Library	401
8.21 Link Aggregation	402
8.22 Link Detection	407
8.23 Outbound Interface Load Balancing	411
8.23.1 Overview	411
8.23.2 Configuring MLLB Based on Uplink Bandwidth for a Network with Specific Routes.....	412
8.23.3 Configuring MLLB Based on Uplink Bandwidth for DNS Transparent Proxy	419
8.23.4 Configuring MLLB Based on Link Priority for Intelligent Routing	427
8.23.5 Configuring MLLB Based on Bandwidth and Sessions for a Network with Specific Routes.....	433
8.23.6 Common Faults Diagnosis.....	440
8.24 SSL VPN.....	440

8.24.1 Overview	440
8.24.2 Application Scenario	441
8.24.3 Typical Configuration of Egress Deployment for Remote Office (Local Authentication) 442	
8.24.4 Typical Configuration of Deployment on the Intranet Side of a NAT Device for Remote Office (Local Authentication).....	452
8.24.5 Typical Configuration of Off-Path Deployment Mode (Local Authentication)	462
8.24.6 Typical Configuration of SSL VPN Access Using a Domain Name over Multiple Lines (Local Authentication)	475
8.24.7 Typical Configuration of RADIUS Authentication Access	486
8.24.8 Typical Configuration of SMS Two-Factor Authentication (Twilio).....	497
8.24.9 Common Faults and Troubleshooting Roadmaps	509
8.25 IPsec VPN.....	514
8.25.1 Overview	514
8.25.2 Principles.....	514
8.25.3 Application Scenario	515
8.25.4 Configuration Examples of Site-to-Site IPsec VPN	517
8.25.5 Configuration Examples of Site-to-Site IPsec VPN (Interconnection with Fortinet Firewall)	538
8.25.6 Configuration Examples of Site-to-Multisite IPsec VPN.....	548
8.25.7 Configuration Examples of Site-to-Multisite IPsec VPN (Interconnection with Fortinet Firewall)	567
8.25.8 Configuration Examples of IPsec VPN with NAT Traversal.....	575
8.25.9 Configuration Examples of IPsec VPN Networking with Link Redundancy	598
8.25.10 Common Faults and Troubleshooting Roadmaps	611

8.26 GRE VPN	613
8.26.1 Overview	613
8.26.2 Working Principle	613
8.26.3 Application Scenario	614
8.26.4 Configuring an IPv4 over IPv4 GRE Tunnel	615
8.26.5 Configuring an IPv6 over IPv4 GRE Tunnel	628
8.26.6 Configuring GRE over IPsec.....	639
8.26.7 Common Fault Diagnosis	656
8.27 VRRP	656
8.27.1 Overview	656
8.27.2 Working Process.....	656
8.27.3 Configuring a VRRP Group	657
8.27.4 Viewing VRRP Logs.....	659
8.28 Web Authentication.....	660
8.28.1 Application Scenario	660
8.28.2 Limitations	661
8.28.3 Configuration Example of Local Portal Authentication	662
8.28.4 Configuration Example of External Portal Authentication.....	668
8.28.5 Common Faults and Troubleshooting Roadmap.....	673
8.29 Overload Protection	674
8.30 Information Push.....	675
8.30.1 Overview	675
8.30.2 Setting the Logo Image.....	675
8.30.3 Editing Text Information	677

8.31 Subinterface.....	680
8.31.1 Overview	680
8.31.2 Configuration Examples of VLAN Interconnection on Sub-interfaces.....	680
8.32 Bridge Interface.....	683
8.32.1 Overview	683
8.32.2 Configuration Examples of Layer-2 Transparent Transmission	683
9 Routine Maintenance	688
9.1 Checking Indicators on the Hardware Device Panel.....	688
9.2 Checking Basic Configurations.....	691
9.3 Log Monitoring	692
9.3.1 Querying System Logs.....	692
9.3.2 Querying Security Logs.....	693
9.3.3 Querying Keyword Filter Logs	695
9.3.4 Querying Behavior Analysis Logs.....	696
9.3.5 Querying Session Logs.....	696
9.3.6 Querying Operation Logs.....	697
9.4 Traffic Monitoring	698
9.4.1 Interface Traffic	698
9.4.2 Real-Time Traffic.....	699
9.4.3 Traffic Statistics	702
9.4.4 Session Number Monitoring	703
9.5 Session Monitoring	703
9.5.1 Overview	703
9.5.2 Session Change Trend	704

9.5.3 Real-Time Session Information	705
9.6 Intelligence Overview.....	707
10 Advanced Features	710
10.1 ALG	710
10.1.1 Overview	710
10.1.2 Configuring ALG.....	710
11 FAQs.....	712
11.1 Product Knowledge.....	712
11.1.1 What Is the Hardware Architecture of the RG-WALL 1600-Z-S Series Firewall? ...	712
11.1.2 What Are the Restrictions of Port MGMT?.....	712
11.2 Firewall Deployment	712
11.2.1 What Firewall Deployment Modes Are Supported?.....	712
11.2.2 Can GE Optical Port and 10GE Optical Port Form a Bridge?.....	715
11.3 Typical Feature Configuration	715
11.3.1 How Is Source NAT Implemented?.....	715
11.3.2 Does the Firewall Support Link Detection?.....	715
11.3.3 Does the Z-S Series Firewall Block TCP Sessions in the Secondary Traversal Scenario?.....	715
11.3.4 Does the Firewall Support Link Aggregation?	716
11.4 Login Management.....	716
11.4.1 What Can I Do If I Fail to Log In to the Web Page?	716
11.4.2 What Can I Do If I Fail to Log In to the System Through SSH?	716
11.5 O&M and Monitoring.....	717
11.5.1 How Do I View the CPU, Memory, and Hard Disk Information of the Firewall?.....	717
11.5.2 How Do I View the Interface Traffic of the Firewall?.....	717

12 Troubleshooting.....	718
12.1 Security Policy	718
12.1.1 Principle	718
12.1.2 Configuration Points of Security Policies.....	718
12.2 Data Packet Processing	719
12.3 Diagnostic Center	720
12.3.1 Network Connectivity Diagnosis	720
12.3.2 IPsec VPN Diagnosis.....	723
12.3.3 SSL VPN Fault Diagnosis	727
12.4 Packet Obtaining.....	731
12.5 Device Self-Test.....	734
12.5.1 Device Self-Test	734
12.5.2 Hardware Self-Test	736
12.6 One-Click Fault Information Collection	737
12.7 Data Flow Diagnosis	738
12.7.1 Packet Statistics Collection.....	738
12.7.2 Flow Status	741
12.7.3 Packet Tracing	743
13 Running Status Check After Product Implementation	746
13.1 Checking the Software Version	746
13.2 Checking the Management Mode.....	747
13.3 Checking Firewall Policies	750
13.4 Checking the Operation Status.....	750
13.5 Checking the System Status.....	751

13.6 Checking the Log Status.....	752
13.7 Checking the Network Connectivity.....	753
13.8 Checking the Service Use Status	754

1 Product Overview

1.1 Overview

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

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

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

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

1.2 Product Characteristics

- Easy configuration

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

- Intelligent policy manager

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

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

- App identification and control

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

- Diversified security defense

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

- High stability and reliability

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

- Flexible expansion

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

- Easy cloud-based O&M

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

1.3 Hardware Description

1.3.1 RG-WALL 1600-Z3200-S Panels

1. Front Panel

Figure 1-1 Front Panel

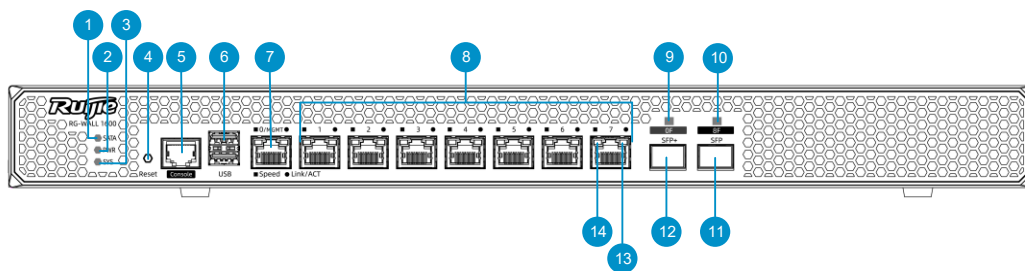


Table 1-1 Components on the Front Panel

No.	Component	Description
1	SATA hard disk status LED (SATA)	<ul style="list-style-type: none"> ● Steady green: A hard disk is connected. ● Blinking green: Data is being read or written.
2	Power module status LED (PWR)	<ul style="list-style-type: none"> ● Steady green: The power supply is normal. ● Off: The power supply is cut off or fails.

No.	Component	Description
3	System status LED (SYS)	<ul style="list-style-type: none"> ● Blinking green: The device is powered on and being initialized. ● Steady green: Initialization is complete. ● Steady red: An alarm is generated.
4	Reset button	<ul style="list-style-type: none"> ● Restarting the device: Press the button for less than 3 seconds. ● Restoring factory settings: Press the button for more than 5 seconds. <p>When you perform either of the preceding operations, device status information is collected. After the device restarts, you can access the web UI of the firewall, choose System > One-Click Collection, and download the information.</p>
5	Console port	<p>It is used to connect to the console for device maintenance and diagnosis.</p> <p>Note:</p> <ul style="list-style-type: none"> ● When the console port is used, set the baud rate to 115,200 bps, data bit to 8, and stop bit to 1, and disable parity check and data flow control. ● The console port is used only in special scenarios. For details, contact technical support personnel.
6	USB port	Two USB 2.0 ports can be used to connect USB drives.
7	MGMT port	It is used to access the device management page upon first login.
8	10/100/1000BASE-T ports	Ports 1 to 7, which are used to connect Ethernet cables.
9	10GE SFP + port LED	<ul style="list-style-type: none"> ● Steady green: The port is connected. ● Blinking green: The port is receiving or sending data. ● Off: The optical port is incorrectly connected.
10	1GE SFP port LED	<ul style="list-style-type: none"> ● Steady green: The port is connected. ● Blinking green: The port is receiving or sending data. ● Off: The optical port is incorrectly connected.
11	1GE SFP port	Port 8F. For details about optical modules that support this port, see Table 1-5 .
12	10GE SFP+ port	Port 0F. For details about optical modules that support this port, see Table 1-5 .
13	Link/ACT status LEDs (square) of 10/100/1000BASE-T ports	<ul style="list-style-type: none"> ● Steady green: The port is connected. ● Blinking green: The port is receiving or sending data. ● Off: The port is incorrectly connected.

No.	Component	Description
14	Speed LEDs (round) of 10/100/1000BASE-T ports	<ul style="list-style-type: none"> Steady orange: Gbit/s port speed Off: 100/10 Mbit/s port speed

2. Rear Panel

Figure 1-2 Rear Panel

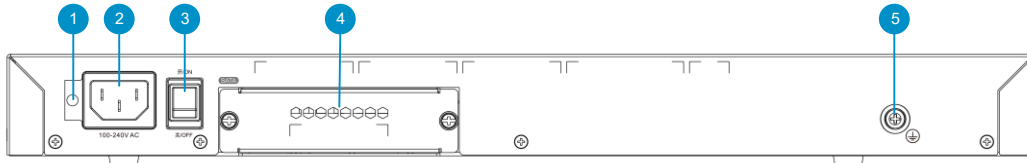


Table 1-2 Components on the Rear Panel

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

1.3.2 RG-WALL 1600-Z5100-S Panels

1. Front Panel

Figure 1-3 Front Panel

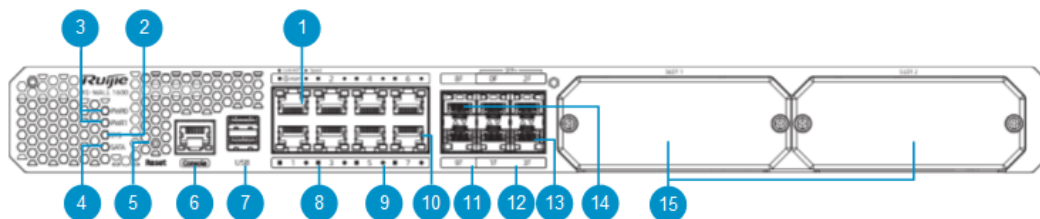


Table 1-3 Components on the Front Panel

No.	Component	Description
1	MGMT port	It is used to access the device management page upon first login.
2	System status LED (SYS)	<ul style="list-style-type: none"> Blinking green: The device is powered on and being initialized, or the system is restoring factory settings. Solid green: Initialization is complete. Solid red: An alarm is generated.
3	Power module status LEDs (PWR0 and PWR1)	<ul style="list-style-type: none"> Solid green: The power module is operating normally. Solid red: The power module is not functioning properly, or the power module is installed but no power cord is connected. Off: No power supply is connected.
4	SATA hard disk status LED (SATA)	Solid green: A hard disk is connected. Blinking green: Data is being read or written.
5	Reset button	<ul style="list-style-type: none"> Restarting the device: Press the button for less than 5 seconds. Restoring factory settings: Press the button for more than 5 seconds. When you perform either of the preceding operations, device status information is collected. After the device starts, you can log in to the web UI of the firewall, choose System > One-Click Collection , and download device status information.
6	Console port	It is used to connect to the console for maintenance and diagnosis. Note: <ul style="list-style-type: none"> When the console port is used, set the baud rate to 115,200 bps, data bit to 8, and stop bit to 1, and disable parity check and data flow control. The console port is used only in special scenarios. For details, contact technical support personnel.
7	USB port	Two USB 2.0 ports can be used to connect USB flash drives.
8	Link/ACT status LEDs (square) of 10/100/1000BASE-T ports	<ul style="list-style-type: none"> Solid green: The link on the port is Up. Blinking green: The port is receiving or sending data. Off: No link is established on the port.
9	Speed LEDs (round) of 10/100/1000BASE-T ports	<ul style="list-style-type: none"> Solid orange: Gbps port speed Off: 100/10 Mbps port speed
10	10/100/1000BASE-T ports	Ports 1 to 7, which are used to connect Ethernet cables.
11	1GE SFP port LEDs	<ul style="list-style-type: none"> Solid green: The port is connected. Blinking green: The port is receiving or sending data.
12	10GE SFP + port LEDs	<ul style="list-style-type: none"> Solid green: The port is connected. Blinking green: The port is receiving or sending data.
13	10GE SFP+ ports	Ports 0F to 3F
14	1GE SFP ports	Ports 8F and 9F
15	Module slots	Expansion module slots

2. Rear Panel

Figure 1-4 Rear Panel

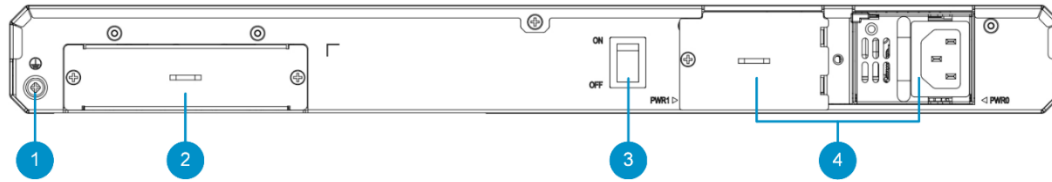


Table 1-4 Components on the Rear Panel

No.	Item	Description
1	Grounding terminal	Used to ground the device to ensure electrical safety.
2	Hard disk slot	Used to install a hard disk.
3	Power switch	Used to power on or power off the device.
4	Power module	Used to connect an AC power cord. Two power modules can be installed.

1.4 Specifications

1.4.1 RG-WALL 1600-Z3200-S Specifications

Table 1-5 Specifications

Model	RG-WALL 1600-Z3200-S
Memory	4 GB DDR4 memory
Boot ROM	8 MB
eMMC	8 GB
Hard Disk	No hard disk is provided in factory delivery. 1 TB HDD or 240 GB/480 GB solid state drive (SSD) can be installed as required.
Hard Disk Hot Swapping	Not supported
Fixed Service Port	<ul style="list-style-type: none"> 8 x 10/100/1000BASE-T ports (10BASE-T/100BASE-TX/1000BASE-TX): support 10/100/1000 Mbps auto-negotiation and auto MDI/MDIX. Port 0 is the default MGMT port. 1 x 1GE SFP port (1000Base-SX/LX/ZX): supports 1000BASE-SX/LX/ZX mini GBIC and GE-SFP-LX20/LH40-BIDI optical transceivers.

	<ul style="list-style-type: none"> 1 x 10GE SFP+ port (1000Base-X/10GBase-R): supports XG-SFP-SR-MM850, XG-SFP-LR-SM1310, and XG-SFP-ER-SM1550 optical transceivers, as well as BIDI optical transceivers.
Fixed Management Port	1 x RJ45 MGMT port (reusing Ge0/0)
	1 x RJ45 console port (RS-232)
USB Port	2 x USB 2.0 ports
Bypass Port	Not supported
Expansion Module	Not supported
Dimensions (W x D x H)	440 mm × 200 mm x 43.6 mm (17.32 in. x 7.87 in. x 1.72 in.; without rubber pads)
Rated Input Voltage	100 V AC to 240 V AC, 50 Hz to 60 Hz
Rated Input Current	0.65 A
Maximum Power Consumption	25 W
Temperature	Operating temperature: 0°C to 45°C (32°F to 113°F)
	Storage temperature: -40°C to +45°C (-40°F to +113°F)
Humidity	Operating humidity: 10% RH to 90% RH (non-condensing)
	Storage humidity: 5% RH to 95% RH (non-condensing)

1.4.2 RG-WALL 1600-Z5100-S Specifications

Table 1-6 Specifications

Model	RG-WALL 1600-Z5100-S
Memory	4 GB DDR4 memory (ECC supported)
eMMC	8 GB
Hard Disk	No hard disk for factory delivery. A 1 TB hard disk drive (HDD) can be added.
Hot Swapping of Hard Disk	Not supported.
Fixed Service Port	<ul style="list-style-type: none"> 8 x 10/100/1000BASE-T ports (10BASE-T/100BASE-TX/1000BASE-TX) 2 x 1GE SFP ports (1000BASE-SX/LX/ZX) 4 x 10GE SFP+ ports (1000BASE-X/10GBASE-R)
Fixed Management Port	<ul style="list-style-type: none"> 1 x RJ45 MGMT port (reusing Ge0/0) 1 x RJ45 console port (RS-232)
USB Port	2 x USB 2.0 ports

Bypass Port	Not supported
Module Slot	2 x expansion module slots (expansion modules not supported) 2 x power module slots. 1 x hard disk slot.
Power Module	2 x pluggable power modules (RG-NSEC-PA70I), one power module for factory delivery.
Hot Swapping of Power Module	The two power modules support hot swapping.
Dimensions (W x D x H)	440 mm x 300 mm x 43.6 mm (17.32 in. x 11.81 in. x 1.72 in.)
Rated Input Voltage	100 V AC to 240 V AC, 50 Hz to 60 Hz
Rated Input Current	2 A (maximum)
Power Consumption	< 60 W
Temperature	<ul style="list-style-type: none"> ● Operating temperature: 0°C to 45°C (32°F to 113°F) ● Storage temperature: -40°C to +70 °C (-40°F to +158°F)
Humidity	<ul style="list-style-type: none"> ● Operating humidity: 40% to 65% RH (non-condensing) ● Storage humidity: 10% to 90% RH (non-condensing)

2 Device Management

2.1 Logging In to the Device

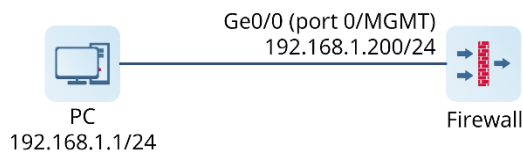
2.1.1 Logging In to the Device from the Web

Application Scenario

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

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

Network Topology



Prerequisites

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

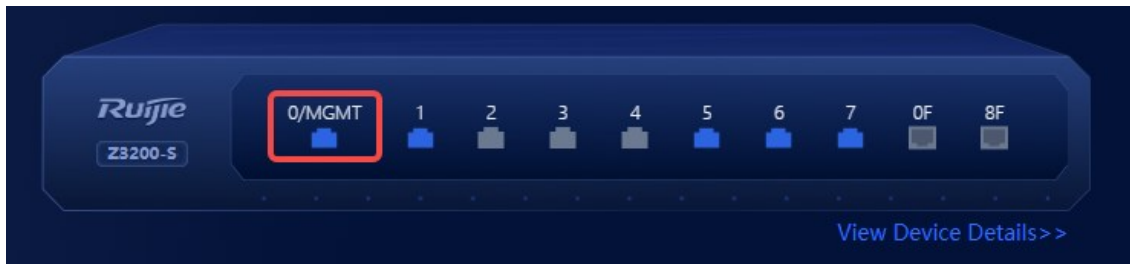
Table 2-1 Default Web Configurations

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

Note

- If the address of port 0/MGMT on the firewall is modified but you forget the address, you can access the Command Line Interface (CLI) to view the current configuration. For details, see [2.1.2 Logging In to the Device from the Console](#).
- If you change the password and forget it, restore the initial password. For details, see [2.6 Password Restoration](#).

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



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

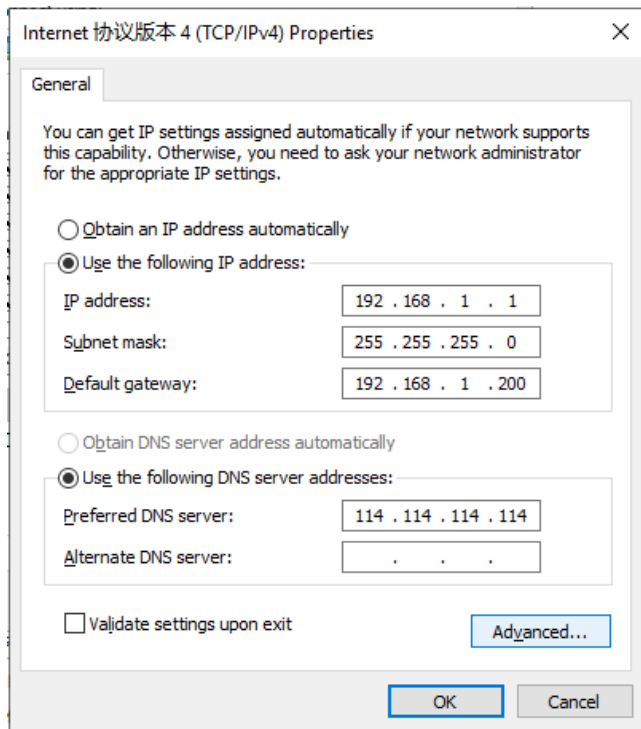
Configuration Points

- (1) Set the IP address of the management PC to one in the same network segment as the IP address of port 0/MGMT.
- (2) Log in to the web management page.
- (3) Configure the Ge0/1 port and enable the management functions on the port. By default, IP addresses or access management functions such as HTTPS are not configured for other ports except 0/MGMT.

Procedure

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

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

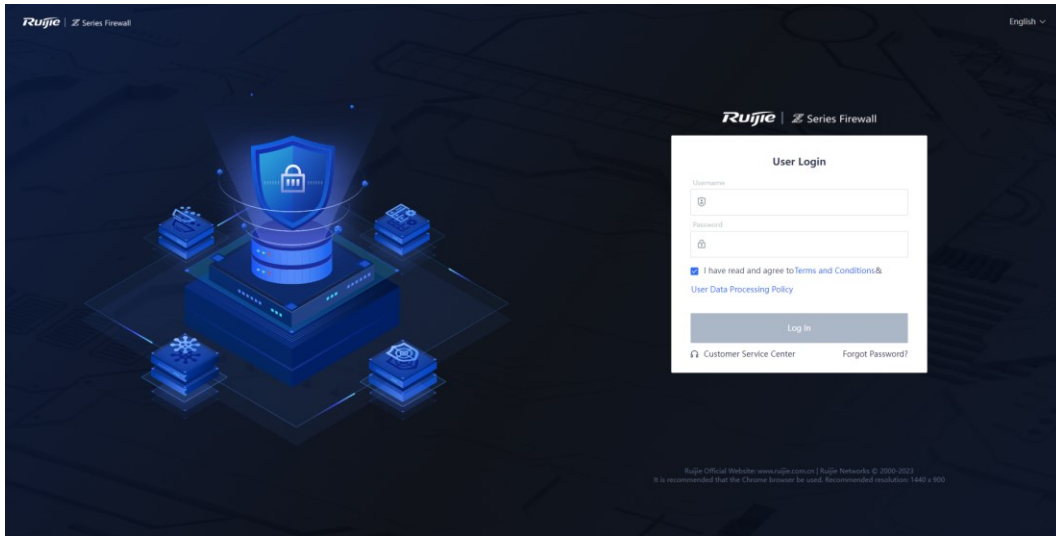


(2) Log in to the web management page.

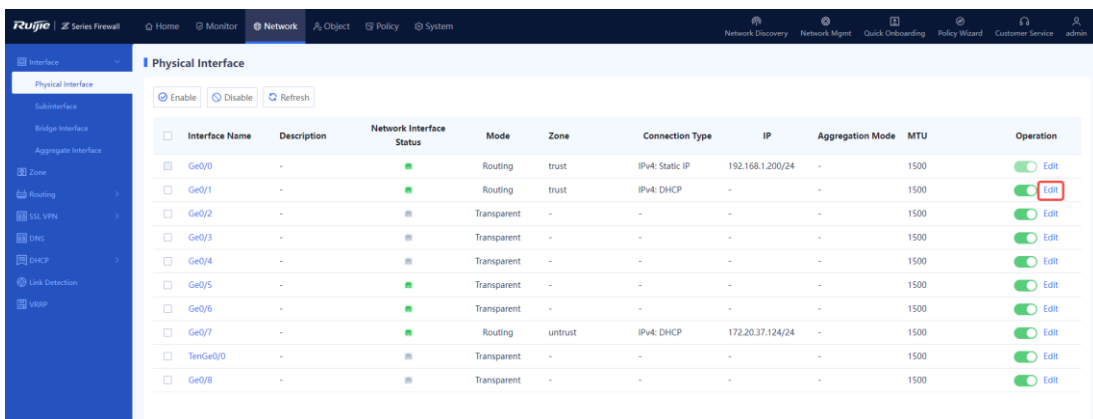
i Note

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

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



- (4) (Optional) If you log in to the web management page for the first time, the system forces you to change the default password of the Super Admin.
- (5) Set the IP address of the Ge0/1 port to 192.168.0.200/24 and enable the management functions on the Ge0/1.
 - a Choose **Network > Interface > Physical Interface**.



- b Select **Ge0/1** and click **Edit**.
- c Configure attributes of Ge0/1.

< Back
Edit Physical Interface

Basic Info

Interface Name

Description

Connection Status Enable Disable

Mode Routing Mode Transparent Mode Off-Path Mode

* Zone [Add Security Zone](#)

Interface Type WAN Interface LAN Interface

Address

IP Type IPv4 IPv6

Connection Type Static Address DHCP PPPoE

* IP/Mask

* Next-Hop Address

Default Route

Line Bandwidth

Uplink

Downlink

Access Management

Permit HTTPS PING SSH

Advanced

ISP Address Library

ⓘ MTU

MAC

Link Detection

Item	Description	Remarks
IP/Mask	IP address of the physical interface.	[Example] 192.168.0.200/24

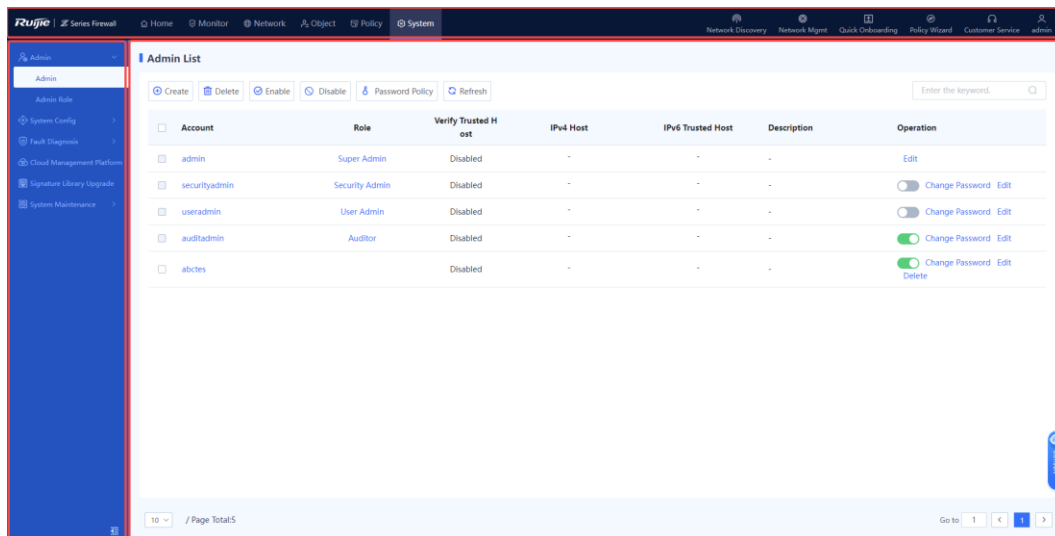
Item	Description	Remarks
Access Management	<p>Whether the interface supports HTTPS, ping, and SSH.</p> <ul style="list-style-type: none"> ● HTTPS: Allows users to access the device using <code>https://Interface IP address</code>, such as <code>https://192.168.0.200</code>. ● PING: Allows users to ping the interface address. If this option is not selected, ping fails even if there is a reachable route. ● SSH: Allows users to access the device by creating an SSH connection with the interface IP address that is used as the destination address, such as <code>ssh 192.168.0.200</code>. 	<p>The configuration takes effect when local defense is enabled on the device.</p> <p>[Example] Select HTTPS.</p>

d Click **Save**.

Follow-up Procedure

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

Figure 2-1 Web Management Page Layout



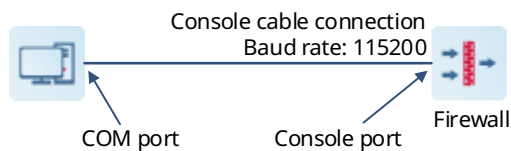
Area	Description
Mark and panel area	<ul style="list-style-type: none"> ● This area displays the company logo, device name, and function panel. ● This area supports new network discovery, network-wide management, quick onboarding, policy configuration wizard, and customer service, helping users quickly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

2.1.2 Logging In to the Device from the Console

Application Scenario

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

Network Topology



Tool Preparation

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



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



- PC with a COM port: The COM port of the PC is usually located near the display interface on the rear panel of the chassis. The COM port has nine pins, as shown in [Figure 2-2](#).
If your PC does not have a COM port (such as the laptop), the USB-to-COM cable (as shown in [Figure 2-3](#)) must be connected to the USB port to convert it into the COM port. You can also use the USB-to-console (RJ45) cable of [Model 2](#) directly.

Figure 2-2 COM port



Figure 2-3 USB-to-COM Cable

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

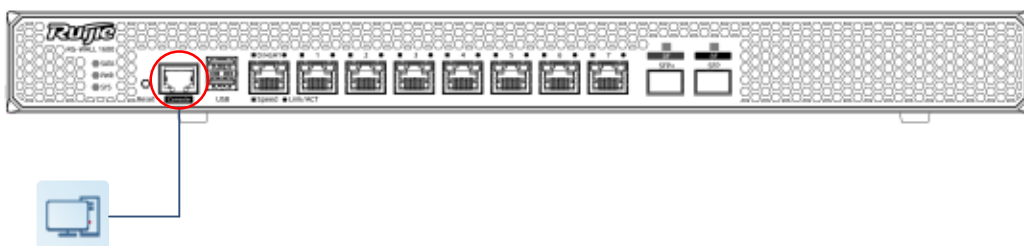
Configuration Points

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

Connect the RJ45 connector of the configuration cable to the console port of the device and the other end to the COM port of the PC.
- (3) Run the terminal simulation software to log in to the device.

Procedure

- (1) Connect the configuration cable.
 - a Insert the RJ45 connector of the console cable to the console port of the device (as shown in the following figure).
 - b Insert the DB9 connector on the other end of the console cable to the 9-pin COM port of the PC.



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

Note

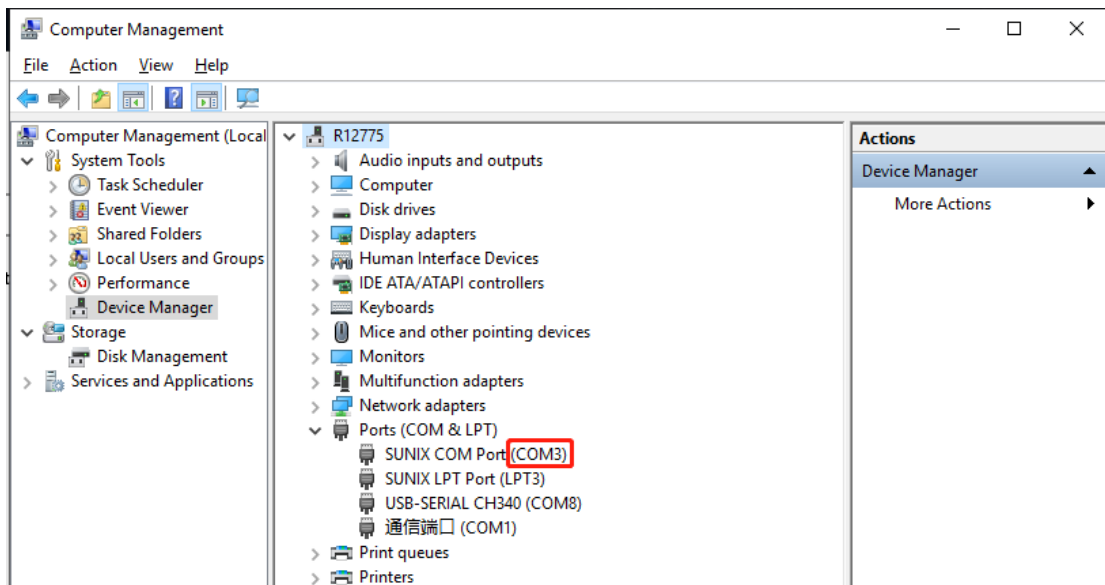
This section uses SecureCRT as an example. For details about other programs, see the corresponding operation manual.


- a View identified COM ports on the PC.

Note

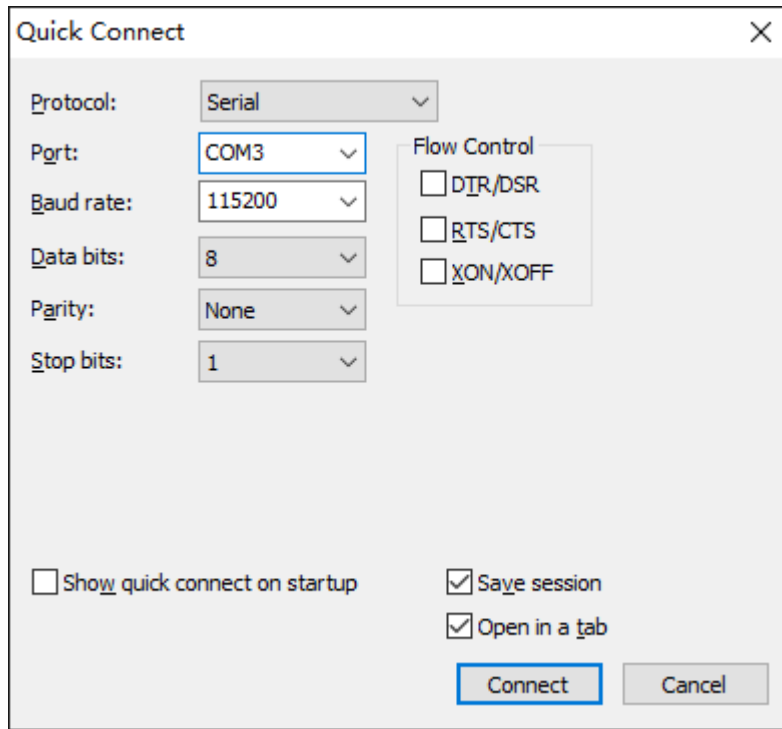
If a PC has only one COM port, it is displayed as COM1 by default. In this case, skip this step.

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



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

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



Configuration Verification

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

Note

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


Caution

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

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

```
Sent SIGKILL to all processes
Switching rootfs

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

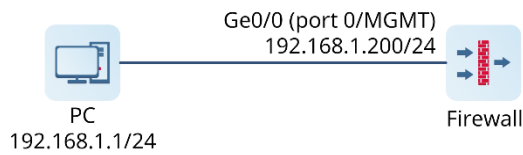


2.1.3 Logging In to the Device Using SSH

Application Scenario

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

Network Topology



Configuration Points

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

- (1) Enable the SSH function on the interface.
- (2) Manage the device using SSH.

Procedure

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

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

Edit Physical Interface

Basic Info

Interface Name: Ge0/0

Description:

Connection Status: Enable Disable

Mode: Routing Mode Transparent Mode Off-Path Mode

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

Interface Type: WAN Interface LAN Interface

Address

IP Type: IPv4 IPv6

Connection Type: Static Address DHCP PPPoE

* IP/Mask: 192.168.1.200/24

Line Bandwidth

Uplink:

Downlink:

Access Management

Permit HTTPS PING SSH

Advanced

MTU: 1500

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

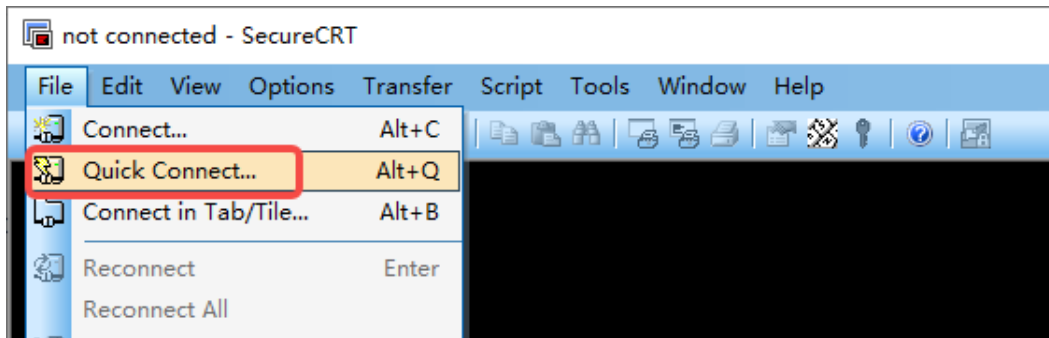
- b In the **Access Management** area, select **SSH** (ping function disabled on the interface by default) and click **Save**.

(2) Manage the device using SSH.

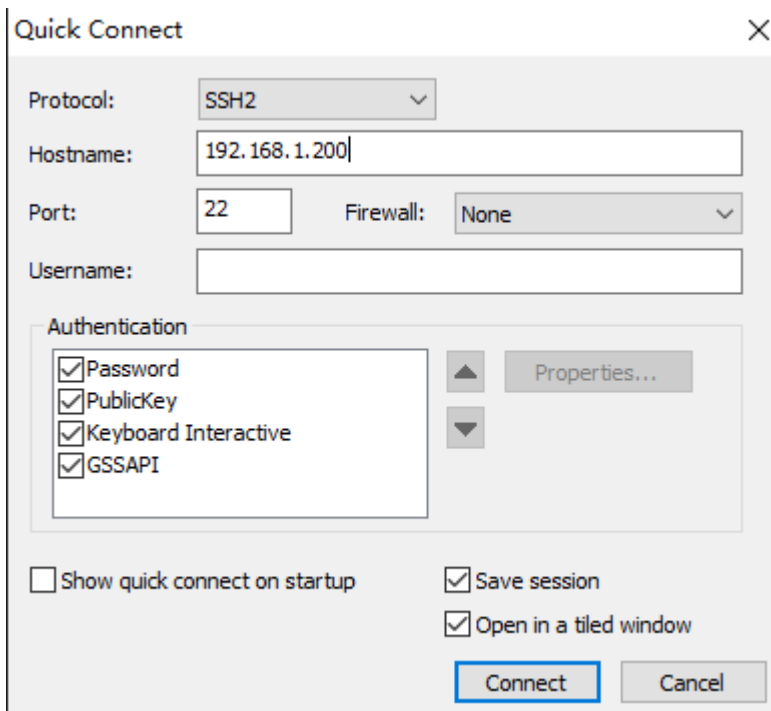
Create an SSH connection using the terminal simulation software (such as SecureCRT), and enter the username and password (for login to the web management page) to manage the device.

The following uses the SecureCRT software as an example.

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



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



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

2.2 Modifying the Web Login Configuration

Application Scenario

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

Procedure

- (1) Choose System > System Config > Service Parameters and click the Web tab.
- (2) Customize the web service configuration.

The screenshot displays the 'Web' configuration page for a device. It features a navigation bar with 'Web', 'SSH', and 'Advanced Settings' tabs. The 'Web' tab is active. The configuration area includes several input fields and a checkbox:

- Device Name:** Z3200-s
- * HTTPS Port:** 443
- * Login Timeout Period (min):** 1440
- * Allowed Consecutive Login Failures:** 6
- * Lockout Period (min):** 3
- Auto Redirection for HTTP:**
- Verification Code:** Enable Disable

At the bottom, there are two buttons: a blue 'Save' button and a white 'Restore Defaults' button.

Item	Description	Remarks
Device Name	Name of the device. In integrated deployment on Ruijie Cloud, you can view the modified device name on the Ruijie Cloud platform and master device. For details about integrated deployment on Ruijie Cloud, see 7.1 Integrated Deployment on Ruijie Cloud .	[Example] RG-WALL
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	Period of time within which if no operation is performed after login to the web management page. The system displays a prompt of login timeout when the administrator tries to log in to the web management page again.	<ul style="list-style-type: none"> ● Enter an integer in the range of 0 to 1440, in minutes. ● The default value is 30 minutes. [Example] 30
Allowed Consecutive Login Failures	Number of consecutive incorrect password attempts. If a user enters an incorrect password for a number of times exceeding the value specified by this parameter, the system automatically locks the user.	<ul style="list-style-type: none"> ● Enter an integer in the range of 0 to 10. ● The default value is 6. [Example] 3
Lockout Period	Period of time within which the automatically locked user is not allowed to log in to the web management page.	<ul style="list-style-type: none"> ● Enter an integer in the range of 0 to 30, in minutes. ● The default value is 3. [Example] 30
Verification Code	Whether a verification code is required for login to the web management page.	By default, the value is Enable . [Example] Enable

(3) Click **Save**.

2.3 Account Permission Settings

2.3.1 Administrator Permission Overview

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

Table 2-2 Permissions of the Default Roles

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

2.3.2 Enabling Default Accounts

Application Scenario

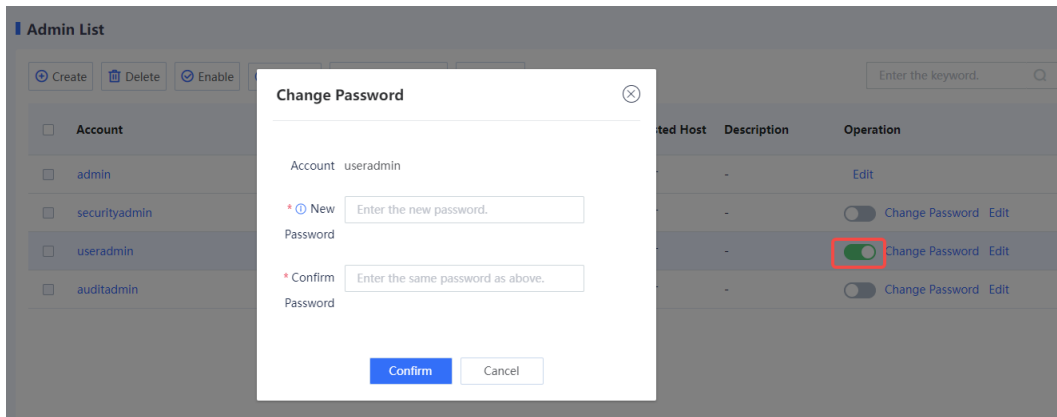
The system default administrator accounts **securityadmin**, **auditadmin**, and **useradmin** take effect after they are enabled and passwords are set for them.

Note

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

Procedure

- (1) Choose **System > Admin**.
The system displays the default accounts.
- (2) Select a default account to be enabled and set its status to **Enable**.
The **Change Password** dialog box is displayed.



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

Password description:

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

- (4) Click **Confirm**.

Follow-up Procedure

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

- The default administrator account cannot be deleted.

2.3.3 Creating an Administrator

1. Creating an Administrator Role

Application Scenario

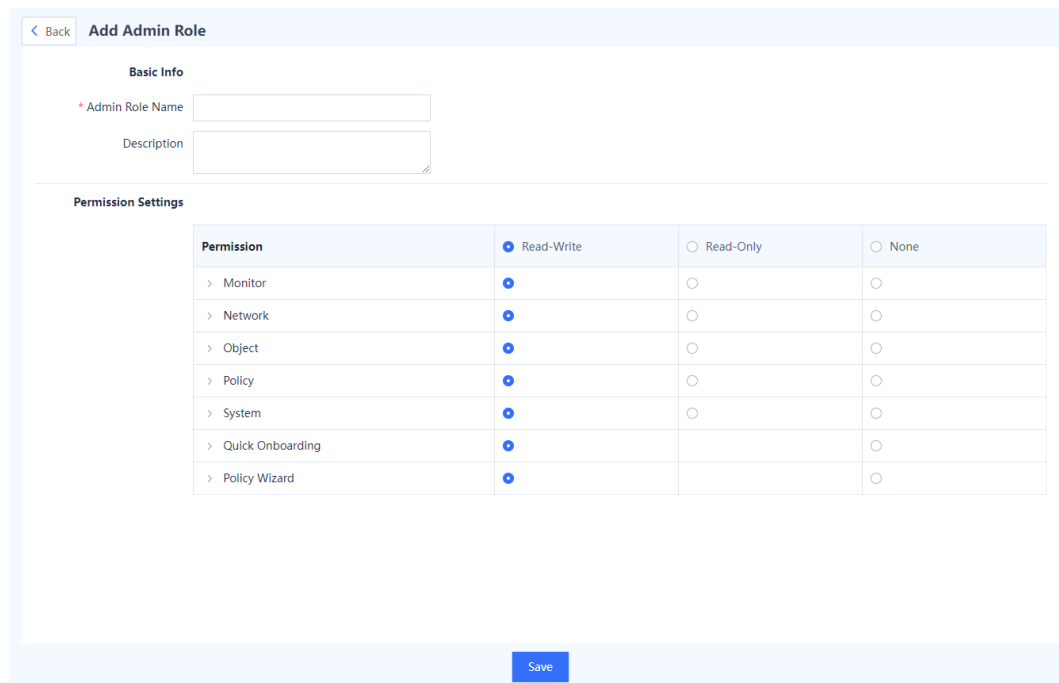
The user scenario grants different permissions to different roles to implement level- and rights-based management. You can customize administrator roles and grant permissions to the roles as required.

Procedure

- (1) Choose System > **Admin Role**.
- (2) In the operation area, click **Create**.



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



Item	Description	Remarks
Admin Role Name	Name of the role, which is used to identify the role.	[Example] Security Admin
Description	Description of the role, which distinguishes role permissions.	[Example] New
Permission Settings		

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

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

2. Creating an Administrator Account

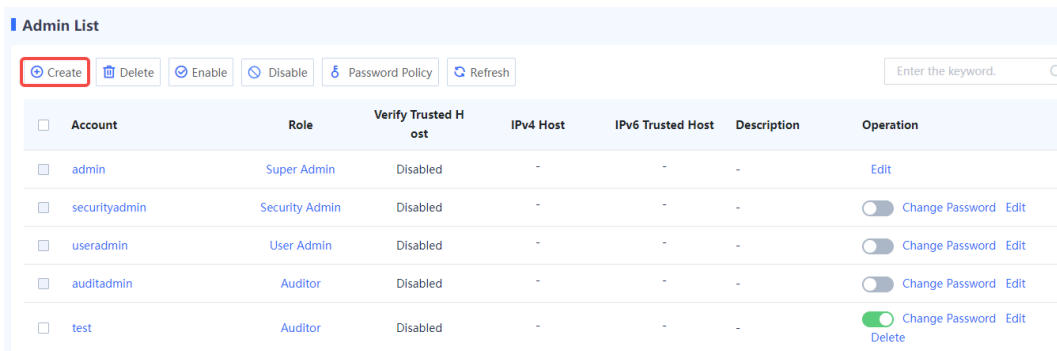
Application Scenario

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

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

Procedure

- (1) Choose **System > Admin**.
- (2) Above the operation area, click **Create**.



- (3) Set parameters for the new administrator.

< Back
Add Admin Account

Basic Info

* Account

* Enabled State Enable Disable

* Role

Description

Advanced

*

* Confirm Password

Configure Trusted Host

Restrict Trusted Host Login

① IPv4 Trusted Host 1 [Delete](#)

[+ Add IPv4 Trusted Host](#)

① IPv6 Trusted Host 1 [Delete](#)

[+ Add IPv6 Trusted Host](#)

① MAC Trusted Host 1 [Delete](#)

[+ Add MAC Trusted Host](#)

Save

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

Item	Description	Remarks
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		
Password	Password used by the new administrator to log in to the web UI.	<ul style="list-style-type: none"> ● A password must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. ● Chinese characters, spaces, and full-width characters are not allowed. ● The password is a string of 8 to 15 characters. ● The password cannot be the same as the username or the username in reverse order. [Example] admin@123
Confirm Password	Enter the login password again.	The value of Confirm Password must be the same as that of Password . [Example] admin@123
Configure Trusted Host		
Restrict Trusted Host Login	If this function is enabled, the account can only log in to the firewall using a specified IP address (trusted host).	[Example] Enable
IPv4 Trusted Host	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

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

2.3.4 Changing the Password

1. Modifying the Administrator Password Security Policy

Application Scenario

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

Procedure

- (1) Access the **Password Policy** page.
 - a Choose **System > Admin**.
 - b Above the operation area, click **Password Policy**.

Password Policy ⊗

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

Mandatory Password

Change

* Maximum Password Day
Age

- (2) Enable Mandatory Password Change.
- (3) Set Maximum Password Age.
- (4) Click **Submit**.

Follow-up Procedure

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

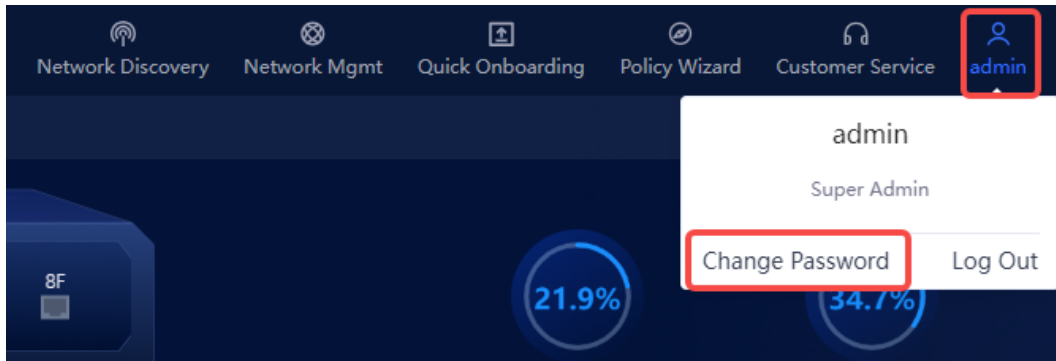
2. Changing the Default User Password of the Super Admin

Application Scenario

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

Procedure

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



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

Change Password ✕

* Old Password

* 🔒 New Password

* Confirm Password

Confirm
Cancel

Item	Description	Remarks
Old Password	Password used by the login user.	You need to obtain the password of the login user in advance.

New Password	Password after change.	<p>The new password must meet the following requirements:</p> <ul style="list-style-type: none"> ● Contain 8 to 15 characters. ● Contain at least three types of the following: uppercase letters, lowercase letters, digits, and special characters, and cannot contain Chinese characters, spaces, or full-width characters. ● Cannot be the same as the username or the username in reverse order.
Confirm Password	Password after change that is entered again.	The value of Confirm Password must be the same as that of New Password .

(7) Click **Confirm**.

3. Changing the Password of Administrators Except the Super Admin

Application Scenario

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

Procedure

- (1) Choose **System > Admin**.
- (2) Select the administrator whose password needs to be changed and click **Change Password** in the **Operation** column.

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

Change Password ⊗

* Old Password

* ⓘ New Password

* Confirm Password

(3) Set a new password for the administrator.

The new password must meet the following requirements:

- Contain 8 to 15 characters.
- Contain at least three types of the following: uppercase letters, lowercase letters, digits, and special

characters, and cannot contain Chinese characters, spaces, or full-width characters.

- o Cannot be the same as the username or the username in reverse order.

(4) Click **Confirm**.

2.4 Configuration Backup and Restoration

2.4.1 Exporting the Configuration

Application Scenario

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

Procedure

- (1) Choose System > System Maintenance > Config Backup.
- (2) Back up the configuration using either of the following methods:
 - o Click **Export Current Config** to download the configuration file.

The screenshot shows the 'Config Backup' interface. At the top, there is a header 'Config Backup'. Below it, the 'Back Up Config' section contains two buttons: 'Manually Back Up' and 'Export Current Config'. The 'Export Current Config' button is highlighted with a red border. Below this is the 'Restoration Config' section. It features a 'Restoration Mode' section with two radio buttons: 'Overwrite Current Config' (selected) and 'Merge Current Config'. Under 'Mode 1: Restore from a backup file on the device.', there is a dropdown menu showing 'running-cfg-20240123163318.tar.gz' and a blue 'Restore' button. Under 'Mode 2: Restore from a local backup file.', there is a text input field with the placeholder 'Select a configuration file.', a grey 'Browse' button, and a blue 'Restore' button.

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

The screenshot shows a web interface for configuration management. At the top, there is a header 'Config Backup'. Below it, the 'Back Up Config' section contains two buttons: 'Manually Back Up' (highlighted with a red box) and 'Export Current Config'. The 'Restoration Config' section has two radio buttons for 'Restoration Mode': 'Overwrite Current Config' (selected) and 'Merge Current Config'. Under 'Overwrite Current Config', there is a text input field containing 'running-cfg-20240123163318.tar.gz' and a 'Restore' button. Under 'Merge Current Config', there is a text input field with the placeholder 'Select a configuration file.', a 'Browse' button, and a 'Restore' button.

2.4.2 Importing the Configuration

Application Scenario

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

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

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.

Config Backup

Back Up Config

📁 Manually Back Up
📄 Export Current Config

Restoration Config

Restoration Mode: Overwrite Current Config Merge Current Config

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

▼
Restore

Mode 2: Restore from a local backup file.

Browse
Restore

- You can restore from a backup file on the device or **click Browse** to select a local backup file.

Config Backup

Back Up Config

📁 Manually Back Up
📄 Export Current Config

Restoration Config

Restoration Mode: Overwrite Current Config Merge Current Config

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

▼
Restore

Mode 2: Restore from a local backup file.

Browse
Restore

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

Follow-up Procedure

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

2.5 Defaults Restoration

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

⚠ Caution

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

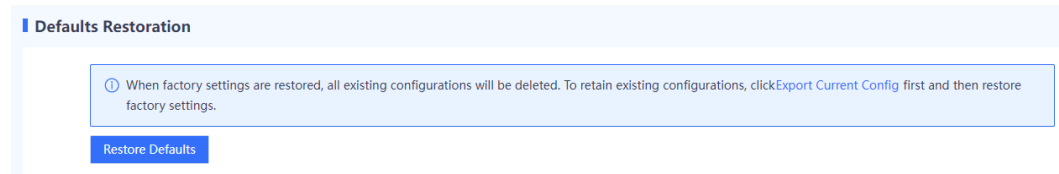
2.5.1 Web-based One-Click Restoration

Application Scenario

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

Procedure

- (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.

2.5.2 Restoration by Pressing the Reset Button

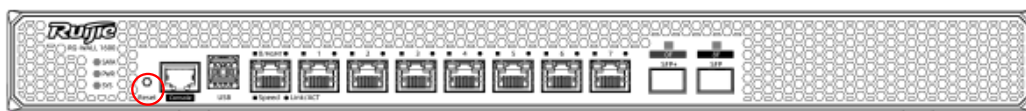
Application Scenario

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

Procedure

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

Figure 2-4 Reset Button on the Front Panel



Follow-up Procedure

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

i Note

The Reset button provides the following functions:

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

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

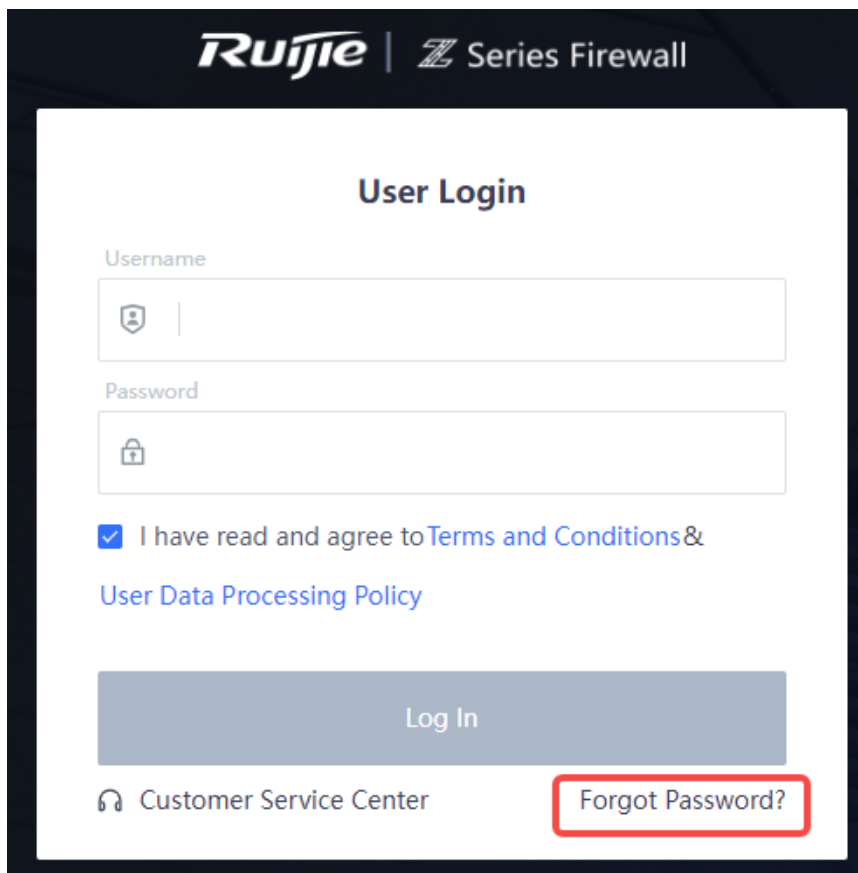
2.6 Password Restoration

Application Scenario

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

Procedure

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



- (2) Click **Forgot Password?**.
- (3) Perform the operation as instructed on the page.

Perform the Following Procedure



1. Hold down the Reset button for over 5s.
2. Log in to 192.168.1.200 through port 0/MGMT using the default account and password: admin and firewall.
3. After login, click Restore Backup File. Then, the system prompts you to restart the device. After the device restarts, the Web login account and password are restored to admin and firewall, and the other configurations are retained. Please note that you need to use the original port and IP address for login.
 - a Hold down the Reset button for over 5s until the device is restored to the factory mode.
 - b Connect the management PC to port 0/MGMT on the device panel through a network cable and set the IP address of the PC to one in the same network segment as that of port 0/MGMT (default address: 192.168.1.200), such as 192.168.1.201. Log in to <https://192.168.1.200> and enter the default username and password (**admin** and **firewall**).
 - c After login, click **Restore Backup File**. Then, the system prompts you to restart the device. After the device restarts, the web login account and password are restored to **admin** and **firewall**, and the other configurations are retained.

Restore Backup File

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

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

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

Restore Backup Config



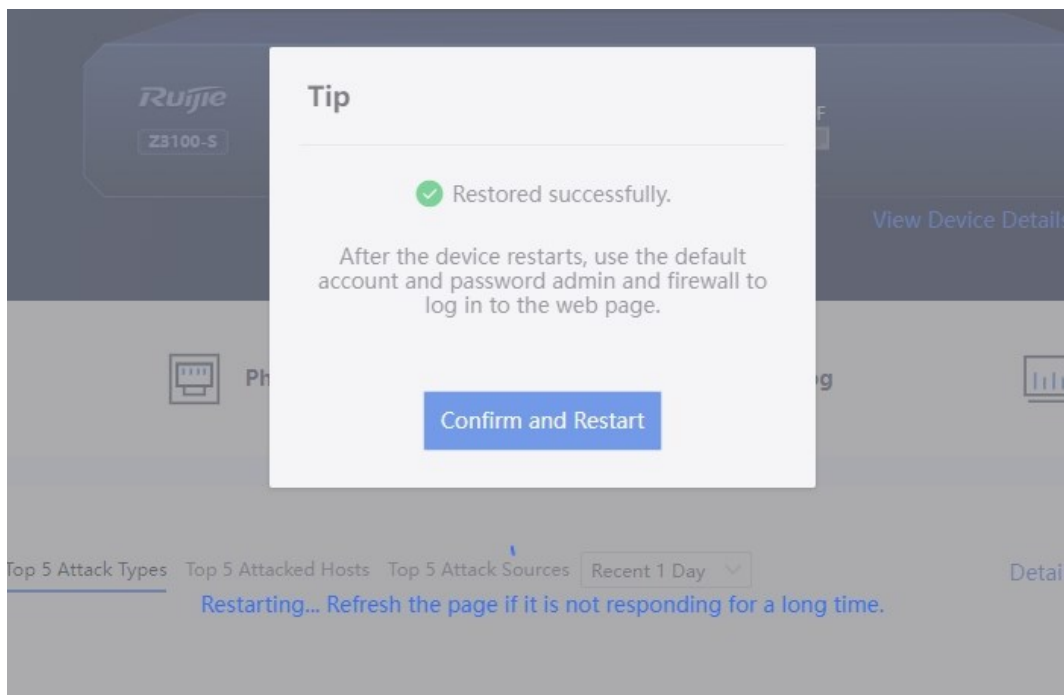
Restoring... Refresh the page if it is not responding for a long time.

Tip

✔ Restored successfully.

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

Confirm and Restart



✔ Restart succeeded.

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

Got It

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

Change Password

To ensure system security, change your password upon login.

* New Password

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

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

Password length range: 8–15 characters

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

* Confirm Password

Confirm

2.7 SNMP Management

2.7.1 Overview

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

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

The firewall supports the following SNMP versions:

- SNMPv1

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

- SNMPv2c

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

- SNMPv3

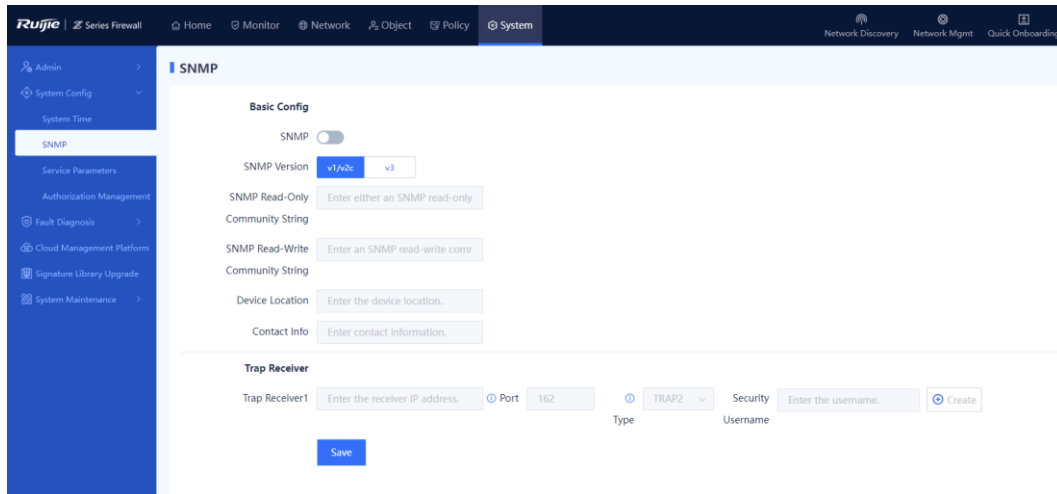
SNMPv3 defines extended security capabilities and provides the following security features through data identification and encryption:

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

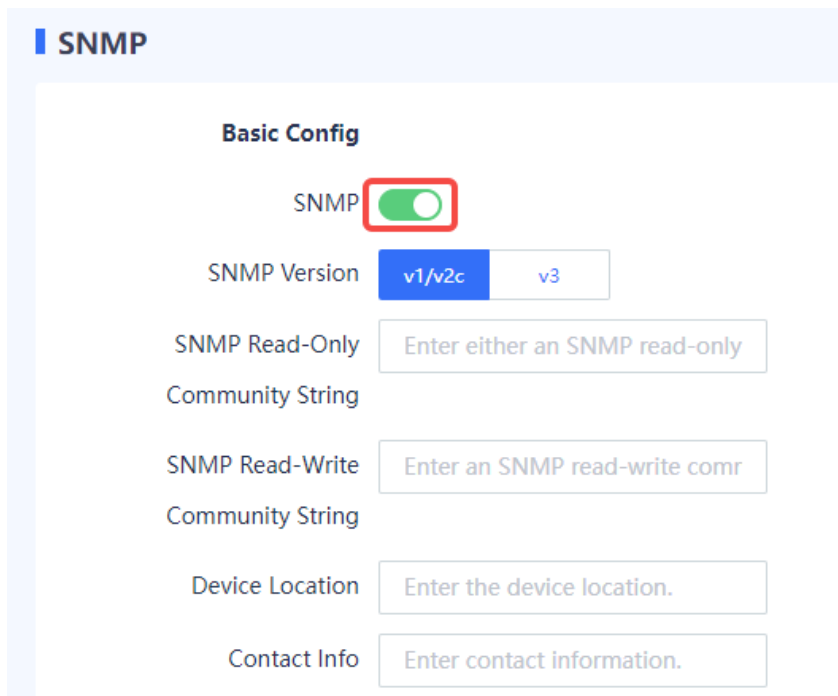
2.7.2 Configuring SNMP

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

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



(2) Enable **SNMP**.



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

Item	Description	Remarks
SNMP Version	Version number of SNMP. The options are v1/v2c and v3 .	The selected version must match that of the NMS server. [Example] v3
SNMP Version: v1/v2c		
SNMP Read-Only Community String	Community name used for authentication between the managed device and NMS server. If the NMS user uses a read-only community name for authentication, the user possesses the read-only permission to query device information.	The value must be the same as the read-only community name on the NMS. Otherwise, access from the NMS to the device may fail. Characters such as `~!#%^&*+\\ {};:'"/<>? and spaces are not allowed. [Example] public
SNMP Read-Write Community String	Community name used for authentication between the managed device and NMS server. If the NMS user uses a read-write community name for authentication, the user possesses the read-write permission on device configuration.	The value must be the same as the read-write community name on the NMS. Otherwise, access from the NMS to the device may fail. Characters such as `~!#%^&*+\\ {};:'"/<>? and spaces are not allowed. [Example] private
SNMP Version: v3		
Security Username	Username used by the NMS user to access the managed device.	The value must be the same as that on the NMS. Characters such as `~!#%^&*+\\ {};:'"/<>? and spaces are not allowed. [Example] user1
Authentication Algorithm	Authentication algorithm used to verify the user identity. MD5 and SHA algorithms are supported.	The value must be the same as that on the NMS. [Example] MD5

Item	Description	Remarks
Authentication Key	Password used to verify whether the NMS user is valid.	The value must be the same as the authentication password configured on the NMS. [Example] authkey
Encryption Algorithm	Encryption algorithm used to encrypt the transmitted data. AES and DES algorithms are supported.	The value must be the same as that on the NMS. [Example] AES
Encryption Key	Password used to encrypt the transmitted data.	The value must be the same as the encryption password configured on the NMS. [Example] prikey
Device Location	Physical location of the managed device. This information allows the administrator to quickly locate a faulty device.	-
Contact Info	Contact information of the maintenance engineer of the managed device. This information allows the administrator to easily get in touch with the device-related personnel.	-
Trap Receiver Click Create to add a trap receiver.		
Trap Receiver	Destination host address that receives the Trap message.	[Example] 1.1.1.2
Port	Number of the port used by the managed device to send a Trap message to the destination host. The default value is 162.	[Example] 162

Item	Description	Remarks
Type	Trap type. The options are TRAP , TRAP2 , and INFORM .	The type is TRAP2 in most cases. [Example] TRAP2
Security Username	Credential used by the device to report alarm information to the NMS server.	The value must be the same as that on the NMS server. [Example] user1

(4) Click **Save**.

3 License Activation

3.1 Authorization Service Overview

After purchasing a device, you can use the 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.

License	Description
RG-WALL 1600-Z3200-S-1G-LIC	Performance expansion license for the RG-WALL 1600-Z3200-S cloud-managed firewall: One license provides expansion of 1 Gbps network throughput. For each device, up to two licenses can be added to achieve 3 Gbps network throughput.
RG-WALL 1600-Z3200-S-LIS-M-1Y	Four-in-one license for the RG-WALL 1600-Z3200-S cloud-managed firewall: One license provides one-year upgrade services for intrusion prevention (IPS), antivirus (AV), app identification (APP), and URL signature libraries.
RG-WALL 1600-Z3200-S-LIS-E-1Y	Five-in-one license for the RG-WALL 1600-Z3200-S cloud-managed firewall: One license provides one-year upgrade services for IPS, AV, APP, and URL signature libraries and one-year threat intelligence services.
RG-WALL 1600-Z5100-S-1G-LIC	Performance expansion license for the RG-WALL 1600-Z5100-S cloud-managed firewall: One license provides expansion of 1 Gbps network throughput. For each device, up to two licenses can be added to achieve 10 Gbps network throughput.
RG-WALL 1600-Z1500-S-LIS-E-1Y	Five-in-one license for the firewall: One license provides one-year upgrade services for IPS, AV, APP, and URL signature libraries and one-year threat intelligence services.

3.2 Ruijie Secure Cloud Platform

3.2.1 Overview

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

3.2.2 Operations on Ruijie Secure Cloud Platform

1. User Registration and Login

(1) Register a user.

Note

When registering a user, you need to bind the user to a device SN. Ensure that the device SN exists in the order system (that is, the device has been properly delivered).

- a Enter <https://secloud1.ruijie.com.cn> in the browser and press **Enter**.
- b Click **Register** to access the registration page.
- c Enter the required user information to complete registration.

Tips

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

Register

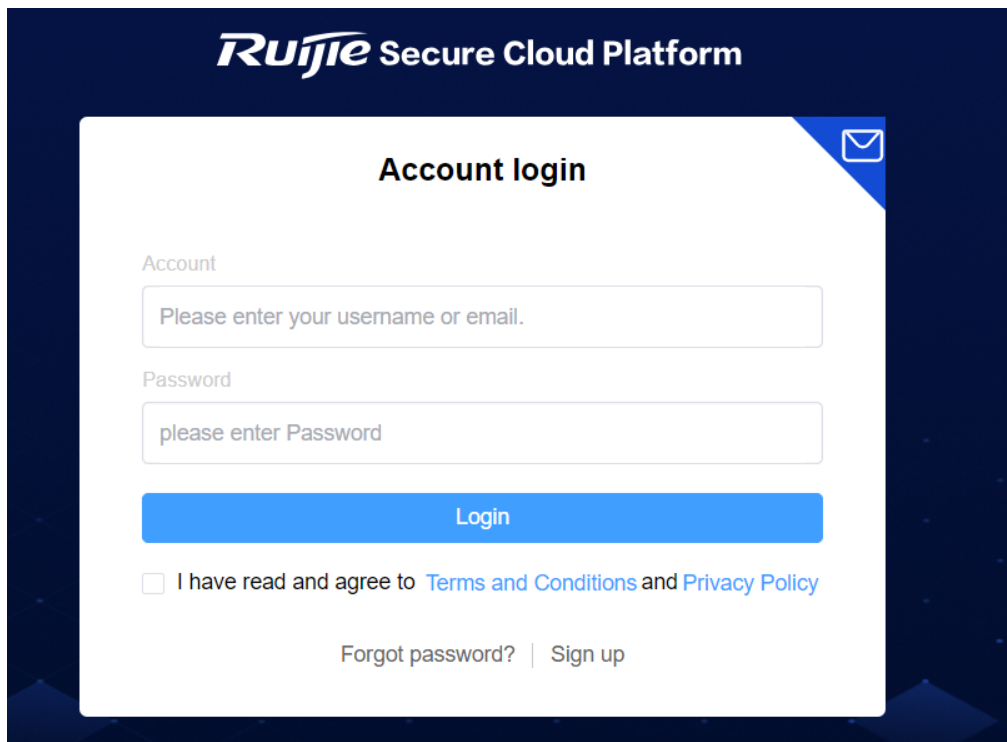
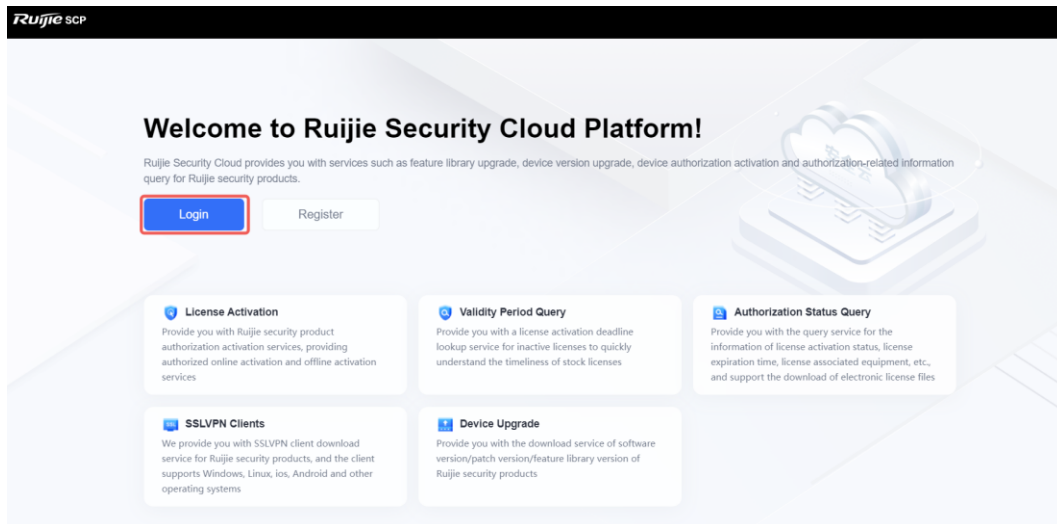
* Country or region	<input type="text" value="Country or region"/>
* Time Zone	<input type="text" value="Time Zone"/>
* Email Address	<input type="text" value="Email Address"/>
* Password	<input type="password" value="Enter the password."/>
* Verification Code	<input type="text" value="Verification Code"/> <input type="button" value="Send Code"/>

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

(2) Log in to the platform.

Visit <https://secloud1.ruijie.com.cn> to access the login page.

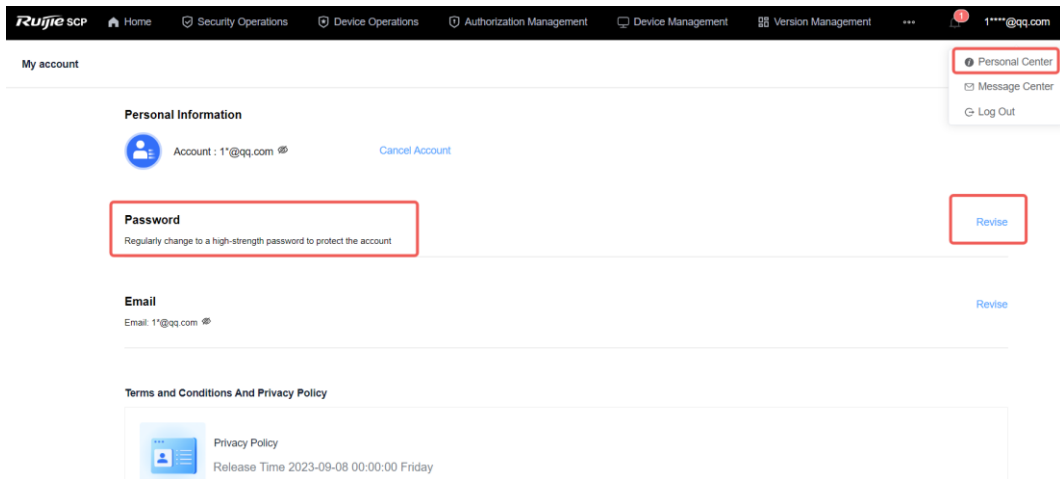
Click **Login** on the home page.



(3) Modify personal information.

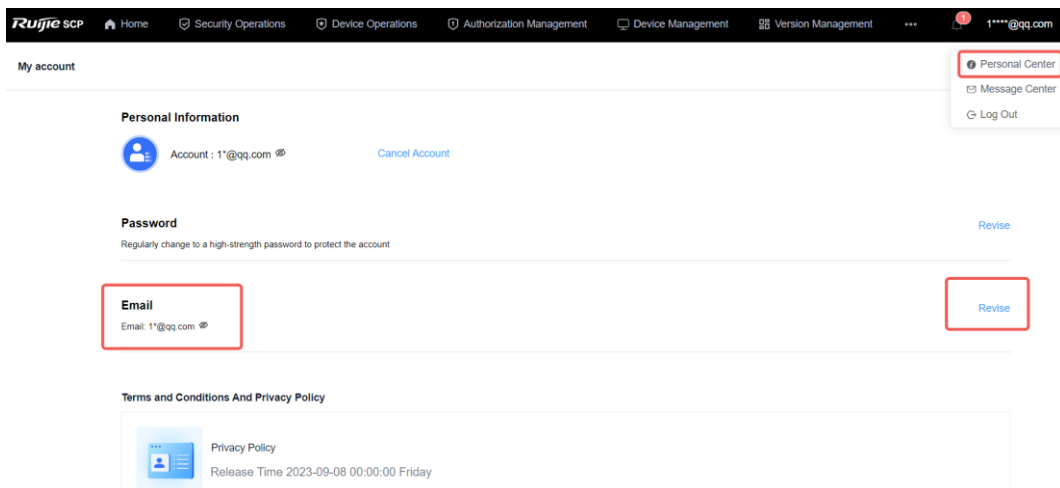
a Change the password.

Click the login username in the upper right corner of the page and select **Personal Center** from the drop-down list box. Click **Revise** to change the login password of the current user.



b Modify the email address.

Click the login username in the upper right corner of the page and select **Personal Center** from the drop-down list box to view the bound email address. Click **Revise** to modify the email address bound to the current user.



2. App Identification Signature Library Upgrade

Prerequisites

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

Procedure

- Offline upgrade
- (1) Download a version file for the app identification signature library.
 - a Log in to Ruijie Secure Cloud Platform using an account with permission on the **Version Management** menu.
 - b Choose **Version Management > Signature Library Version > App Identification Signature Library**, find the applicable version, and click **Download** in the **Operation** column to download the version file to the local device.

No.	File Name	Version Number	Version Description	Model	Software Version	releaseTime	File Size (MB)	MD5	Operation
1	app_signature.zip	20231222.1615	20231222.1615	Universal	Universal	2023-12-22	0.69MB	4d98dda4e02d3...	Download
2	app_signature.zip	20231221.1601	20231221.1601	Universal	Universal	2023-12-19	0.69MB	b3055177e9f6dd...	Download
3	app_signature.zip	20231118.1428	20231118.1428	Universal	Universal	2023-11-17	0.91MB	f4048ec083e03...	Download
4	app_signature.zip	20231110.1660	20231110.1660	Universal	Universal	2023-11-13	0.67MB	8432da4d2bfed6...	Download
5	app_signature.zip	20231103.1103	20231103.1103	Universal	Universal	2023-11-03	1.10MB	5e9aea1d86a27e...	Download
6	app_signature.zip	20231012.1011	20231012.1011	Universal	Universal	2023-10-12	0.67MB	269d3a893a1571...	Download
7	app_signature.zip	20230611.1649	20230611.1649	Universal	Universal	2023-09-21	0.51MB	7025ac553576d5...	Download
8	app_signature.zip	20230913.1719	20230913.1719	Universal	Universal	2023-09-12	0.57MB	ac59fbd07cbcd...	Download
9	app_signature.zip	20230912.1053	20230912.1053	Universal	Universal	2023-09-11	0.57MB	1a2b5792b3e33...	Download
10	app_signature.zip	20230612.1213	20230612.1213	Universal	Universal	2023-08-24	0.51MB	da1b2c79e9927...	Download

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

Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time: Daily 16 Hour 22 Minute

Signature Library: Select All

App Identification Signature Library Virus Protection Signature Library (Deep Scan) Virus Protection Signature Library (Quick Scan) Intrusion Prevention Signature Library

ISP Address Library Threat Intelligence Signature Library URL Signature Library Behavior Analysis Signature Library

Signature Library Type

Upgrade All (Upgrade all signature libraries online simultaneously)

App Identification Signature Library

Current Version: 20231222.1615

Last Upgrade Time: -

Latest Version: Unable to obtain the latest version. No SN record is found.

Version State: -

Activation State: Not Activated

[Online Upgrade](#) [Local Upgrade](#) [Rolling back](#)

Virus Protection Signature Library (Deep Scan)

Current Version: -

Last Upgrade Time: -

Latest Version: Unable to obtain the latest version. No SN record is found.

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

Activation State: Not Activated

[Online Upgrade](#) [Local Upgrade](#)

Virus Protection Signature Library (Quick Scan)

Current Version: 20230619.0232

Last Upgrade Time: -

Latest Version: Unable to obtain the latest version. No SN record is found.

Version State: -

Activation State: Not Activated

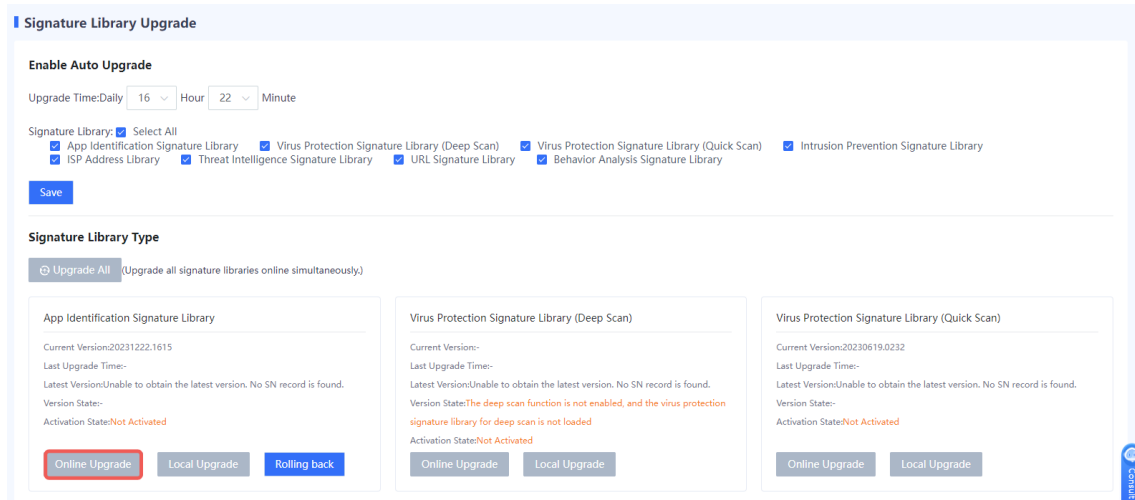
[Online Upgrade](#) [Local Upgrade](#)

- Online upgrade

Note

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

On the firewall web UI, choose **System > Signature Library Upgrade**, On the firewall, find **App Identification Signature Library**, and upgrade the app identification signature library in online mode.



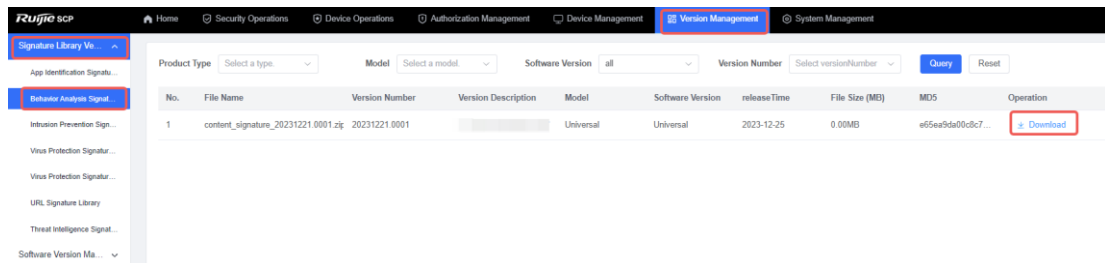
3. Behavior Analysis Signature Library Upgrade

Procedure

- Offline upgrade

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

- Log in to Ruijie Secure Cloud Platform using an account with permission on the **Version Management** menu.
- Choose **Version Management > Signature Library Version > Behavior Analysis Signature Library**, find the applicable version, and click **Download** in the **Operation** column to download the upgrade file to the local device.



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

The screenshot shows the 'Signature Library' management interface. At the top, there are checkboxes for selecting different signature libraries: App Identification Signature Library, URL Signature Library, Behavior Analysis Signature Library, Virus Protection Signature Library (Deep Scan), Virus Protection Signature Library (Quick Scan), Intrusion Prevention Signature Library, ISP Address Library, and Threat Intelligence Signature Library. Below this is a 'Save' button. The main section is titled 'Signature Library Type' and contains a grid of cards for each library. Each card displays the library name, current version, last upgrade time, latest version (with a note that it is unavailable to obtain), version state, and activation state. At the bottom of each card are buttons for 'Online Upgrade', 'Local Upgrade', and 'Rolling back'. The 'Behavior Analysis Signature Library' card is highlighted with a red border, and its 'Local Upgrade' button is also highlighted with a red border.

- Online upgrade

Note

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

Choose **System > Signature Library Upgrade** on the firewall, find **Behavior Analysis Signature Library**, and upgrade the behavior analysis signature library in online mode.

This is an identical duplicate of the screenshot above, showing the 'Signature Library' management interface with the 'Behavior Analysis Signature Library' card highlighted.

4. IPS Signature Library Upgrade

Prerequisites

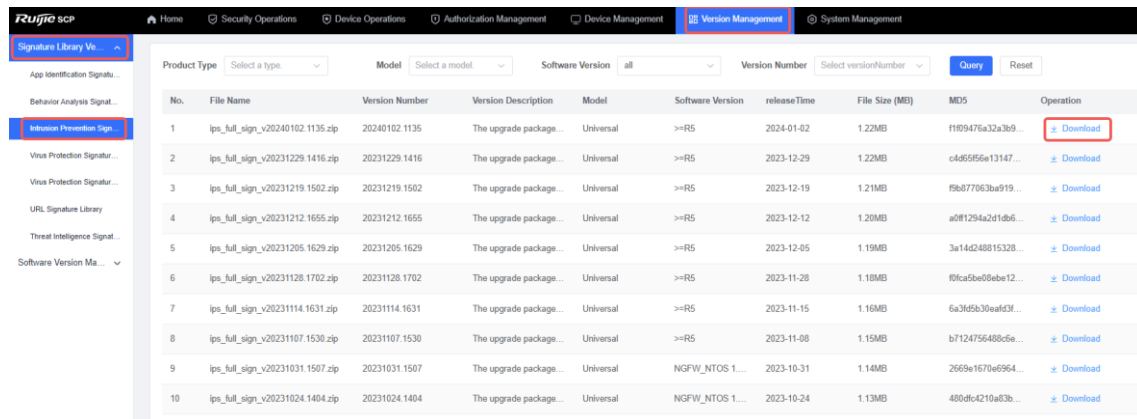
The Intrusion Prevention (IPS) license has been activated for the firewall and the license is within the validity period.

Procedure

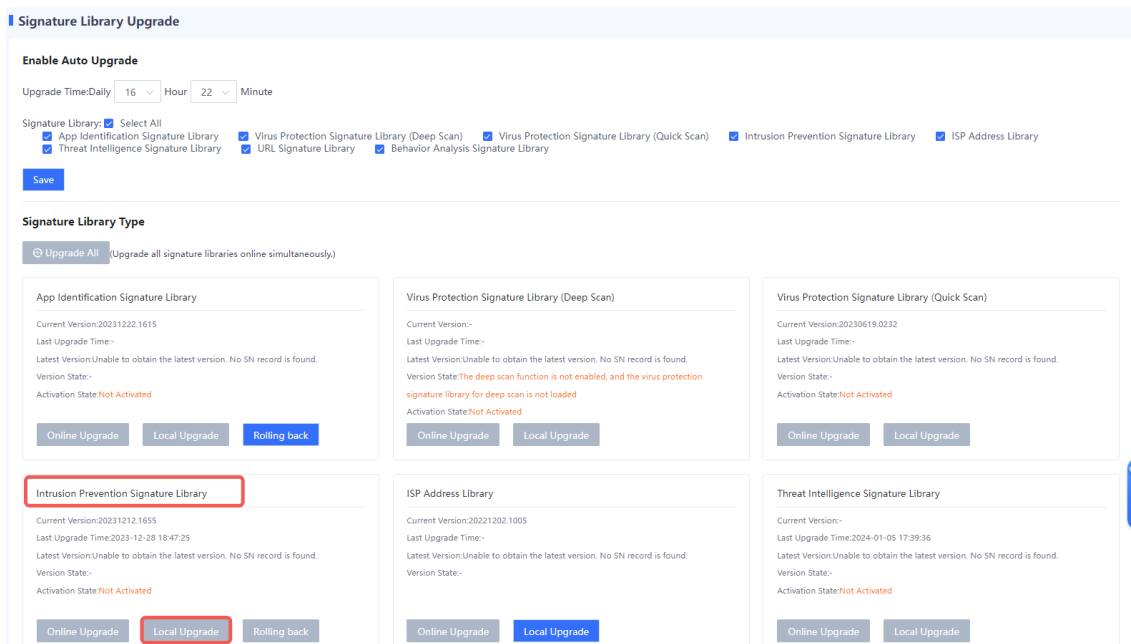
- Offline upgrade

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

- Log in to Ruijie Secure Cloud Platform using an account with permission on the **Version Management** menu.
- Choose **Version Management > Signature Library Version > Intrusion Prevention Signature Library**, find the applicable version, and click **Download** in the **Operation** column to download the version file to the local device.



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

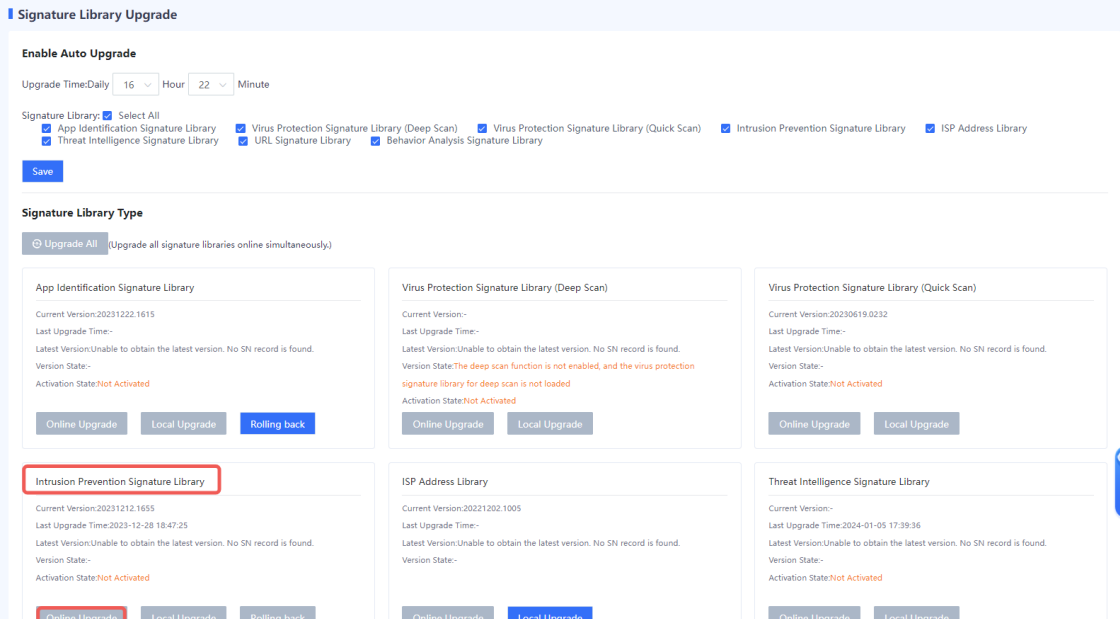


- Online upgrade

Note

- The firewall must be connected to the Internet.
- When the current version information about the signature library of the firewall exists on Ruijie Secure Cloud Platform and a new version is available, online upgrade of the IPS signature library can be performed on the firewall web UI.

On the firewall web UI, choose **System > Signature Library Upgrade**, On the firewall, find **Intrusion Prevention Signature Library**, and upgrade the IPS signature library in online mode.



Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time: Daily 16 Hour 22 Minute

Signature Library: Select All

App Identification Signature Library Virus Protection Signature Library (Deep Scan) Virus Protection Signature Library (Quick Scan) Intrusion Prevention Signature Library ISP Address Library

Threat Intelligence Signature Library URL Signature Library Behavior Analysis Signature Library

Save

Signature Library Type

Upgrade All (Upgrade all signature libraries online simultaneously)

App Identification Signature Library

Current Version: 20231222.1615
Last Upgrade Time: --
Latest Version: Unable to obtain the latest version. No SN record is found.
Version State: --
Activation State: Not Activated

Online Upgrade **Local Upgrade** **Rolling back**

Virus Protection Signature Library (Deep Scan)

Current Version: --
Last Upgrade Time: --
Latest Version: Unable to obtain the latest version. No SN record is found.
Version State: The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded
Activation State: Not Activated

Online Upgrade **Local Upgrade**

Virus Protection Signature Library (Quick Scan)

Current Version: 20230619.0232
Last Upgrade Time: --
Latest Version: Unable to obtain the latest version. No SN record is found.
Version State: --
Activation State: Not Activated

Online Upgrade **Local Upgrade**

Intrusion Prevention Signature Library

Current Version: 20231212.1655
Last Upgrade Time: 2023-12-28 18:47:25
Latest Version: Unable to obtain the latest version. No SN record is found.
Version State: --
Activation State: Not Activated

Online Upgrade **Local Upgrade** **Rolling back**

ISP Address Library

Current Version: 20221202.1005
Last Upgrade Time: --
Latest Version: Unable to obtain the latest version. No SN record is found.
Version State: --

Online Upgrade **Local Upgrade**

Threat Intelligence Signature Library

Current Version: --
Last Upgrade Time: 2024-01-05 17:39:36
Latest Version: Unable to obtain the latest version. No SN record is found.
Version State: --
Activation State: Not Activated

Online Upgrade **Local Upgrade**

5. Virus Protection Signature Library (Quick Scan) Upgrade

Prerequisites

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

Procedure

- Offline upgrade
- (1) Download the version file for the virus protection signature library (quick scan).
 - a Log in to Ruijie Secure Cloud Platform using an account with permission on the **Version Management** menu.
 - b Choose **Version Management > Signature Library Version > Virus Protection Signature Library (Quick Scan)**, find the applicable version, and click **Download** in the **Operation** column to download the version file to the local device.

No.	File Name	Version Number	Version Description	Model	Software Version	releaseTime	File Size (MB)	MD5	Operation
1	hash_20240112.1530_full_sig.zi	20240112.1530	hash_20240112.1530...	Z3200-S	Universal	2024-01-12	8.91MB	6160b9a7e62ae3...	Download
2	hash_20240112.0403_full_sig.zi	20240112.0403	hash_20240112.0403...	Z8620.Z8680	Universal	2024-01-12	76.35MB	82df841b4cd08...	Download
3	hash_20240112.0316_full_sig.zi	20240112.0316	hash_20240112.0316...	Z3200-S	Universal	2024-01-12	8.98MB	c5081449485e3...	Download
4	hash_20240111.1502_full_sig.zi	20240111.1502	hash_20240111.1502...	Z3200-S	Universal	2024-01-11	8.93MB	52a30c0370fa51...	Download
5	hash_20240111.1403_full_sig.zi	20240111.1403	hash_20240111.1403...	Z8620.Z8680	Universal	2024-01-11	76.43MB	ccb85d27c54e0...	Download
6	hash_20240111.0254_full_sig.zi	20240111.0254	hash_20240111.0254...	Z3200-S	Universal	2024-01-11	9.04MB	9e5182768ff4da...	Download
7	hash_20240111.0003_full_sig.zi	20240111.0003	hash_20240111.0003...	Z8620.Z8680	Universal	2024-01-11	76.40MB	271dab7bc1ab35...	Download
8	hash_20240110.1440_full_sig.zi	20240110.1440	hash_20240110.1440...	Z3200-S	Universal	2024-01-10	9.11MB	b4af4a92e63351...	Download
9	hash_20240110.1003_full_sig.zi	20240110.1003	hash_20240110.1003...	Z8620.Z8680	Universal	2024-01-10	76.45MB	6e749203a7e02ff...	Download
10	hash_20240110.0234_full_sig.zi	20240110.0234	hash_20240110.0234...	Z3200-S	Universal	2024-01-10	9.10MB	cd2926f3b8f6dc3...	Download

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

Signature Library Type

Upgrade All (Upgrade all signature libraries online simultaneously.)

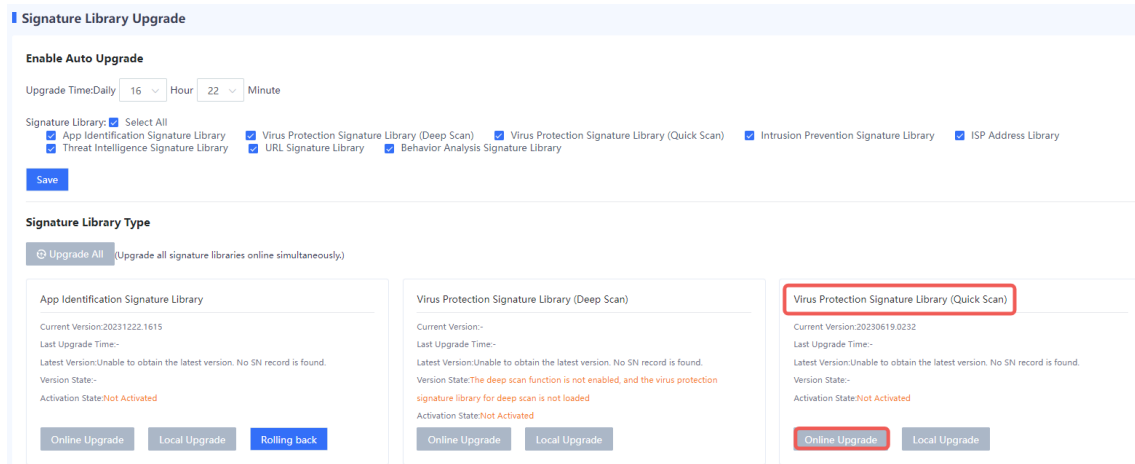
<p>App Identification Signature Library</p> <p>Current Version:20231222.1615 Last Upgrade Time:- Latest Version:Unable to obtain the latest version. No SN record is found. Version State:- Activation State:Not Activated</p> <p>Online Upgrade Local Upgrade Rolling back</p>	<p>Virus Protection Signature Library (Deep Scan)</p> <p>Current Version:- Last Upgrade Time:- Latest Version:Unable to obtain the latest version. No SN record is found. Version State:The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded Activation State:Not Activated</p> <p>Online Upgrade Local Upgrade</p>	<p>Virus Protection Signature Library (Quick Scan)</p> <p>Current Version:20230619.0232 Last Upgrade Time:- Latest Version:Unable to obtain the latest version. No SN record is found. Version State:- Activation State:Not Activated</p> <p>Online Upgrade Local Upgrade</p>
<p>Intrusion Prevention Signature Library</p> <p>Current Version:20231212.1655 Last Upgrade Time:2023-12-28 18:47:25 Latest Version:Unable to obtain the latest version. No SN record is found. Version State:- Activation State:Not Activated</p> <p>Online Upgrade Local Upgrade Rolling back</p>	<p>ISP Address Library</p> <p>Current Version:20221202.1005 Last Upgrade Time:- Latest Version:Unable to obtain the latest version. No SN record is found. Version State:-</p> <p>Online Upgrade Local Upgrade</p>	<p>Threat Intelligence Signature Library</p> <p>Current Version:- Last Upgrade Time:2024-01-05 17:39:36 Latest Version:Unable to obtain the latest version. No SN record is found. Version State:- Activation State:Not Activated</p> <p>Online Upgrade Local Upgrade</p>
<p>URL Signature Library</p> <p>Current Version:- Last Upgrade Time:2024-01-04 04:29:17 Latest Version:Unable to obtain the latest version. No SN record is found. Version State:- Activation State:Not Activated</p>	<p>Behavior Analysis Signature Library</p> <p>Current Version:20231221.0001 Last Upgrade Time:- Latest Version:Unable to obtain the latest version. No SN record is found. Version State:-</p>	

- Online upgrade

i Note

- The firewall must be connected to the Internet.
- When the current version information about the signature library of the firewall exists on Ruijie Secure Cloud Platform and a new version is available, online upgrade of the virus protection signature library (quick scan) can be performed on the firewall.

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



6. Virus Protection Signature Library (Deep Scan) Upgrade

Prerequisites

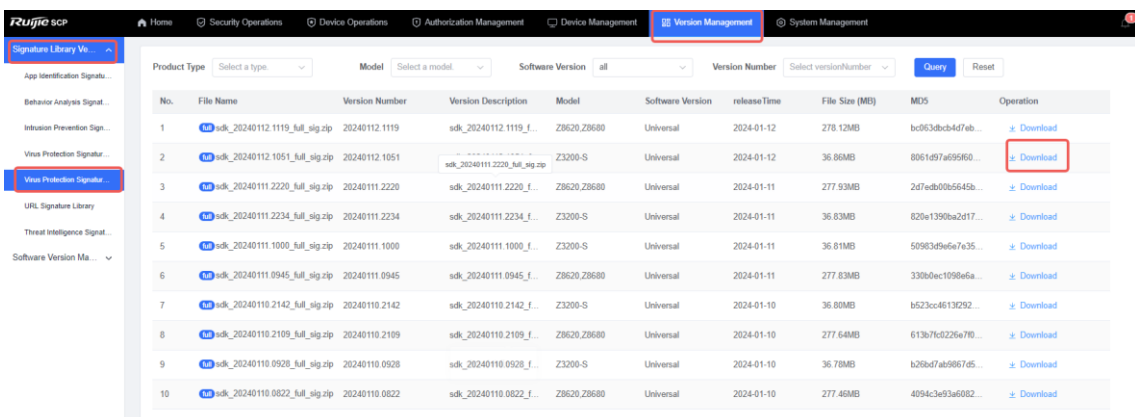
The Antivirus (AV) license has been activated for the firewall and the license is within the validity period.

Procedure

- Offline upgrade

(1) Download the version file for the virus protection signature library (deep scan).

- Log in to Ruijie Secure Cloud Platform using an account with permission on the **Version Management** menu.
- Choose **Version Management > Signature Library Version > Virus Protection Signature Library (Deep Scan)**, find the applicable version, and click **Download** in the **Operation** column to download the version file to the local device.



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

Signature Library Type

⊕ Upgrade All (Upgrade all signature libraries online simultaneously)

Virus Protection Signature Library (Deep Scan)

Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version. No SN record is found.
Version State:-
Activation State:Not Activated

Online Upgrade Local Upgrade **Rolling back**

Virus Protection Signature Library (Quick Scan)

Current Version:20230619.0232
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version. No SN record is found.
Version State:-
Activation State:Not Activated

Online Upgrade Local Upgrade

Intrusion Prevention Signature Library

Current Version:20231212.1655
Last Upgrade Time:2023-12-28 18:47:25
Latest Version:Unable to obtain the latest version. No SN record is found.
Version State:-
Activation State:Not Activated

Online Upgrade Local Upgrade Rolling back

ISP Address Library

Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version. No SN record is found.
Version State:-

Online Upgrade Local Upgrade

Threat Intelligence Signature Library

Current Version:-
Last Upgrade Time:2024-01-05 17:39:36
Latest Version:Unable to obtain the latest version. No SN record is found.
Version State:-
Activation State:Not Activated

Online Upgrade Local Upgrade

URL Signature Library

Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version. No SN record is found.
Version State:-
Activation State:Not Activated

Behavior Analysis Signature Library

Current Version:20231221.0001
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version. No SN record is found.
Version State:-

- Online upgrade

Note

- The firewall must be connected to the Internet.
- When the current version information about the signature library of the firewall exists on Ruijie Secure Cloud Platform and a new version is available, online upgrade of the virus protection signature library (deep scan) can be performed on the firewall.

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

Signature Library Type

⊕ Upgrade All (Upgrade all signature libraries online simultaneously)

Virus Protection Signature Library (Deep Scan)

Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version. No SN record is found.
Version State:-
Activation State:Not Activated

Online Upgrade Local Upgrade **Rolling back**

Virus Protection Signature Library (Quick Scan)

Current Version:20230619.0232
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version. No SN record is found.
Version State:-
Activation State:Not Activated

Online Upgrade Local Upgrade

Intrusion Prevention Signature Library

Current Version:20231212.1655
Last Upgrade Time:2023-12-28 18:47:25
Latest Version:Unable to obtain the latest version. No SN record is found.
Version State:-
Activation State:Not Activated

Online Upgrade Local Upgrade Rolling back

ISP Address Library

Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version. No SN record is found.
Version State:-

Online Upgrade Local Upgrade

Threat Intelligence Signature Library

Current Version:-
Last Upgrade Time:2024-01-05 17:39:36
Latest Version:Unable to obtain the latest version. No SN record is found.
Version State:-
Activation State:Not Activated

Online Upgrade Local Upgrade

URL Signature Library

Current Version:-
Last Upgrade Time:2024-01-04 04:29:17
Latest Version:Unable to obtain the latest version. No SN record is found.
Version State:-
Activation State:Not Activated

Behavior Analysis Signature Library

Current Version:20231221.0001
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version. No SN record is found.
Version State:-

7. URL Signature Library Upgrade

Prerequisites

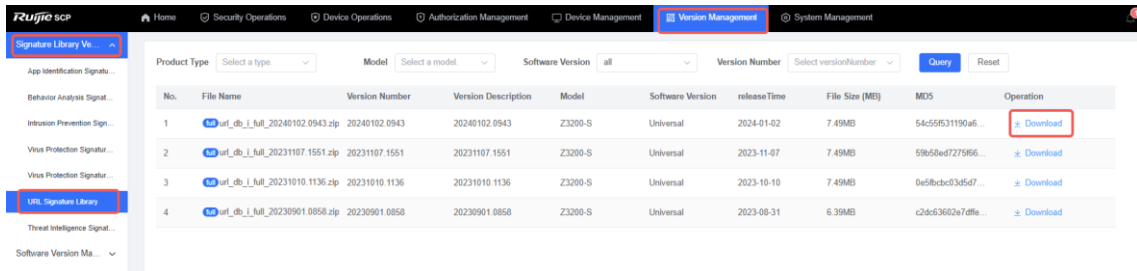
The URL filtering license has been activated for the firewall and the license is within the validity period.

Procedure

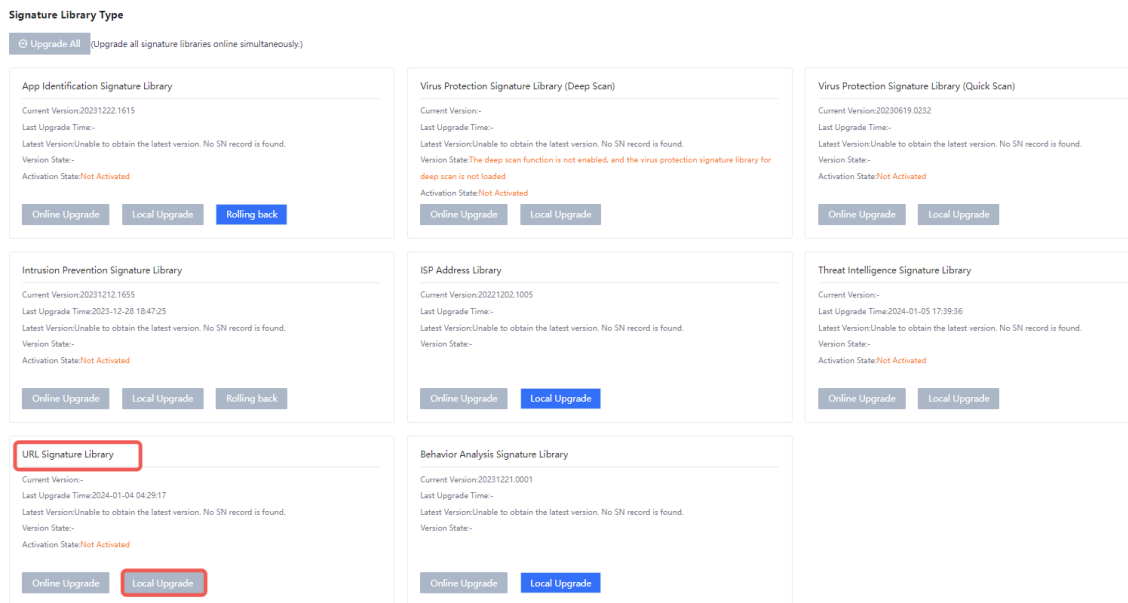
- Offline upgrade

(1) Download the version file for the URL signature library.

- Log in to Ruijie Secure Cloud Platform using an account with permission on the **Version Management** menu.
- Choose **Version Management > Signature Library Version > URL Signature Library**, find the applicable version, and click **Download** in the **Operation** column to download the version file to the local device.



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



- Online upgrade

Note

- The firewall must be connected to the Internet.
- When the current version information about the signature library of the firewall exists on Ruijie Secure Cloud Platform and a new version is available, online upgrade of the URL signature library can be performed on the firewall.

On the firewall web UI, choose **System > Signature Library Upgrade**. On the firewall, find **URL Signature Library**, and click **Online Upgrade** to perform online upgrade.

Signature Library Type
 Upgrade All (Upgrade all signature libraries online simultaneously)

App Identification Signature Library

Current Version:20231222.1615
 Last Upgrade Time:-
 Latest Version:Unable to obtain the latest version. No SN record is found.
 Version State:-
 Activation State:Not Activated

Online Upgrade Local Upgrade Rolling back

Virus Protection Signature Library (Deep Scan)

Current Version:-
 Last Upgrade Time:-
 Latest Version:Unable to obtain the latest version. No SN record is found.
 Version State:The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded
 Activation State:Not Activated

Online Upgrade Local Upgrade

Virus Protection Signature Library (Quick Scan)

Current Version:20230619.0202
 Last Upgrade Time:-
 Latest Version:Unable to obtain the latest version. No SN record is found.
 Version State:-
 Activation State:Not Activated

Online Upgrade Local Upgrade

Intrusion Prevention Signature Library

Current Version:20231212.1655
 Last Upgrade Time:2023-12-28 18:47:25
 Latest Version:Unable to obtain the latest version. No SN record is found.
 Version State:-
 Activation State:Not Activated

Online Upgrade Local Upgrade Rolling back

ISP Address Library

Current Version:20221202.1005
 Last Upgrade Time:-
 Latest Version:Unable to obtain the latest version. No SN record is found.
 Version State:-

Online Upgrade Local Upgrade

Threat Intelligence Signature Library

Current Version:-
 Last Upgrade Time:2024-01-05 17:39:36
 Latest Version:Unable to obtain the latest version. No SN record is found.
 Version State:-
 Activation State:Not Activated

Online Upgrade Local Upgrade

URL Signature Library

Current Version:-
 Last Upgrade Time:2024-01-04 04:29:17
 Latest Version:Unable to obtain the latest version. No SN record is found.
 Version State:-
 Activation State:Not Activated

Online Upgrade Local Upgrade

Behavior Analysis Signature Library

Current Version:20231221.0001
 Last Upgrade Time:-
 Latest Version:Unable to obtain the latest version. No SN record is found.
 Version State:-

Online Upgrade Local Upgrade

8. Threat Intelligence Library Upgrade

Prerequisites

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

Procedure

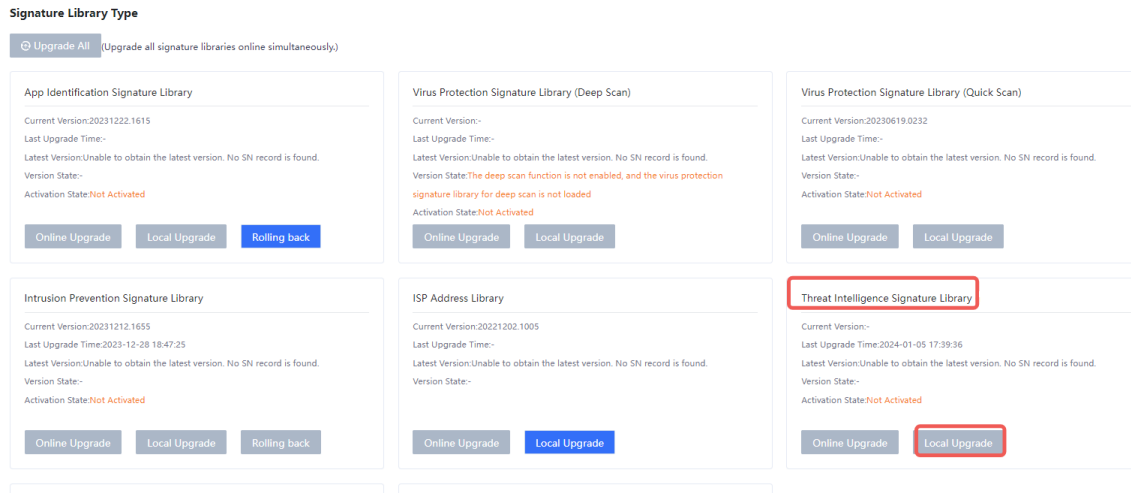
- Offline upgrade

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

- a Log in to Ruijie Secure Cloud Platform using an account with permission on the **Version Management** menu.
- b Choose **Version Management > Signature Library Version > Threat Intelligence Signature Library**, find the applicable version, and click **Download** in the **Operation** column to download the version file to the local device.

No.	File Name	Version Number	Version Description	Model	Software Version	releaseTime	File Size (MB)	MD5	Operation
1	ti_03_20240112.0356_full_sig.zip	20240112.0356	ti_03_20240112.0356...	Universal	Universal	2024-01-12	6.36MB	7d5e3f5dbd345d...	Download
2	ti_03_20240111.1356_full_sig.zip	20240111.1356	ti_03_20240111.1356...	Universal	Universal	2024-01-11	6.33MB	2d1097a27b6743...	Download
3	ti_03_20240110.2356_full_sig.zip	20240110.2356	ti_03_20240110.2356...	Universal	Universal	2024-01-10	6.32MB	f3c2d3b6c2177d...	Download
4	ti_03_20240110.0956_full_sig.zip	20240110.0956	ti_03_20240110.0956...	Universal	Universal	2024-01-10	6.32MB	87edc3a9e6d95a...	Download
5	ti_03_20240109.1956_full_sig.zip	20240109.1956	ti_03_20240109.1956...	Universal	Universal	2024-01-09	6.31MB	5fab5a32c24958...	Download
6	ti_03_20240109.0156_full_sig.zip	20240109.0156	ti_03_20240109.0156...	Universal	Universal	2024-01-09	6.30MB	0f7b15c49d7cc2...	Download
7	ti_03_20240108.1156_full_sig.zip	20240108.1156	ti_03_20240108.1156...	Universal	Universal	2024-01-08	6.31MB	17cca6af100e8b...	Download
8	ti_03_20240107.2156_full_sig.zip	20240107.2156	ti_03_20240107.2156...	Universal	Universal	2024-01-07	6.32MB	2b7467d83e2b5...	Download
9	ti_03_20240107.0756_full_sig.zip	20240107.0756	ti_03_20240107.0756...	Universal	Universal	2024-01-07	6.35MB	727a43916ea78f...	Download
10	ti_03_20240106.1756_full_sig.zip	20240106.1756	ti_03_20240106.1756...	Universal	Universal	2024-01-06	6.33MB	8c2d400643c9db...	Download

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

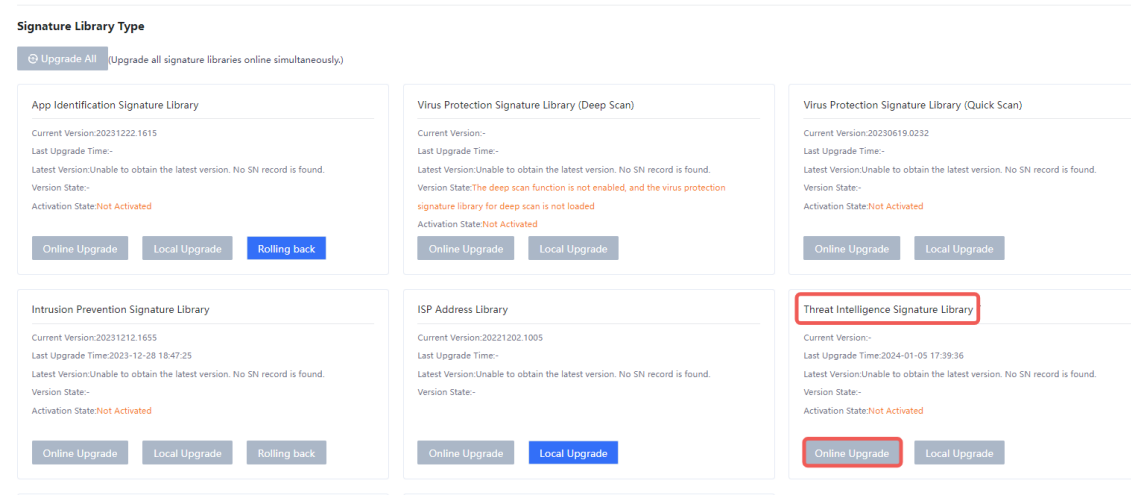


- Online upgrade

Note

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

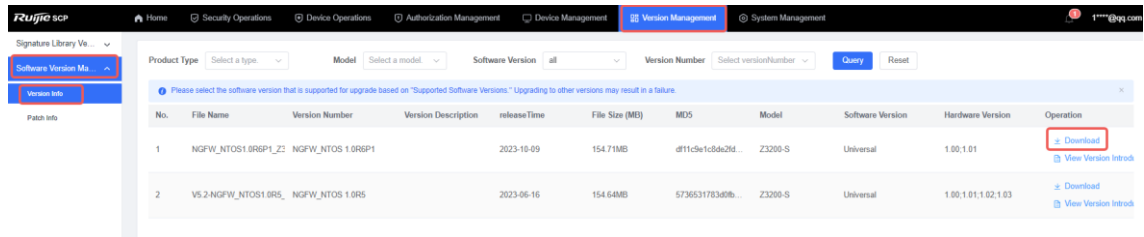
On the firewall web UI, choose **System > Signature Library Upgrade**. On the firewall, find **Threat Intelligence Signature Library**, and click **Online Upgrade** to perform online upgrade.



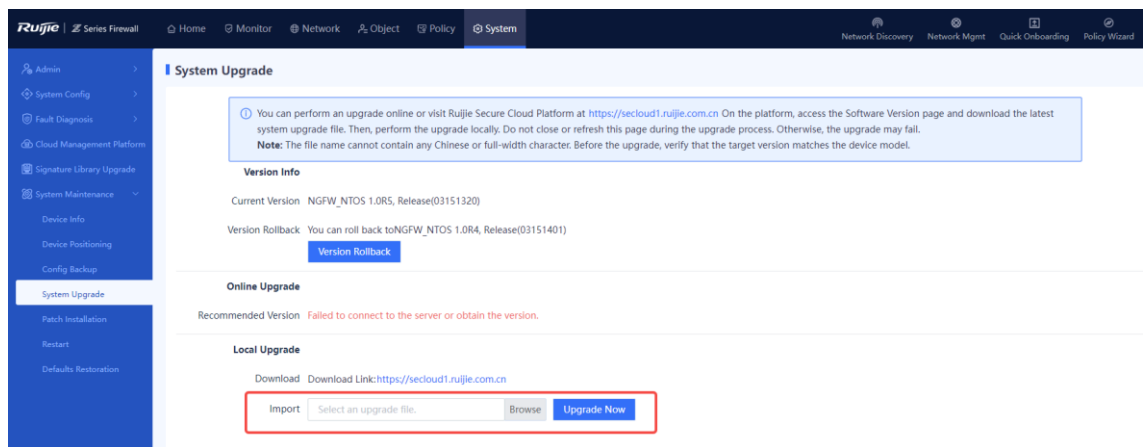
9. System Upgrade

- Offline upgrade
- (1) Download a version file.
 - a Confirm that the current user possesses the permission on the **Version Management** menu.

- b Log in to Ruijie Secure Cloud Platform. Choose **Version Management > Software Version Management > Version Info**, find the applicable version, and click **Download** in the **Operation** column to download the version file to the local device.



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

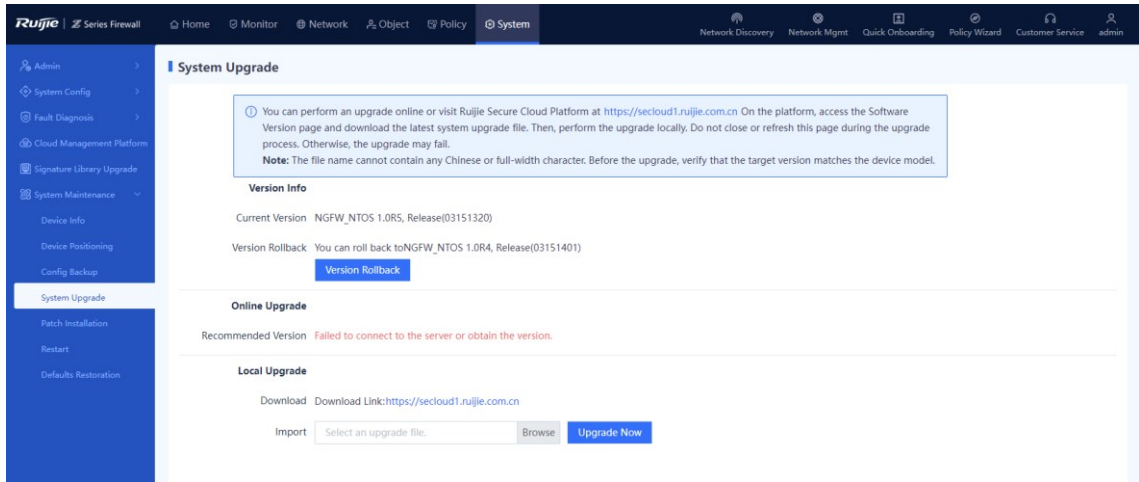


- Online upgrade

i Note

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

On the firewall web UI, choose **System > System Maintenance > System Upgrade**. On the page that is displayed, click **Upgrade Now** to perform online upgrade.



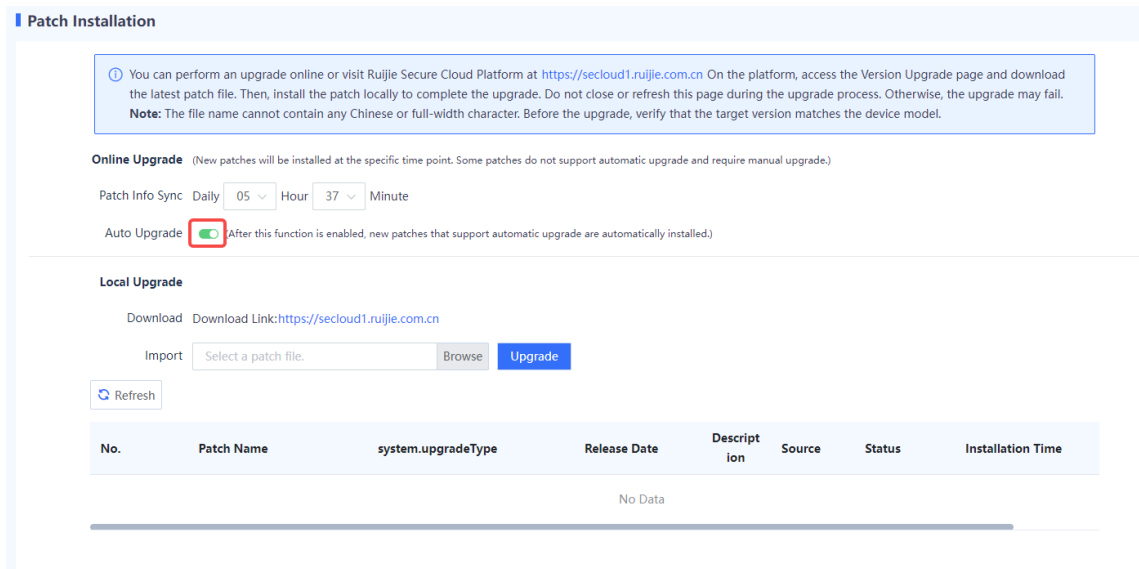
10. Patch Installation

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

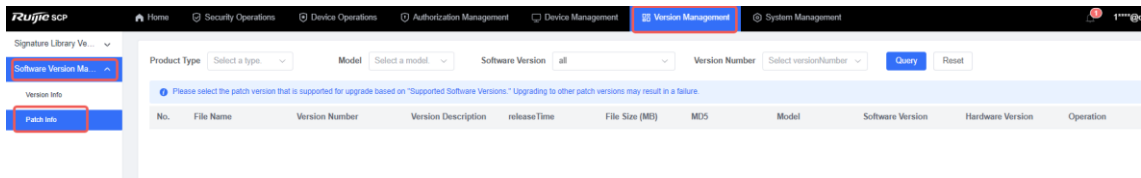
- Online patch installation
 - a Log in to the firewall web UI and choose **System > System Maintenance > Patch Installation**.
 - b Toggle on **Auto Upgrade** under **Online Upgrade**. The system automatically installs the patch packages.

⚠ Caution

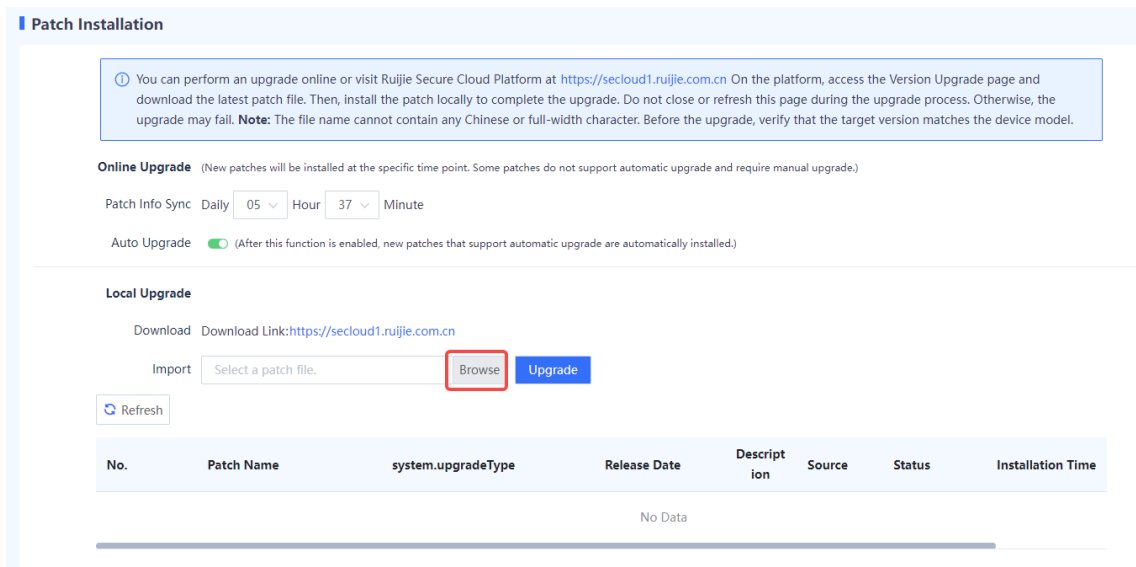
Online upgrade is successful only when the firewall can properly communicate with Ruijie Secure Cloud Platform.



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



- b Log in to the firewall and choose System > System Maintenance > Patch Installation.
- c In the **Local Upgrade** area, click **Browse** and select a patch file.



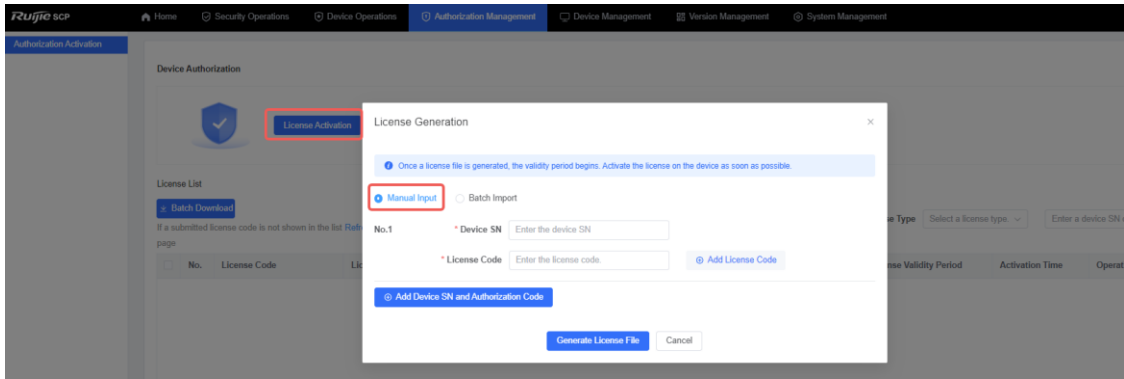
- d Click **Upgrade** to start system upgrade.

Note

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

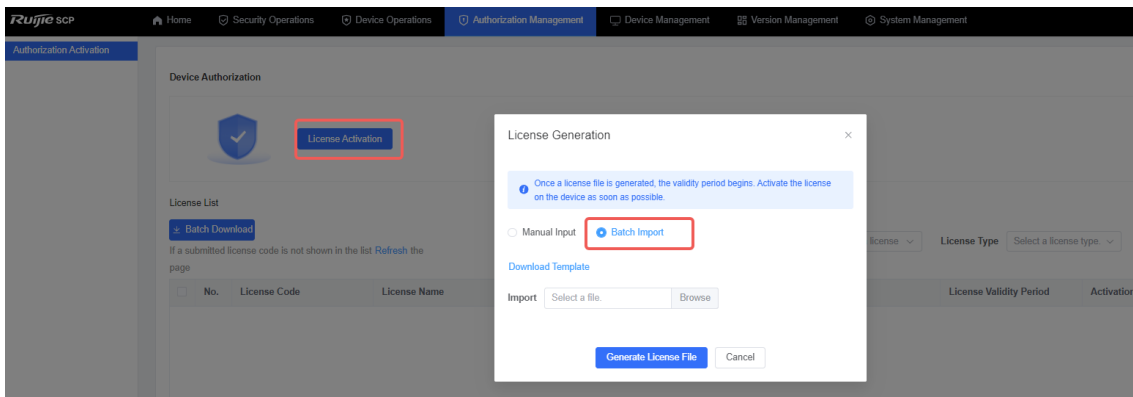
11. License Activation

- License binding
 - (1) Confirm that the current user possesses the permission on the **Authorization Management** menu.
 - (2) Log in to Ruijie Secure Cloud Platform. Choose **Authorization Management > Authorization Activation**. On the page that is displayed, click **License Activation**. In the **License Generation** dialog box that is displayed, bind licenses using one of the following methods:
 - Manually add the device SN and license code.
Click **Manual Input**, enter the device SN and license code, and click **Generate License File**.



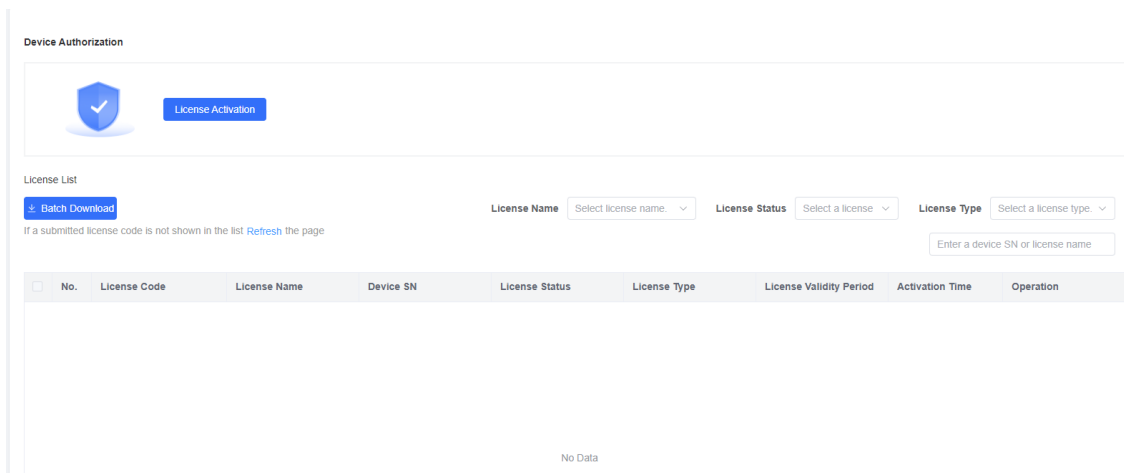
- o Batch import device SNs and license codes.

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

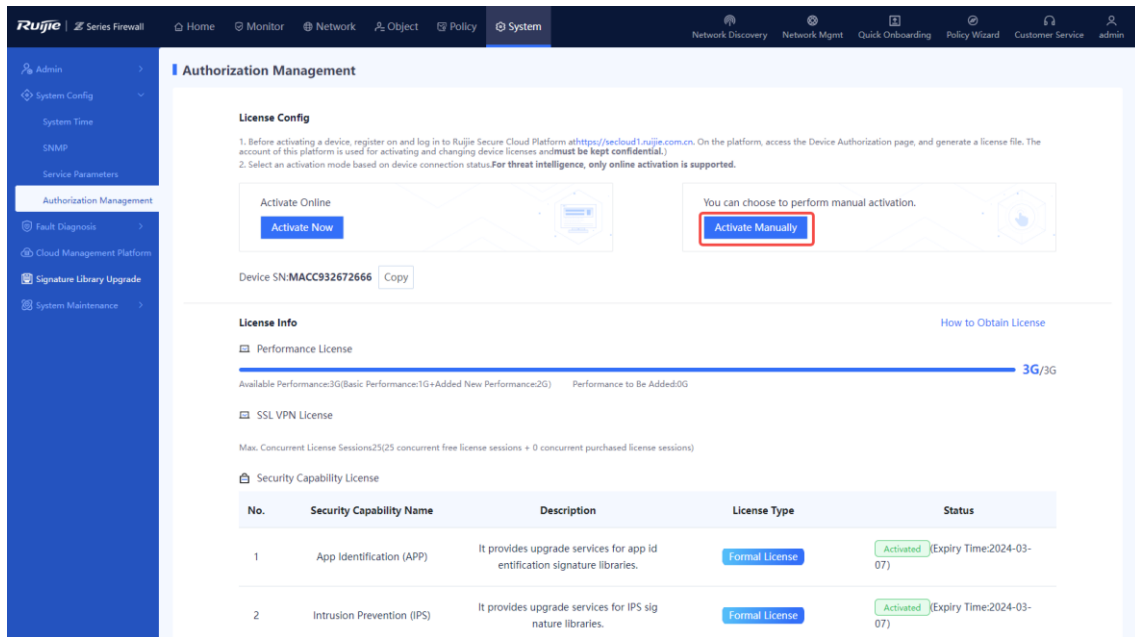


- Offline activation

- (1) Log in to Ruijie Secure Cloud Platform and bind the device SN to the license code. On the **Authorization Management** page, find the desired item in the license list, and click **Download** in the **Operation** column to download the license file.

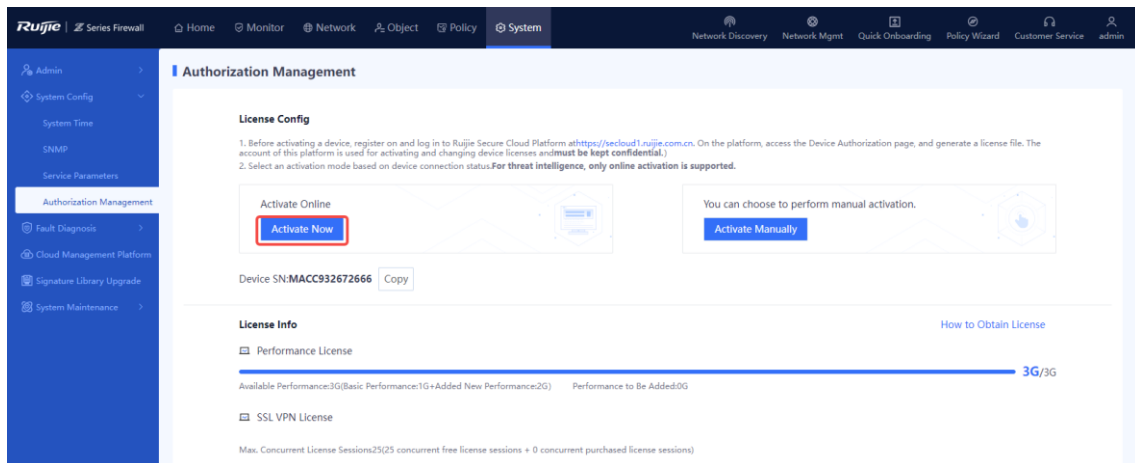


- (2) On the firewall, choose **System > System Config > Authorization Management** and click **Activate Manually** to upload the license file for offline license activation. For details, see [3.2.3 2. Manual Activation](#).



● Online activation

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



3.2.3 License Activation Methods

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

⚠ Caution

The threat intelligence function supports online license activation only.

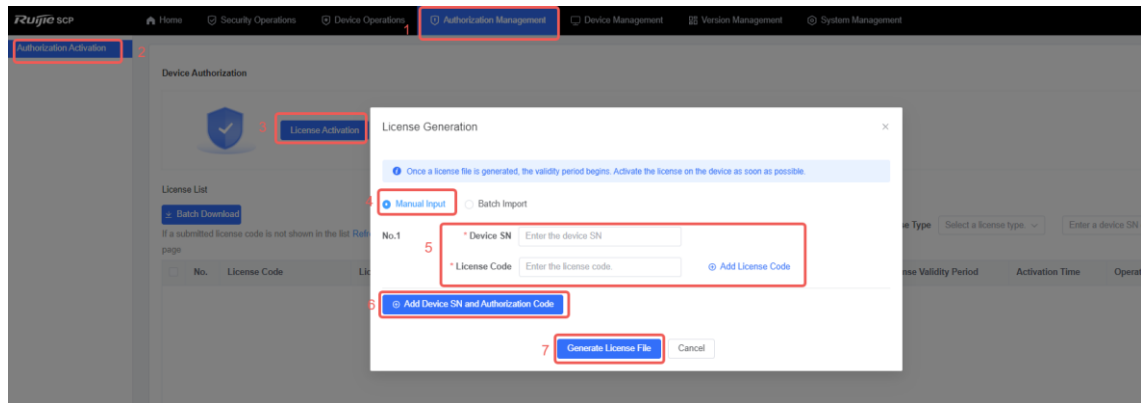
1. Automatic Activation

Application Scenario

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

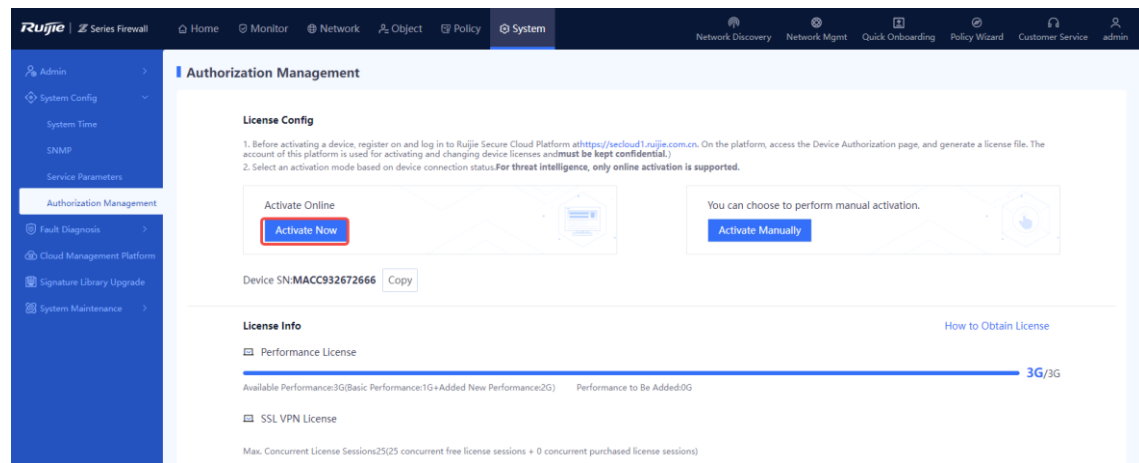
Prerequisites

- Automatic activation is supported only when the license code is within the validity period. If the license code has expired (obtaining the validity period in the license file), contact the technical support personnel.
- You have performed the following operations: Log in to Ruijie Secure Cloud Platform (<https://secloud1.ruijie.com.cn>) and choose **Authorization Management** > **Authorization Activation**. On the page that is displayed, click **License Activation** and generate a license file.



Procedure

- Log in to the firewall web UI and choose **System** > **System Config** > **Authorization Management**.
- Click **Activate Now**.



i Note

NTOS1.0R1P1 and later versions support automatic license activation after the device is connected to the Internet. After the device SN and license code are bound on Ruijie Secure Cloud Platform, you do not need to click **Activate Now** on the firewall web UI.

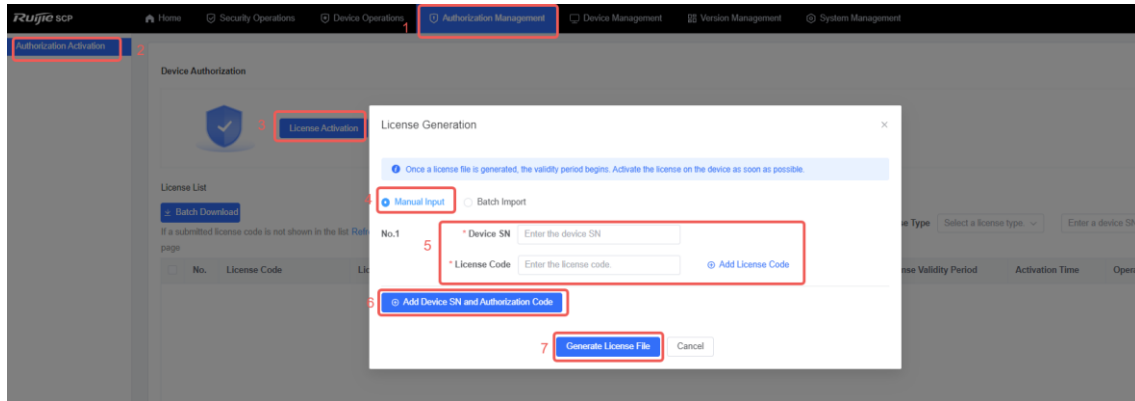
2. Manual Activation

Application Scenario

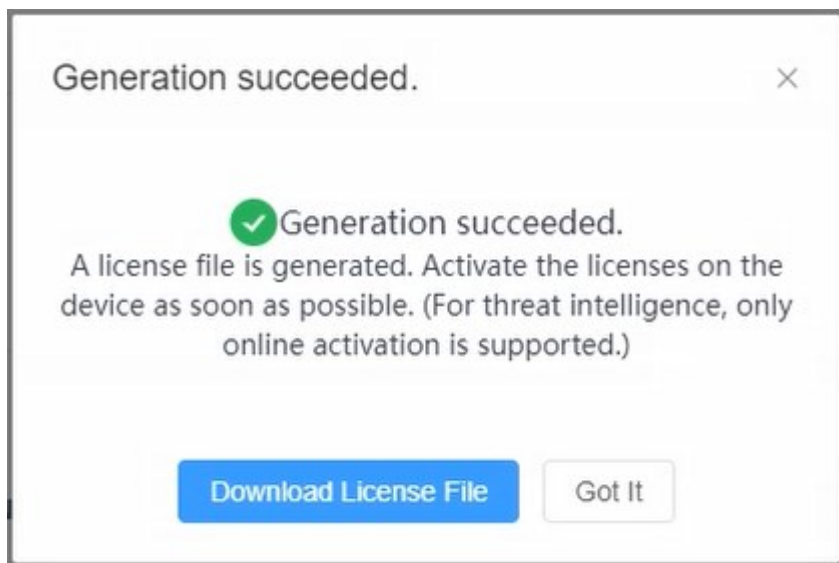
When the device is not connected to the Internet, you can use the manual activation method to manually upload a license file for activation.

Prerequisites

You have performed the following operations: Log in to Ruijie Secure Cloud Platform (<https://secloud1.ruijie.com.cn>) and choose **Authorization Management** > **Authorization Activation**. On the page that is displayed, click **License Activation**, and generate a license file.



Click **Download License File** to save the license file to the local device.



Procedure

- (1) Log in to the firewall web UI and choose **System** > **System Config** > **Authorization Management**.
- (2) Click **Activate** Manually.

The **Manual License Activation Procedure** dialog box is displayed.

Manual License Activation Procedure ⊗

1. Obtain Device Info

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

Device SN:MACC93

2. Export License File

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

3. Import License File

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

Upload

- (3) Copy the device SN and log in to Ruijie Secure Cloud Platform to export the license file.
- (4) Click **Browse**, under **Import License File** and import the downloaded license file.
- (5) Click **Activate** to activate the license.

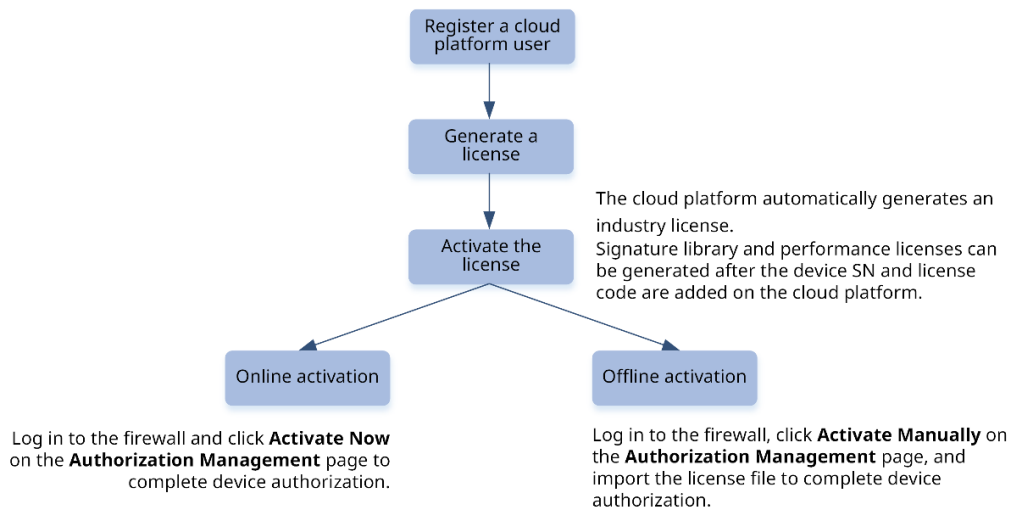
Follow-up Procedure

After license activation, check the the license activation status on the page.

3.3 Precautions for License Activation

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

- After license activation, ensure that DNS is correctly configured for the firewall and the firewall is properly connected to the Internet.
- Before license activation, log in to Ruijie Secure Cloud Platform (<https://secloud1.ruijie.com.cn>) and choose **Authorization Management > Authorization Activation**. On the page that is displayed, click **License Activation**, and generate a license file. (The account of Ruijie Secure Cloud Platform is used to activate and change licenses. Please properly keep the account information.)



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

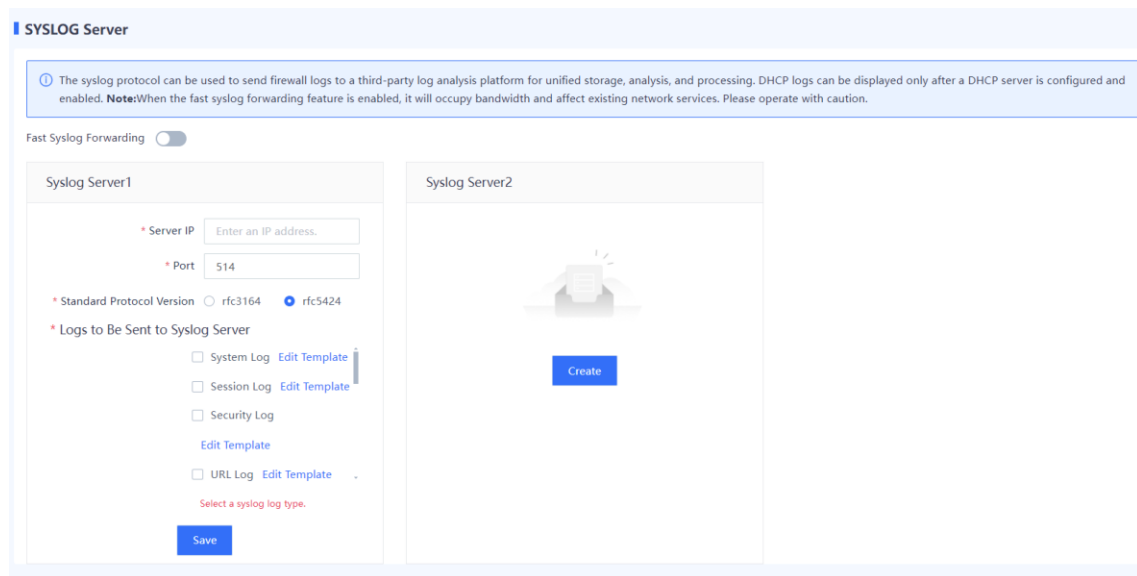
4 Configuring the Syslog Server

Application Scenario

If the firewall is not installed with a hard disk upon factory delivery, logs can only be stored in the memory (for no longer than 1 day) and all the logs in the memory will be lost after device restart. To ensure that more log information can be obtained, the system logs and security logs of the firewall can be transmitted to a third-party log platform through Syslog for storage and analysis.

Procedure

- (1) Choose **System > System Config > Syslog Server**.
- (2) Set parameters for the Syslog server.



Item	Description	Remarks
Server IP	IP address of the Syslog server.	Set this parameter to the IP address of the Syslog server.
Port	Port number for receiving the log notifications.	The default value is 514. The value must be the same as that configured on the Syslog server.
Standard Protocol Version	Protocol used for formatting logs.	Select a protocol version supported by the Syslog server. [Example] RFC5424

Logs to Be Sent to Syslog Server	Types of logs to be sent to the Syslog server.	Select specific log types to be forwarded to the server. [Example] System Log
----------------------------------	--	---

(3) Click **Save**.

5 Signature Library Upgrade

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

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

5.1 Configuring Automatic Upgrade

Application Scenario

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

Procedure

- (1) Choose System > Signature Library Upgrade.

Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time: Daily Hour Minute

Signature Library: Select All

App Identification Signature Library Virus Protection Signature Library (Deep Scan) Virus Protection Signature Library (Quick Scan) Intrusion Prevention Signature Library

ISP Address Library Threat Intelligence Signature Library URL Signature Library Behavior Analysis Signature Library

[Save](#)

Signature Library Type

[Upgrade All](#) (Upgrade all signature libraries online simultaneously)

Signature Library	Current Version	Last Upgrade Time	Latest Version	Version State	Activation State
App Identification Signature Library	20231118.1428	2023-12-08 20:06:22	Unable to obtain the latest version.	-	Activated
Virus Protection Signature Library (Deep Scan)	20231101.0604	2023-11-11 04:42:08	20231101.0604	The latest version is installed.	Activated
Virus Protection Signature Library (Quick Scan)	20231027.0201	2023-10-27 11:46:55	Unable to obtain the latest version.	-	Activated
Intrusion Prevention Signature Library	20231024.1404	2023-11-11 04:46:16	20231024.1404	The latest version is installed.	-
ISP Address Library	20221202.1005	-	Unable to obtain the latest version.	-	-
Threat Intelligence Signature Library	20231101.0350	2023-11-11 04:47:27	20231101.0350	The latest version is installed.	-

The system displays information about the current signature libraries:

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

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

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

- a Set the time for automatic upgrade.
You are advised to configure an off-peak period.
- b Select the type of signature library to be upgraded.

(3) Click **Save**.

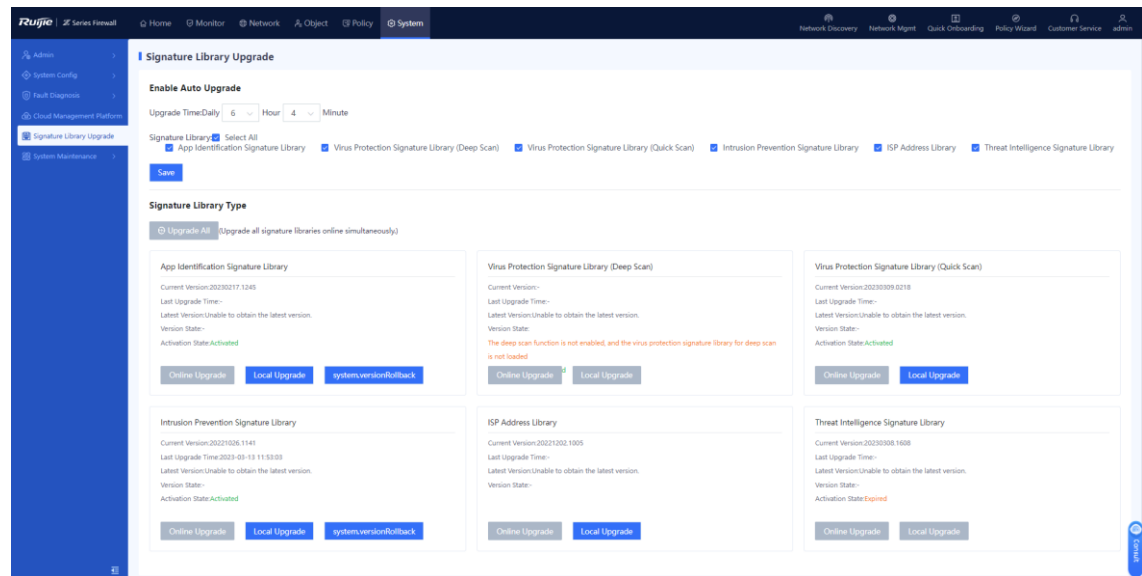
5.2 Local Manual Upgrade

Application Scenario

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

Procedure

(1) Choose System > Signature Library Upgrade.



The system displays information about the current signature libraries:

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

(2) Perform local manual upgrade.

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

Signature Library Type

Upgrade All (Upgrade all signature libraries online simultaneously)

App Identification Signature Library

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

Virus Protection Signature Library (Deep Scan)

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

Intrusion Prevention Signature Library

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

ISP Address Library

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

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

Local Upgrade ⊗

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

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

Import

- c Click **Browse** to import the upgrade file.
- d Click **Upgrade Now**.

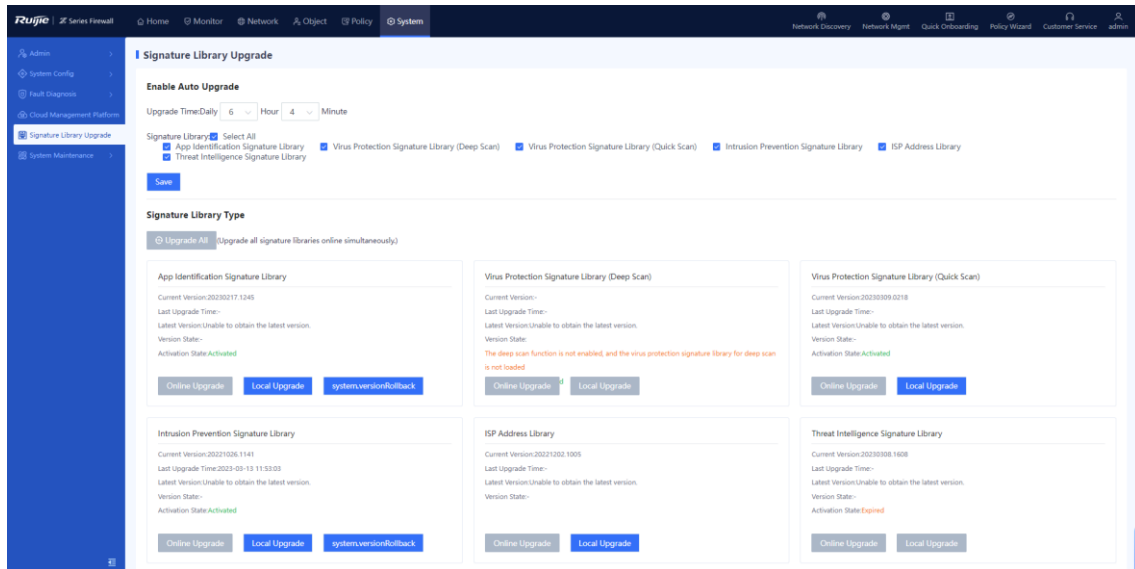
5.3 Online Automatic Upgrade

Application Scenario

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

Procedure

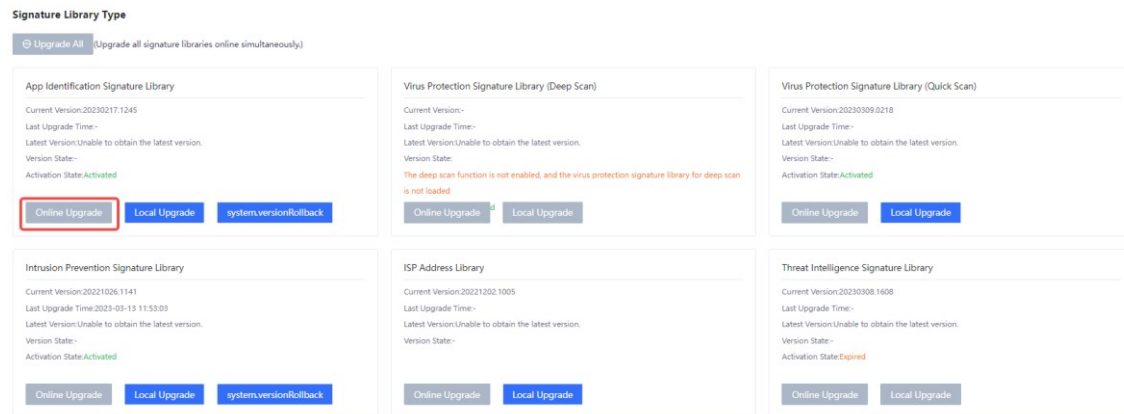
(1) Choose System > Signature Library Upgrade.



The system displays information about the current signature libraries:

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

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



Note

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

6 Version Upgrade

6.1 Overview

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

Description of firewall software version:

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

The following describes information of a sample release version.

Note

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

File Name	NGFW_NTOS1.0R7_Z3200-S_04130623_install.bin
File Description	System upgrade installation package, universal version
File Size	168,187,952 bytes
Applicable Product	RG-WALL-1600-Z3200-S
MD5 Value	7c2025e9642b3de1d09643e0d314675f
Software Version	NGFW_NTOS1.0R7, Release(04130623)

Caution

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

6.2 Upgrade Operations

Note

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

6.2.1 Offline Upgrade

Application Scenario

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

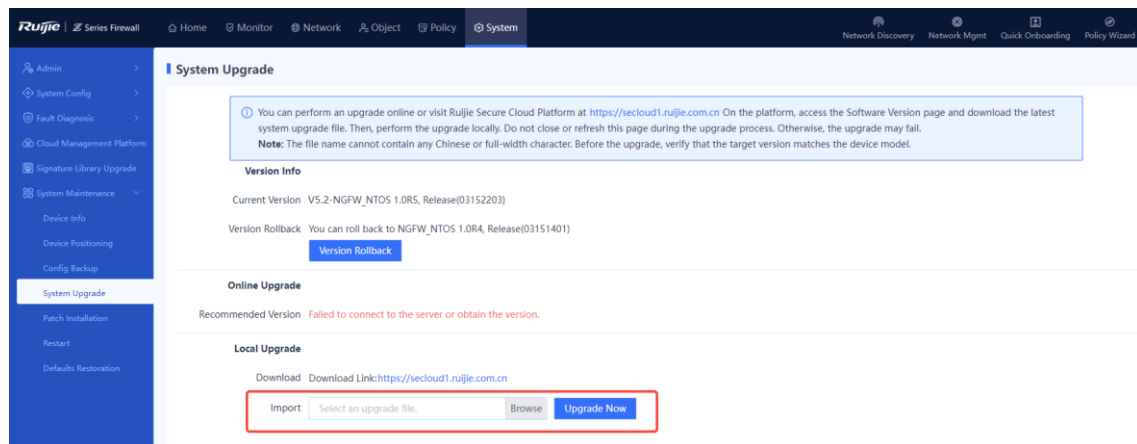
Prerequisites

An upgrade file is obtained in advance.

Procedure

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

The **System Upgrade** page is displayed.



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

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

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

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

Follow-up Procedure

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

⚠ Caution

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

6.2.2 Online Upgrade

Application Scenario

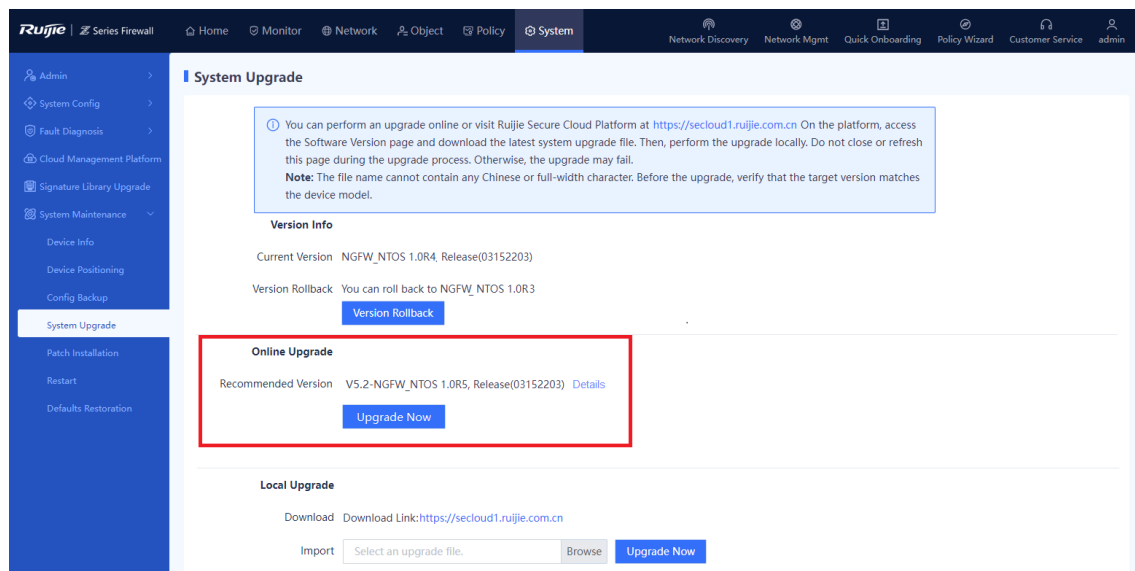
When the network communication is normal and the system displays a recommended version, you can upgrade the software version in online mode.

Procedure

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

The **System Upgrade** page is displayed.

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



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

The system starts system upgrade automatically.

Follow-up Procedure

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

⚠ Caution

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

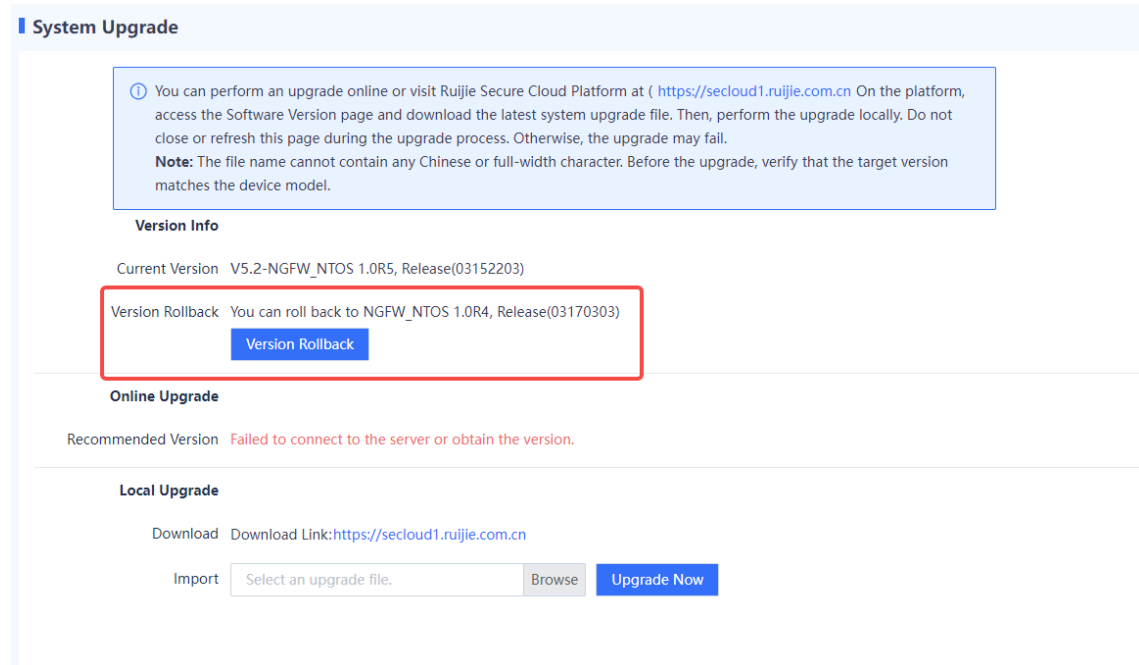
6.2.3 Version Rollback

Application Scenario

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

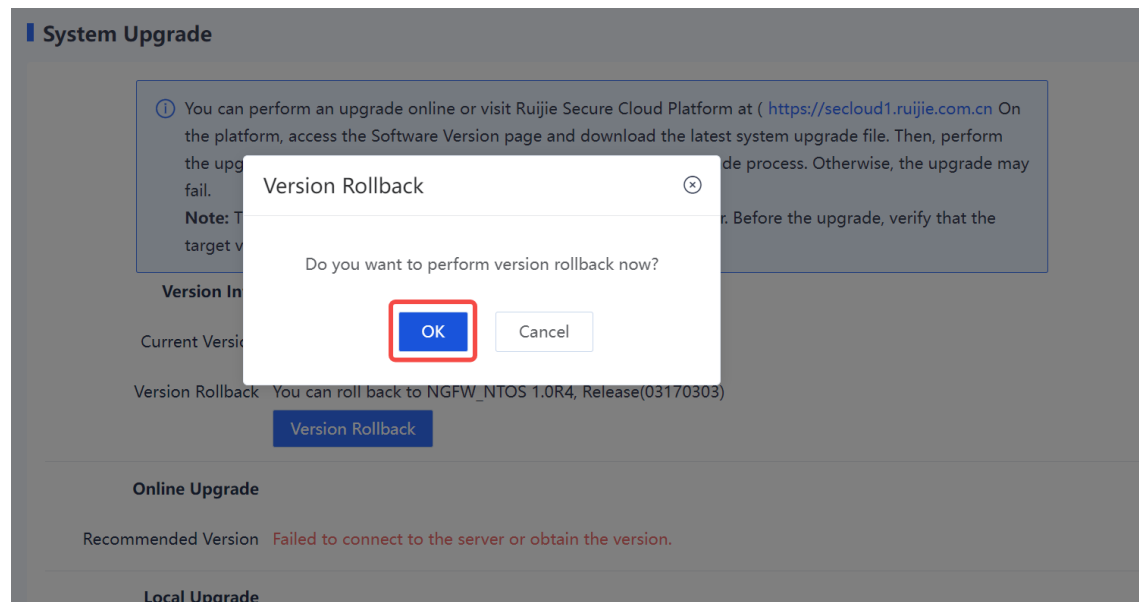
Procedure

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



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

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



7 Configuration Examples for Typical Scenarios

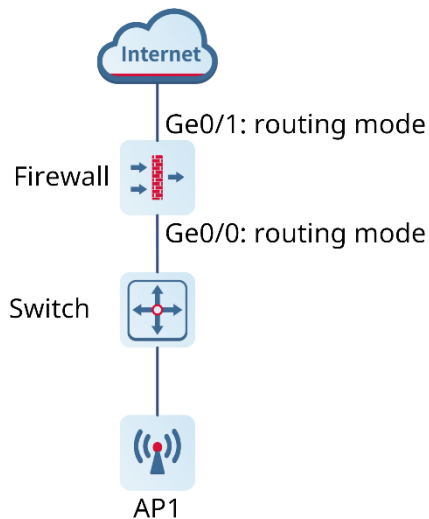
7.1 Integrated Deployment on Ruijie Cloud

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

7.1.1 Firewall Deployment (Routing Mode)

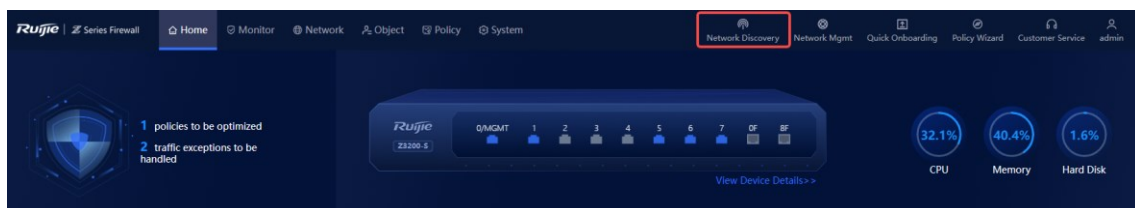
1. Application Scenario

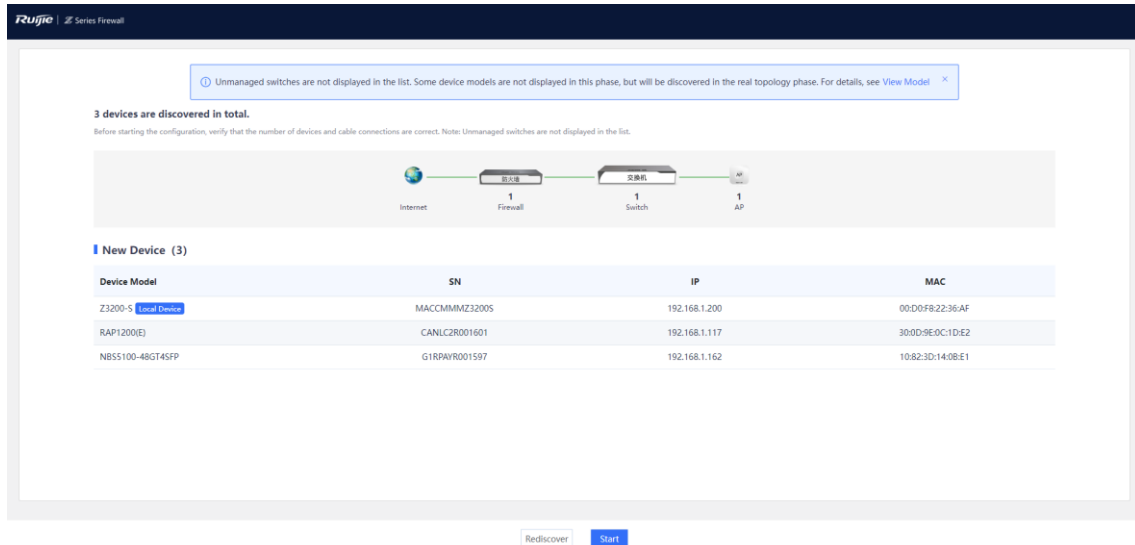
The firewall functions as an egress router and it is uplinked to the Internet and downlinked to a switch. You are advised to deploy the firewall in routing mode. The uplink interface is configured to work in routing mode to access the Internet and the downlink interface is configured to work in routing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



2. Procedure

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

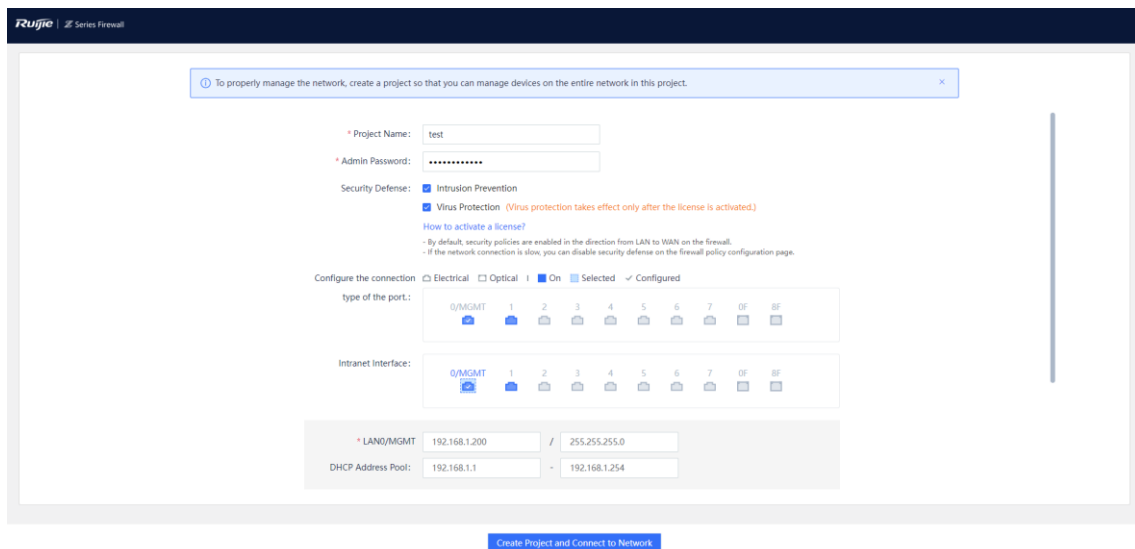


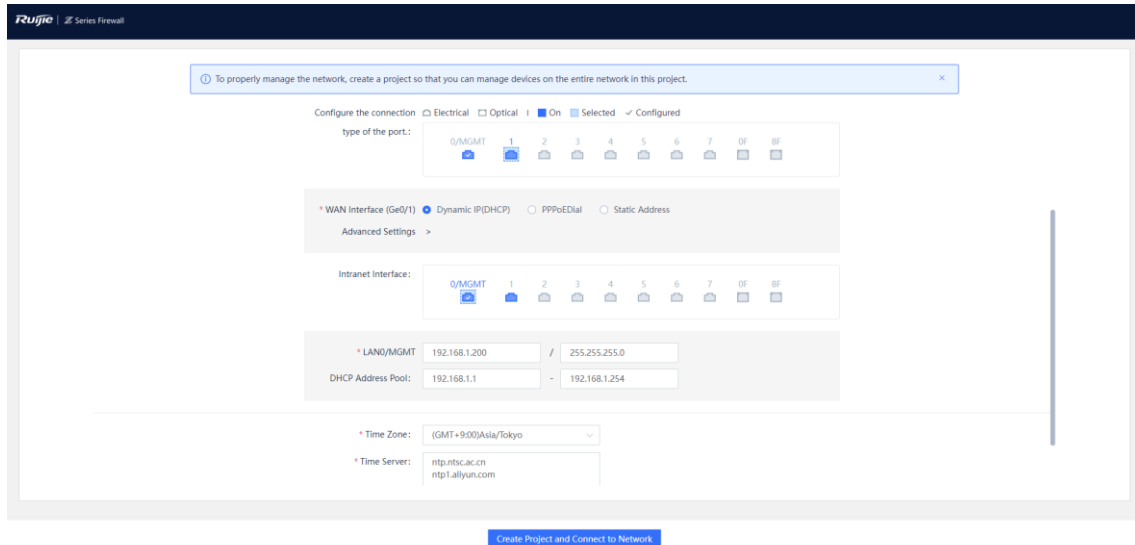


(2) Click **Start**. Enter the network project name and configure a port IP address as prompted.

Note

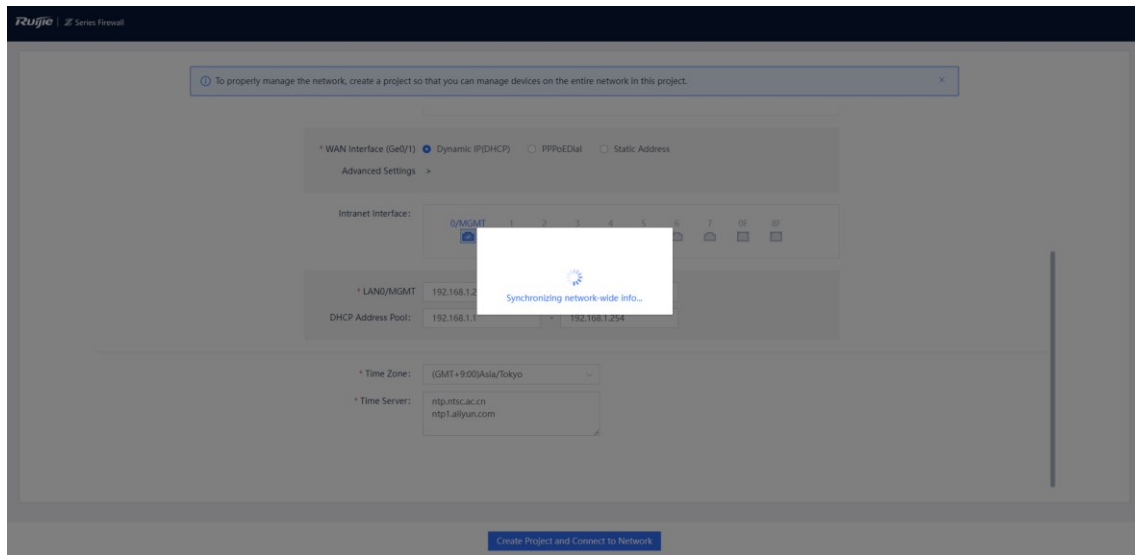
- The DHCP server function is enabled on the firewall by default, and the default DHCP address pool is configured on the management port.
- Intrusion prevention and virus protection are enabled on the firewall by default. You can choose to disable these functions based on actual needs. The virus protection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





Item	Description	Remarks
WAN Interface	<p>Connects the firewall to the Internet. Generally, the WAN interface is directly connected to the fiber to the home (FTTH) Optical Network Unit (ONU) of the ISP.</p> <p>Three methods are available for a WAN interface to obtain an IP address:</p> <ul style="list-style-type: none"> ● Dynamic IP (DHCP): Applicable when no professional network administrator is available. The user terminal automatically obtains an IP address to access the Internet after the terminal is connected to the firewall. ● PPPoE: Applicable for dialup access to the ISP network. The username and password of the dialup user must be configured. ● Static Address: Applicable when the network administrator specifies an IP address for the device based on the predefined IP address planning. This connection type requires the network administrator to possess certain network knowledge. The IP address/mask and next-hop address must be configured. 	<p>[Example]</p> <p>Ge0/1</p> <p>Dynamic IP (DHCP)</p>
LAN Interface	<p>Connects to the LAN. The LAN interface IP address must be configured based on the predefined IP address planning.</p>	<p>[Example]</p> <p>192.168.1.1/24</p>

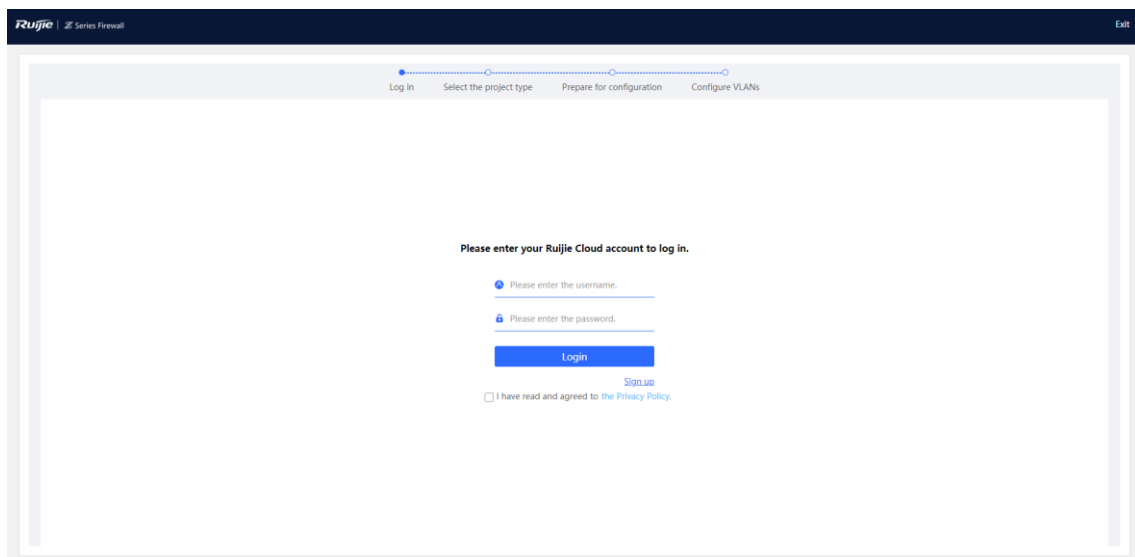
(3) Click **Create Project and Connect to Network**. The system delivers configuration information.



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

i Note

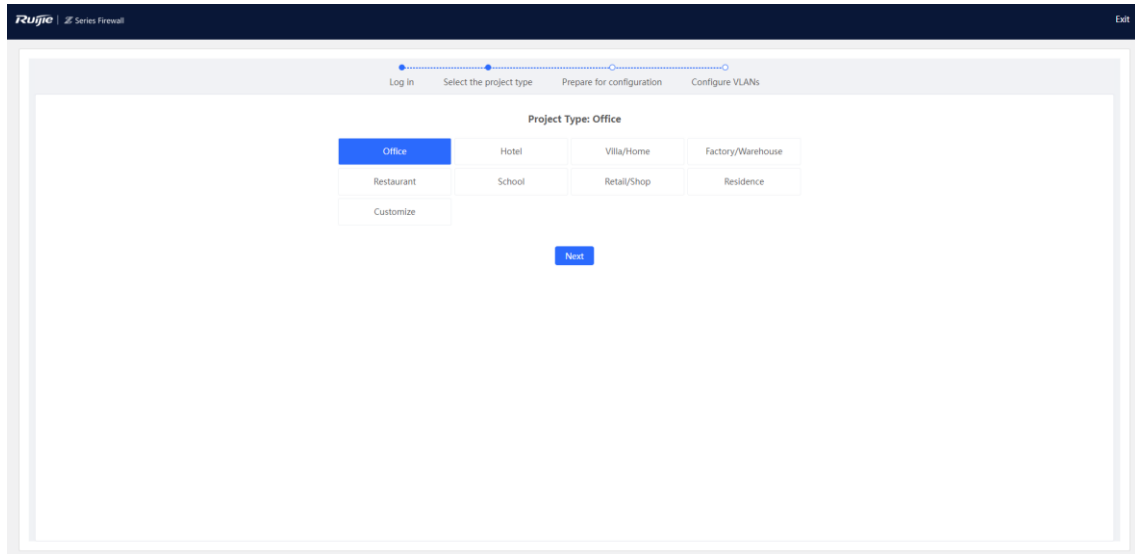
After successful configuration, the firewall automatically adds the IP address of the DHCP server in the networking to the allowlist and generates a security policy (with the name **trust-untrust** and enabled with intrusion prevention).



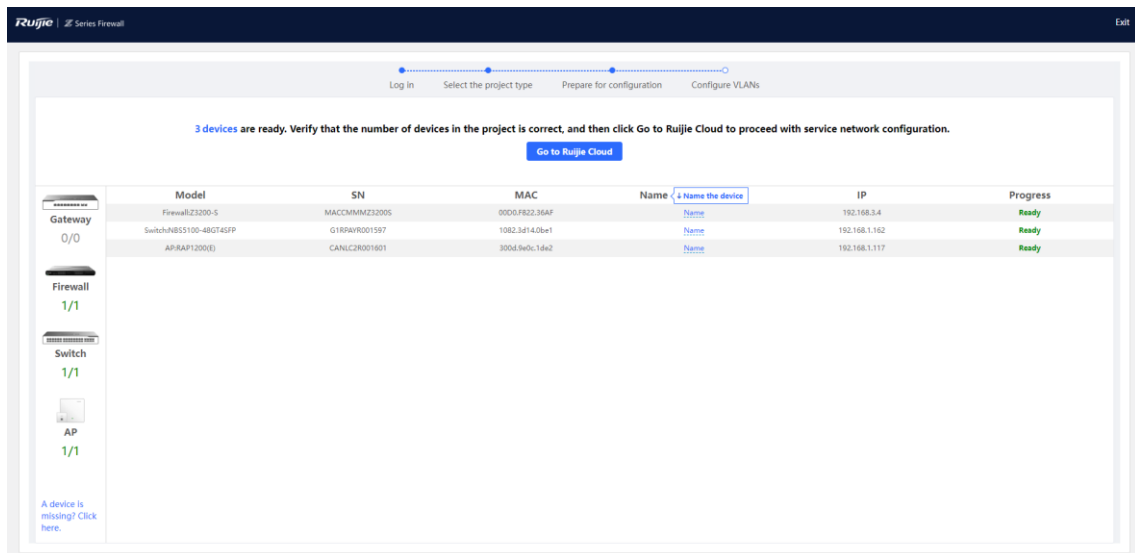
i Note

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

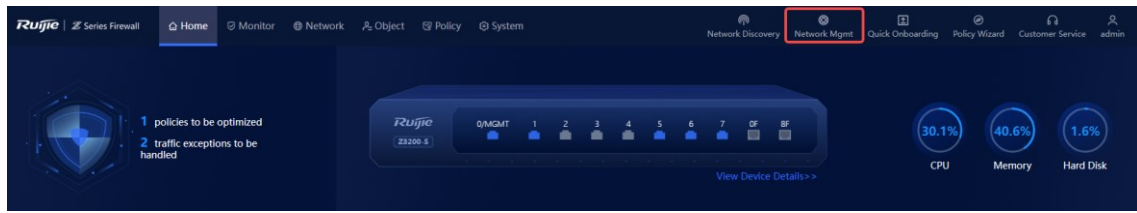
- After successful login, select a project type based on the actual networking scenario and click **Next**. The initial configuration delivered varies by the project type, so the project type must be set based on the actual service scenario.



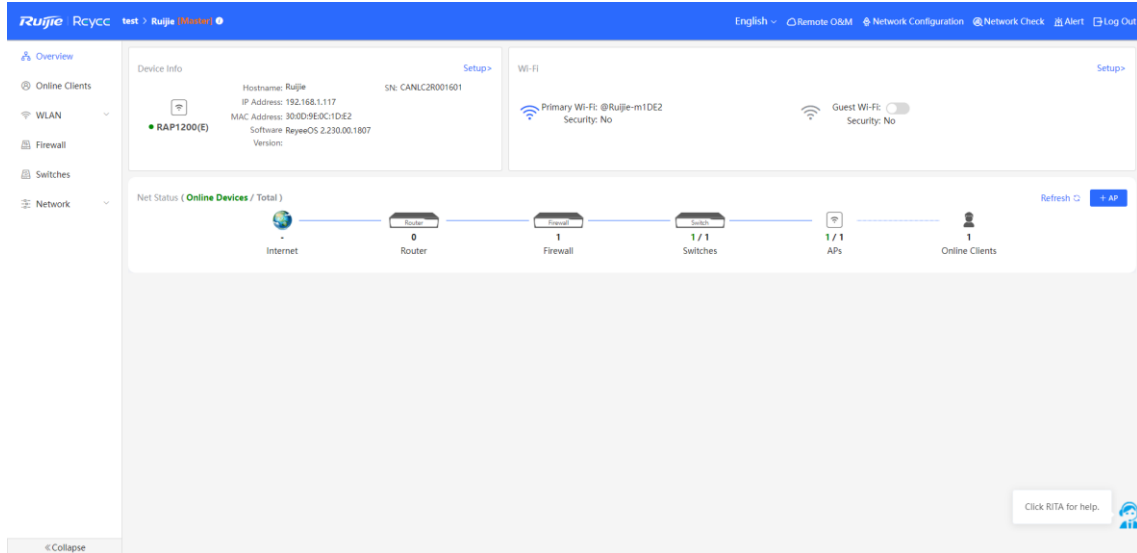
- Wait until preparations before configuration are complete and then configure the service network.
- After all devices go online, click **Go to the cloud platform for management** and perform service configuration on the Ruijie Cloud platform.



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



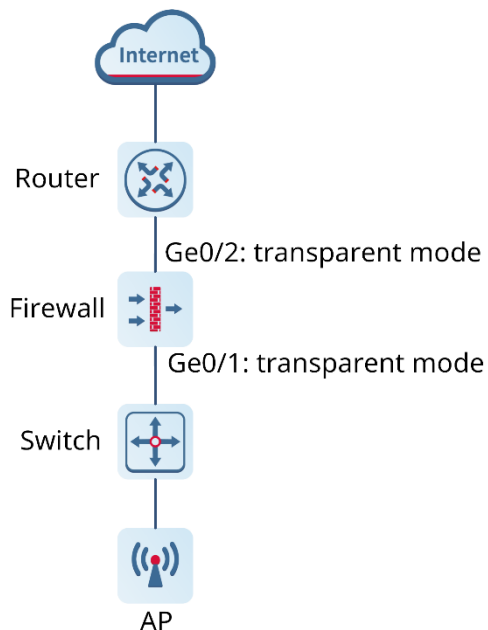
The following figure shows the **Overview** page of the master device.



7.1.2 NBR Deployment (Transparent Mode)

1. Application Scenario

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



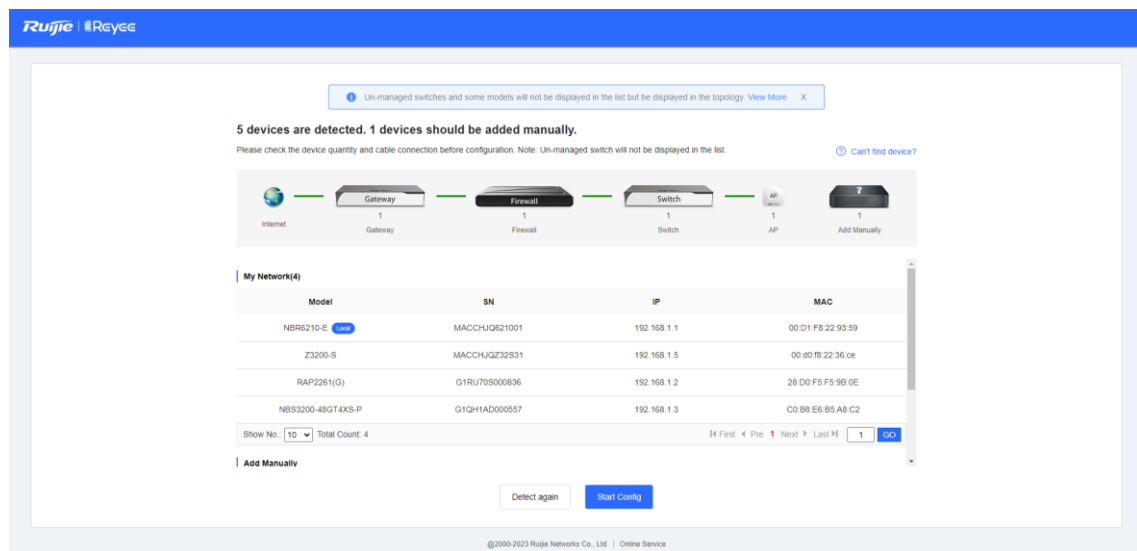
2. Procedure

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

Note

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

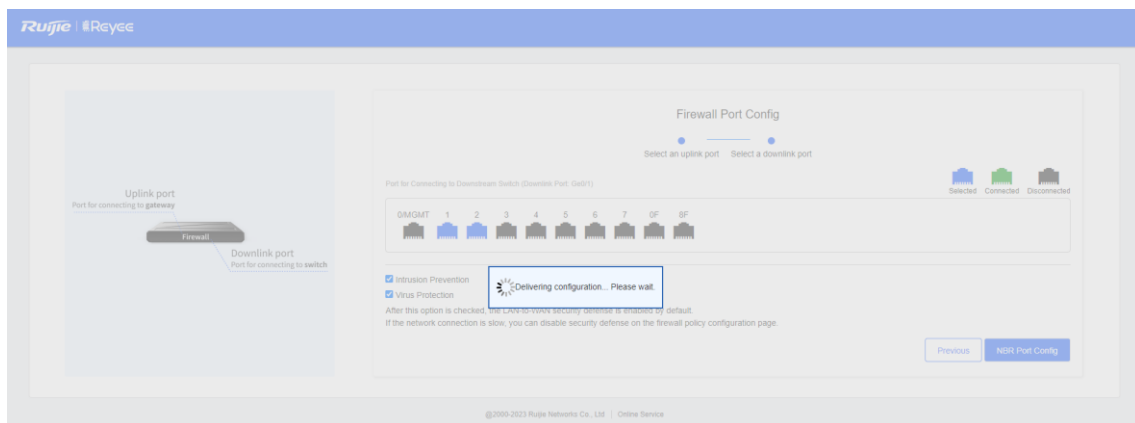
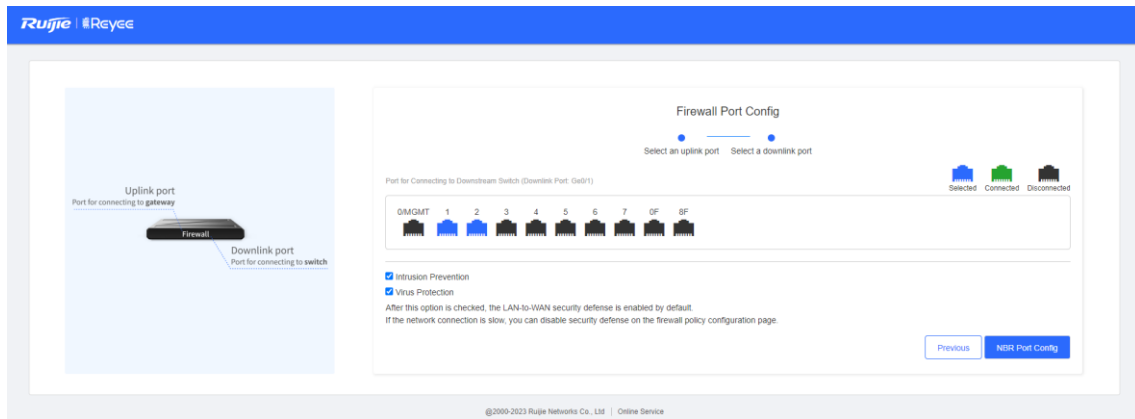
- (2) Log in to the web page of the NBR. The following page is displayed by default. Click **Start**.



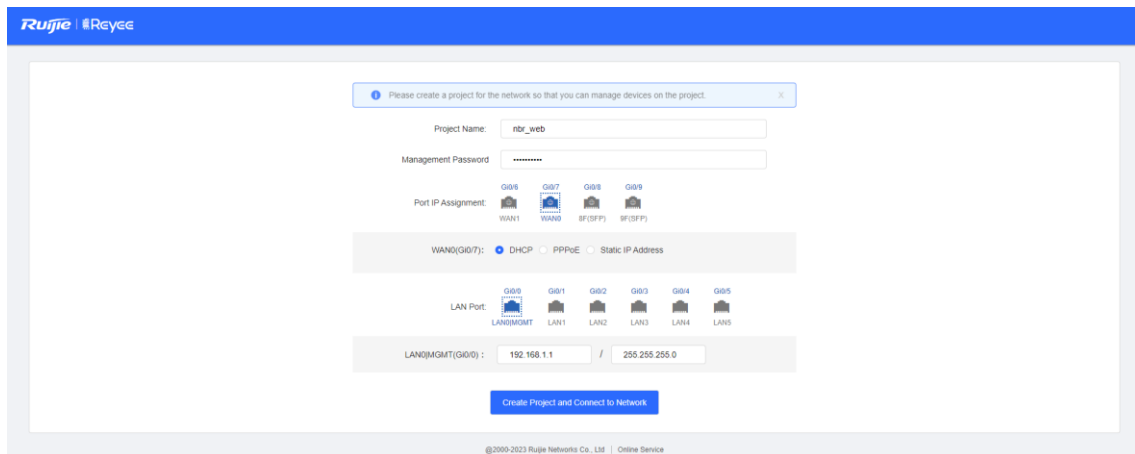
- (3) Select the WAN interface (interface connected to the gateway, Ge0/2 in this example) of the firewall based on the actual networking and click **Next**.



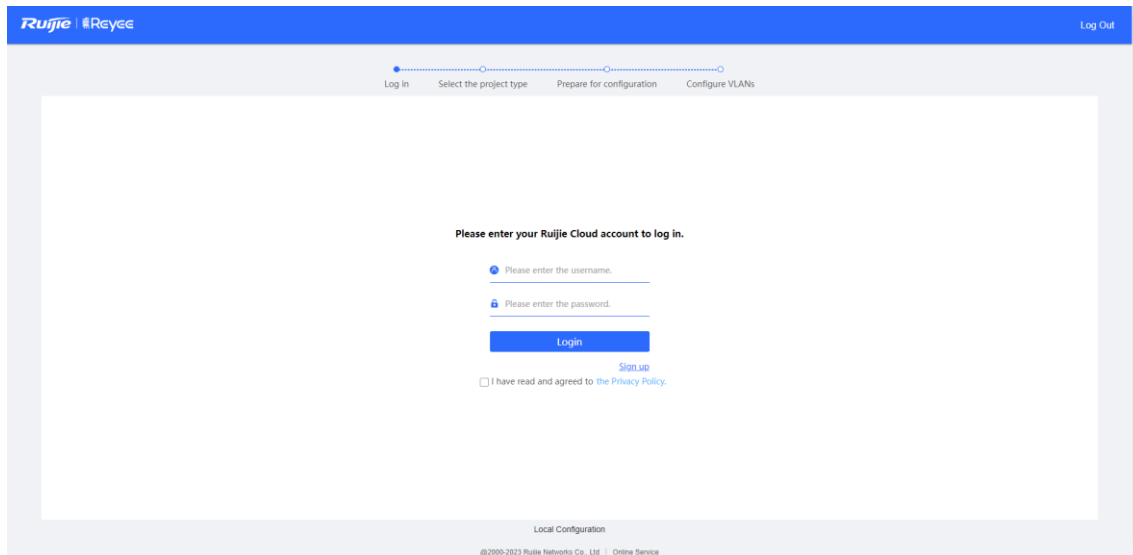
- (4) Select the LAN interface (interface connected to the switch, Ge0/1 in this example) of the firewall based on the actual networking and click **NBR Port Config**.



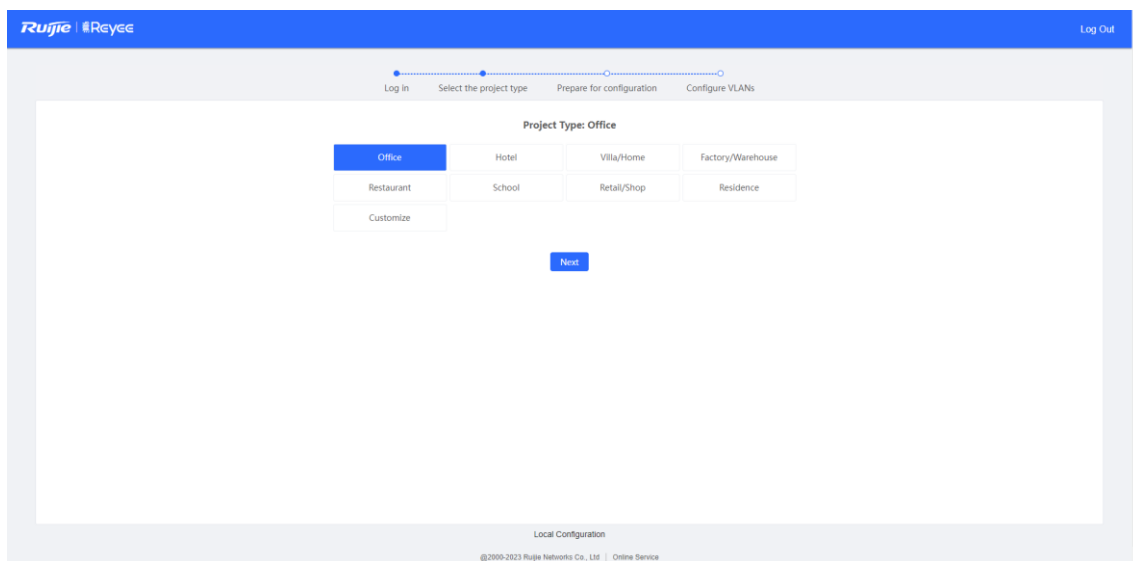
- (5) After successful configuration delivery, the following page is displayed. On this page, enter the project name and management password and click **Create Project and Connect to Network**.



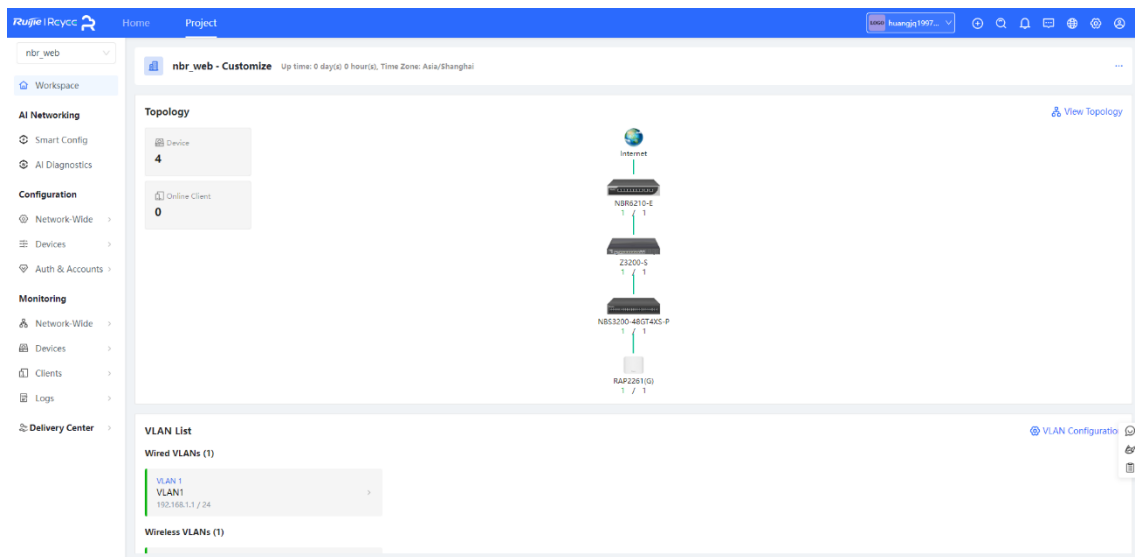
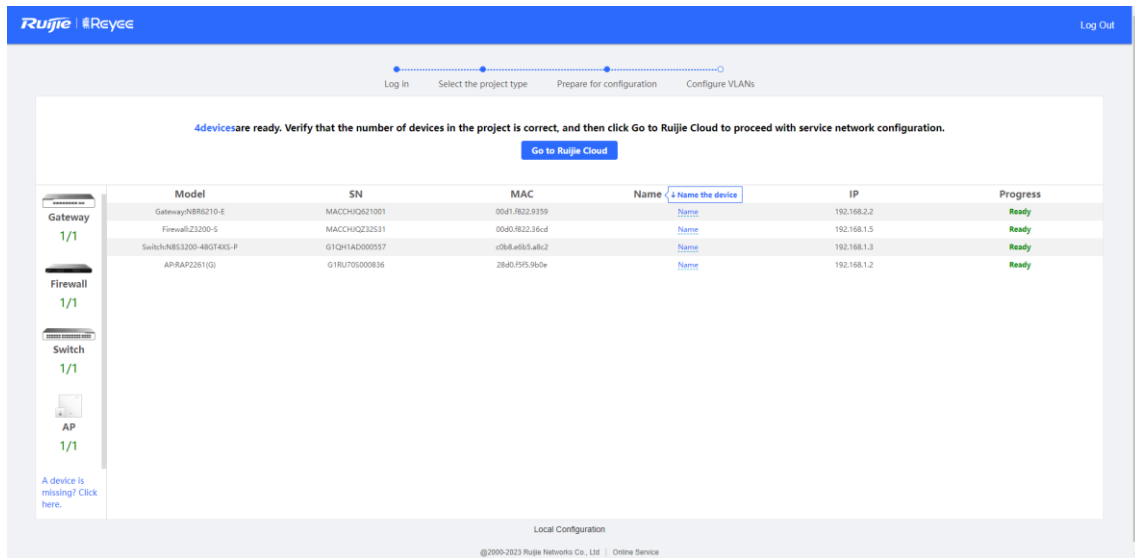
- (6) Check the system prompt. A prompt indicating successful configuration is displayed after the configurations are completed. You can scan the username and password to log in to Ruijie Cloud and migrate the firewall to the cloud.



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



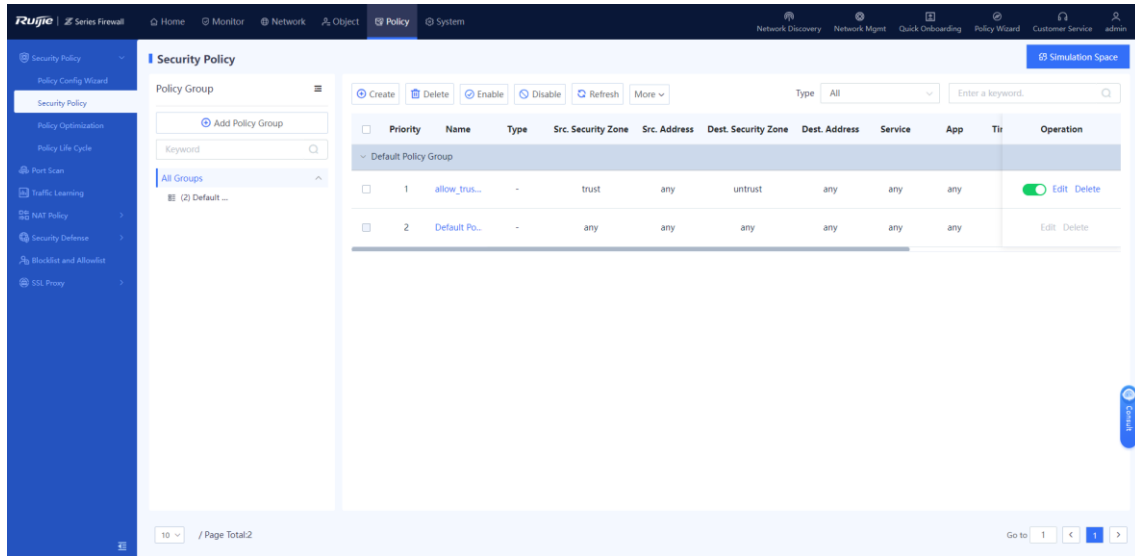
- (8) Wait until preparations before configuration are complete and then configure the service network.
- (9) After all devices go online, click **Go to the cloud platform for management** and perform service configuration (such as interfaces and routes) on the Ruijie Cloud platform.



Note

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

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



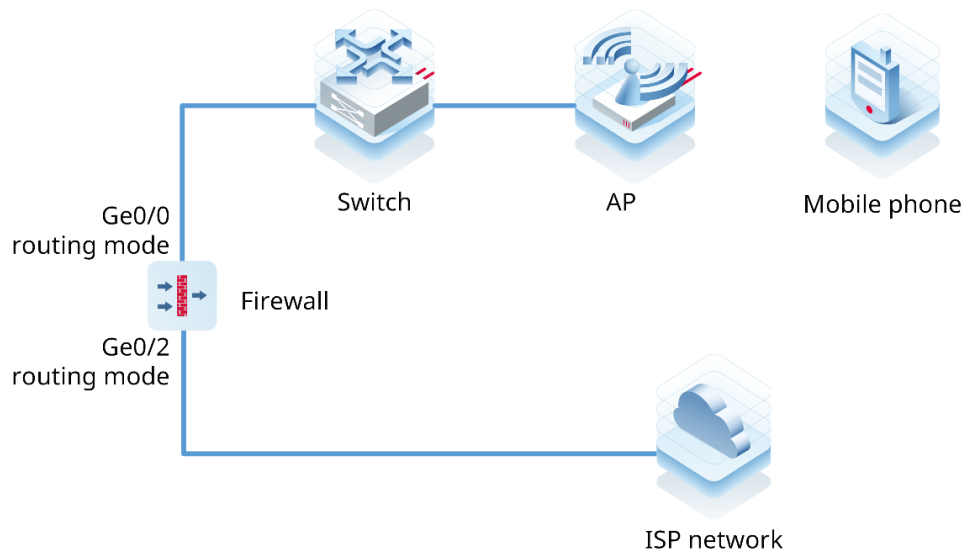
7.1.3 Deployment Using Ruijie Cloud App (Routing Mode)

1. Application Scenario

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

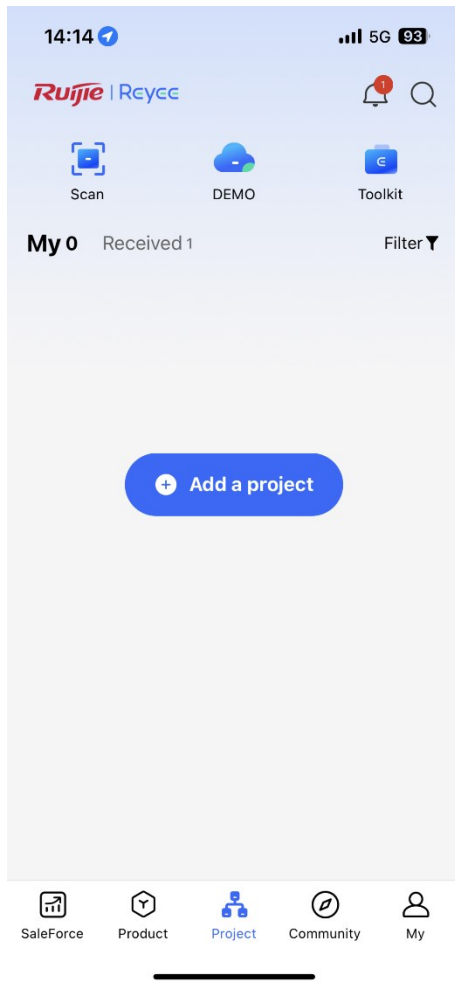
Note

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

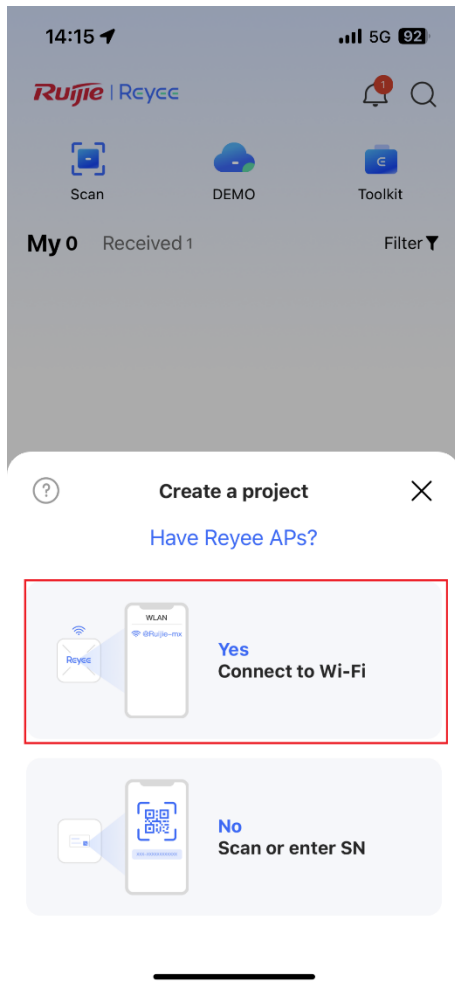


2. Procedure

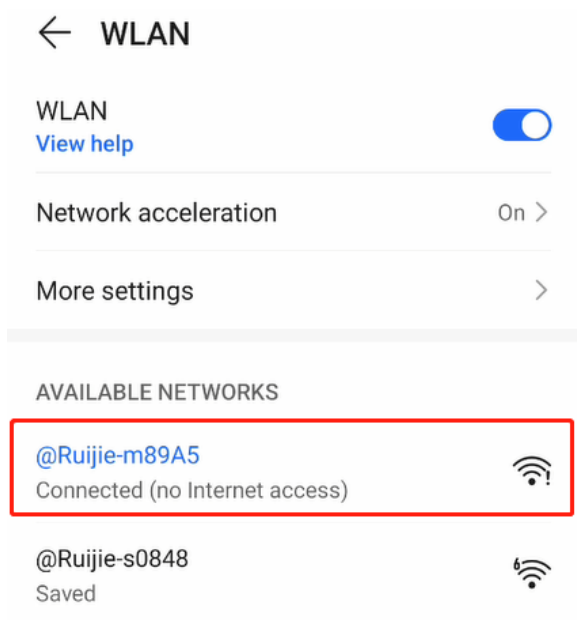
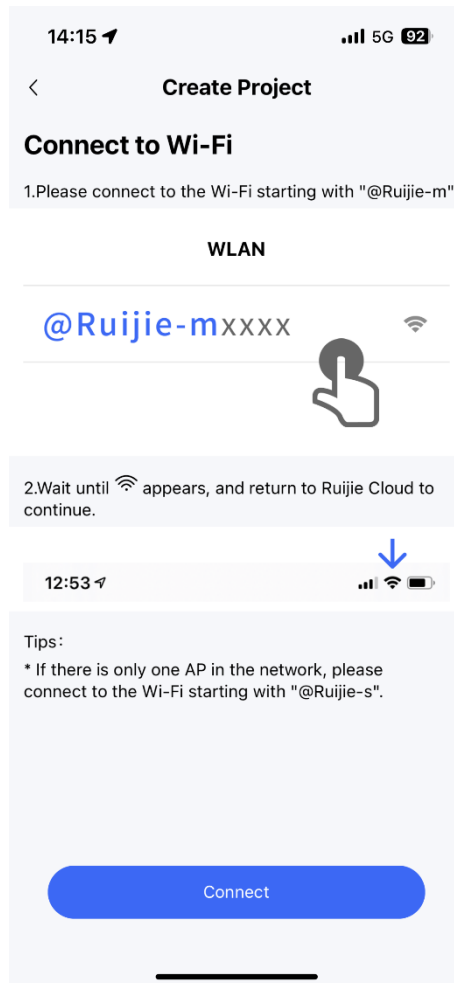
- (1) After the network environment is established according to the preceding figure, start the Ruijie Cloud app and choose **Project > Add a project**.



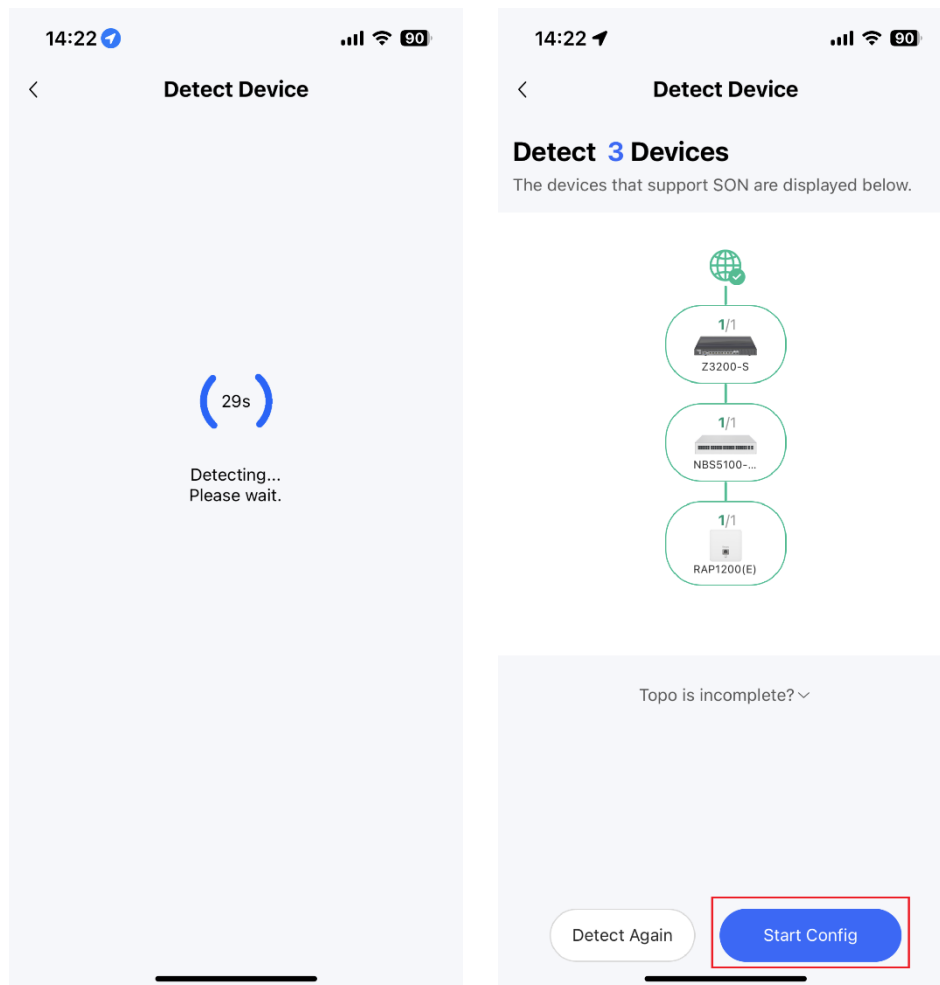
(2) Select **Connect to Wi-Fi** and add a project.



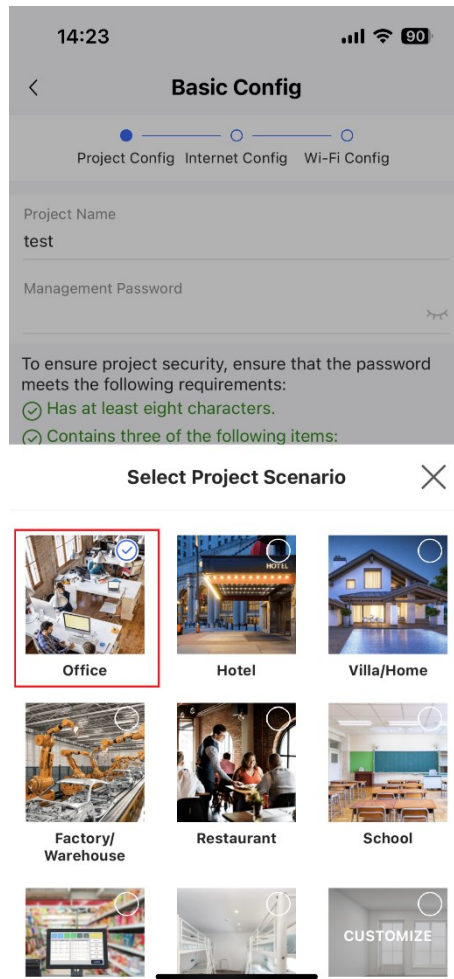
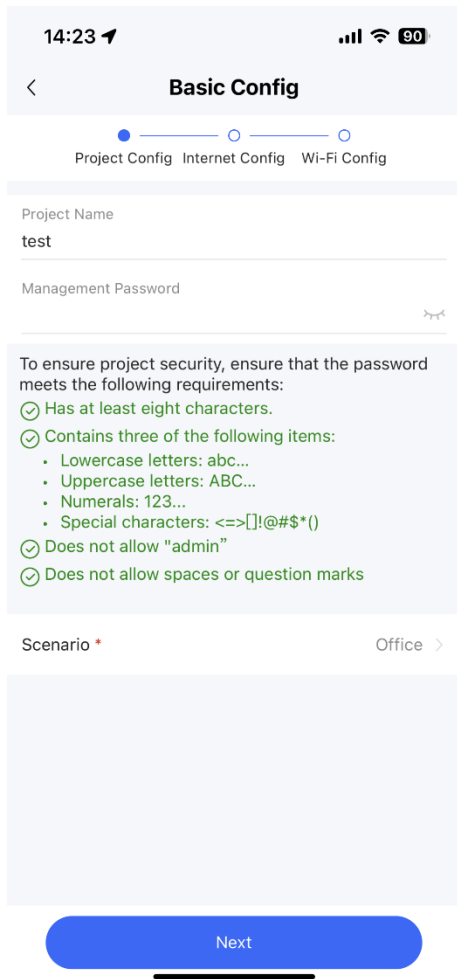
(3) Tap **Connect** to connect to the Wi-Fi signal of the Reyee AP.



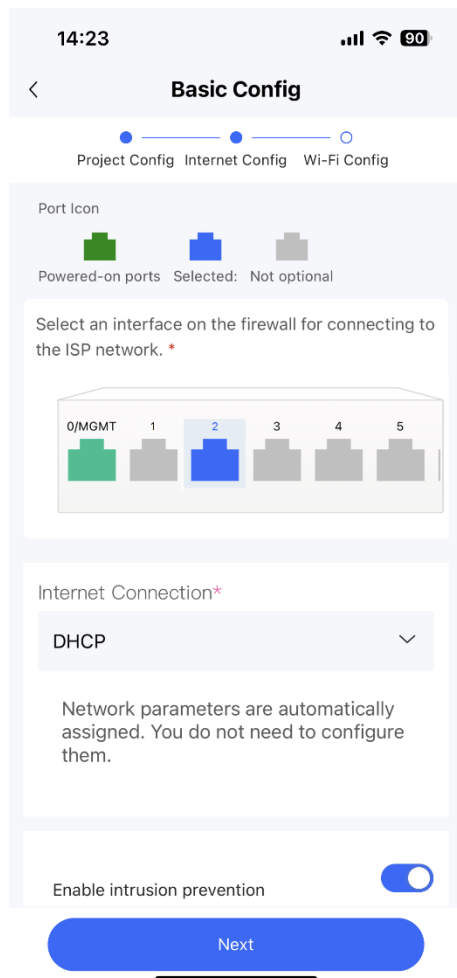
(4) Wait for about 30s until the system automatically generates the network topology. Then, tap **Start Config**.



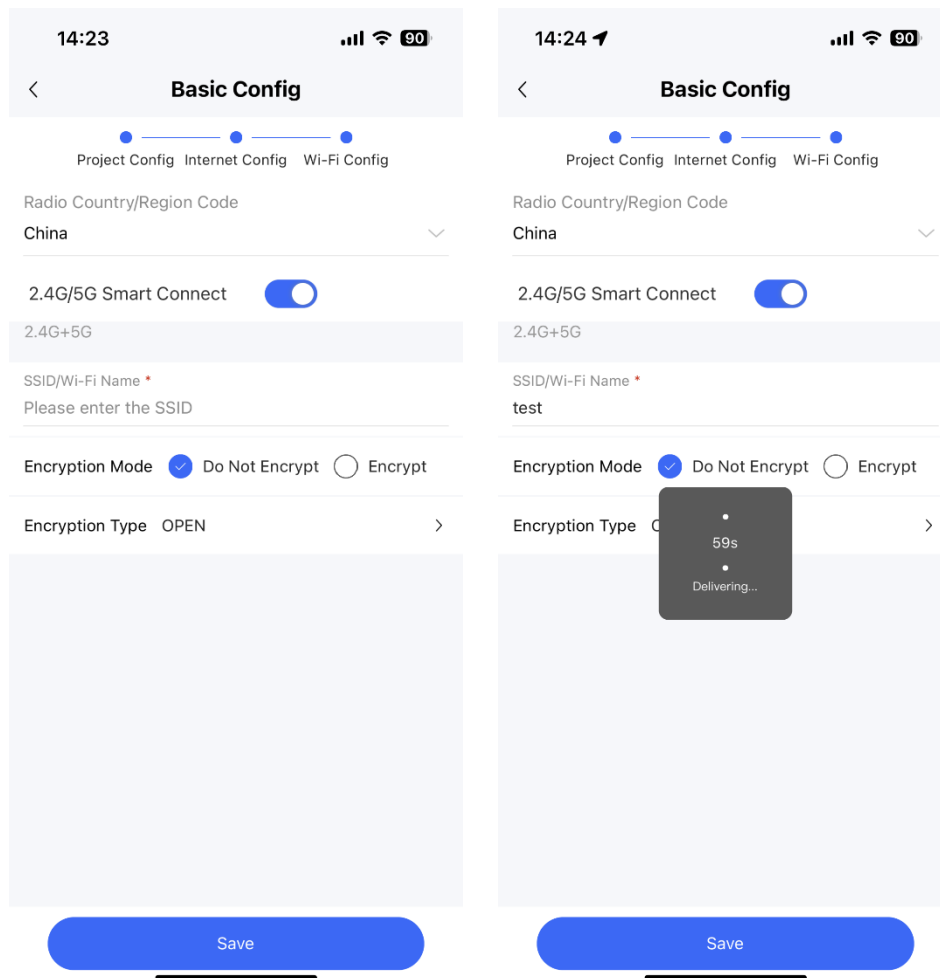
(5) Enter the project name and password and tap **Next**.



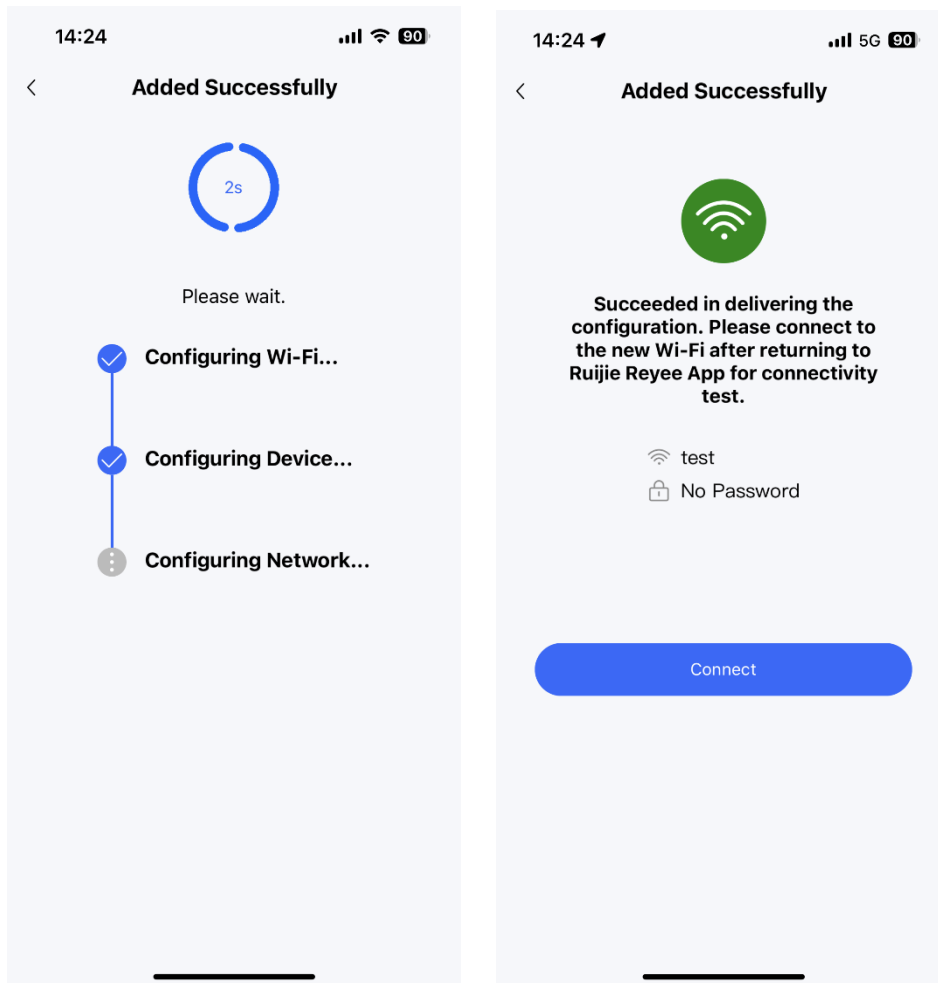
(6) Select the firewall interface (WAN interface) connected to the Internet, set an Internet access method, and tap **Next**.



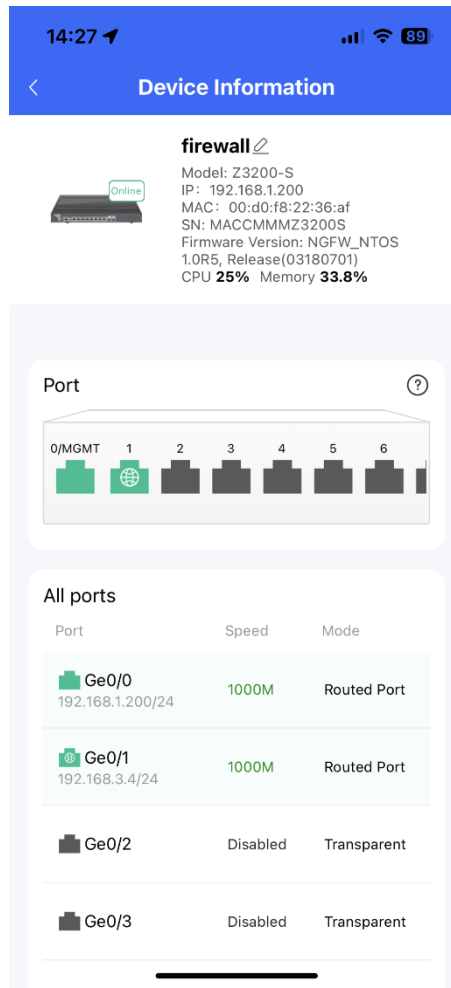
(7) Set the Wi-Fi name and password and tap **Save**.



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



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



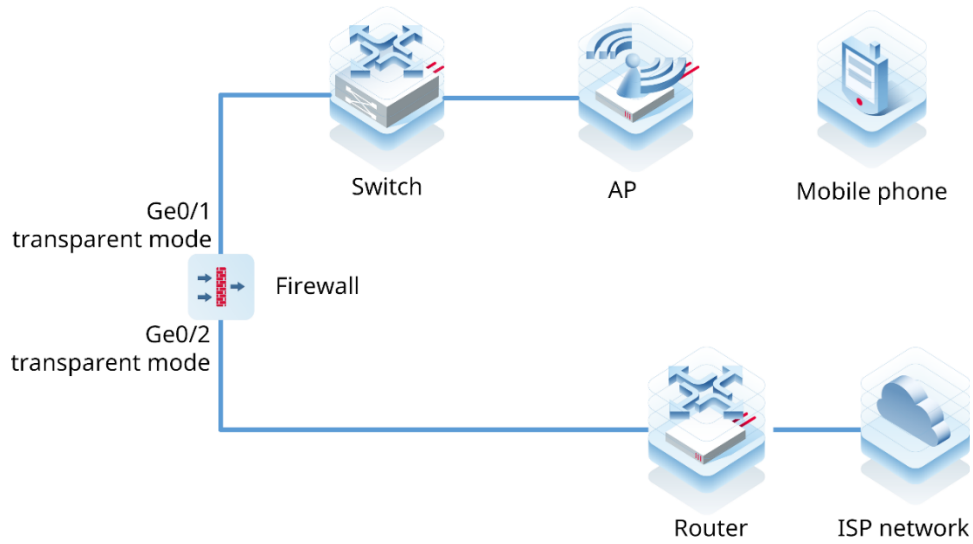
7.1.4 Deployment Using Ruijie Cloud App (Transparent Mode)

1. Application Scenario

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

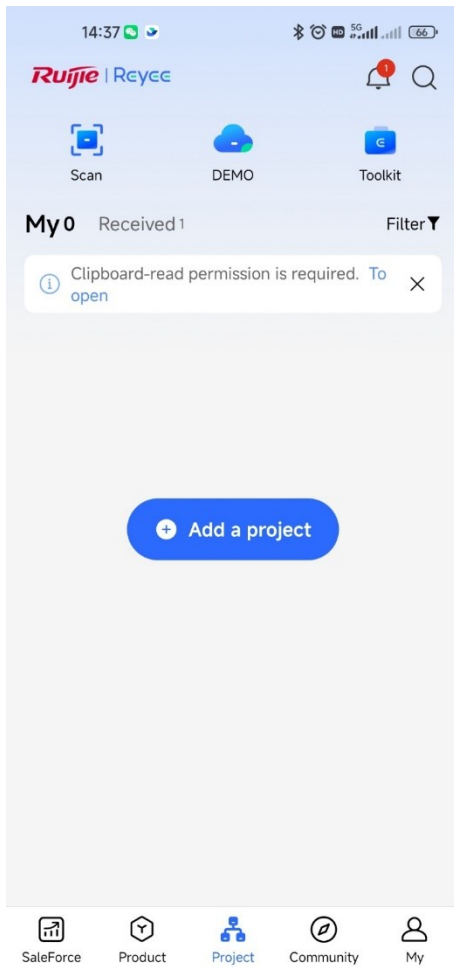
i Note

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

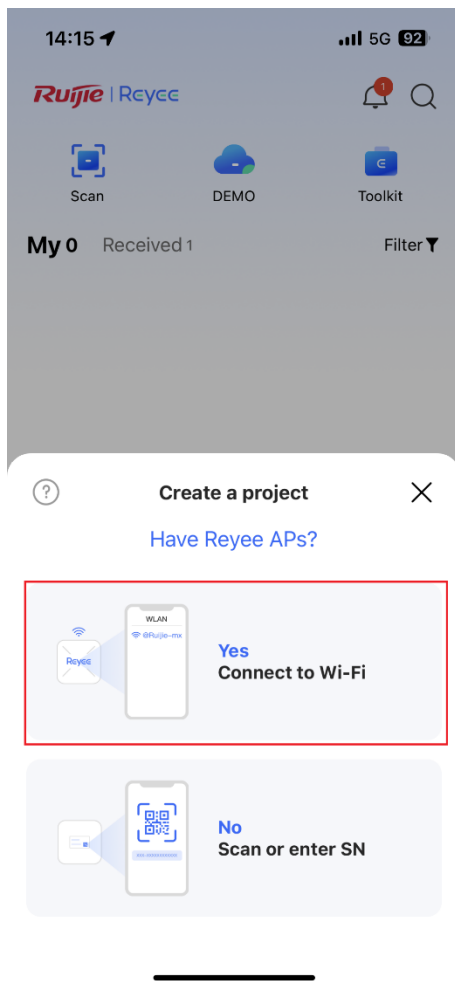


2. Procedure

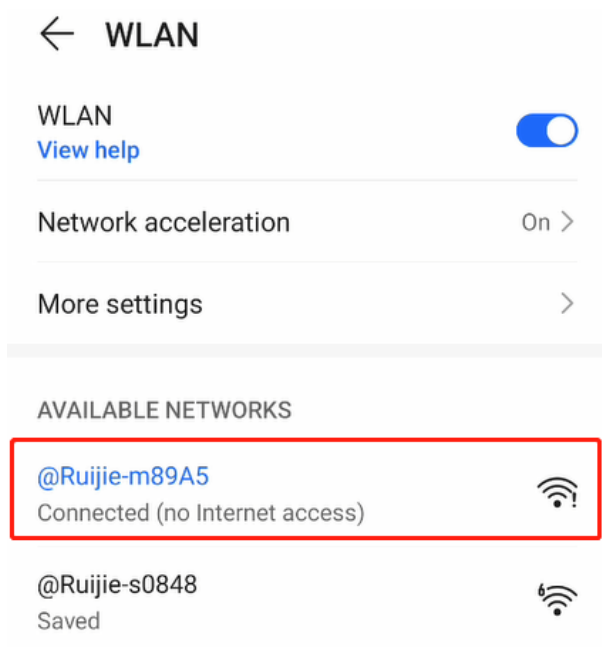
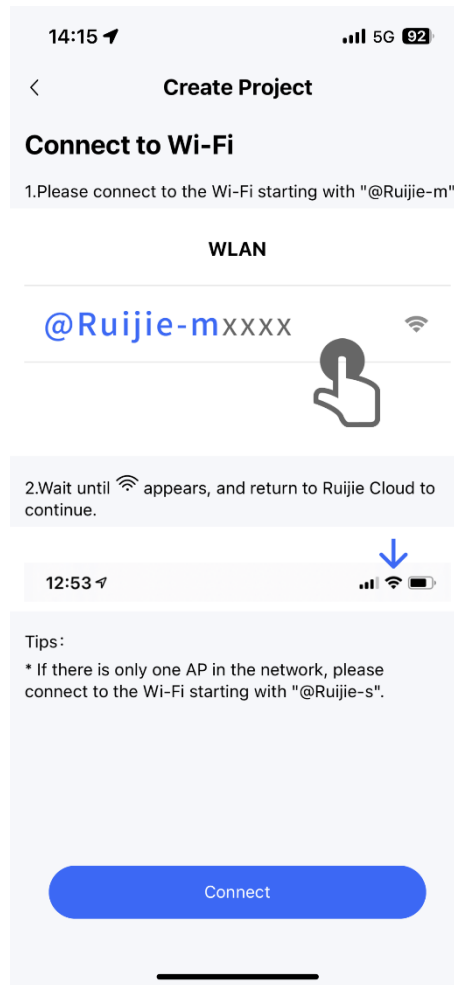
- (1) After the network environment is established according to the preceding figure, start the Ruijie Cloud app and choose **Project > Add a project**.



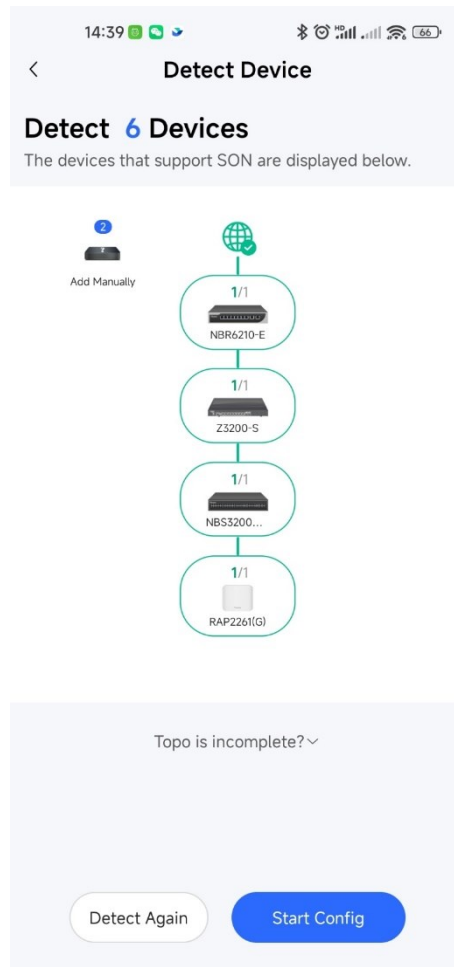
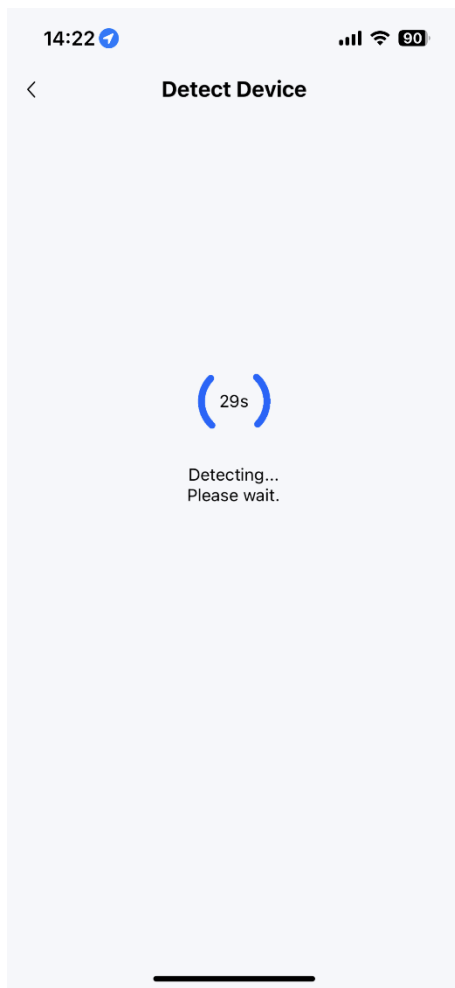
(2) Select **Connect to Wi-Fi** and add a project.



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



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



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

14:39

Basic Config

Project Config Internet Config Firewall Configuration Wi-Fi Config

Project Name
nbr_app

Management Password
ruijie@123

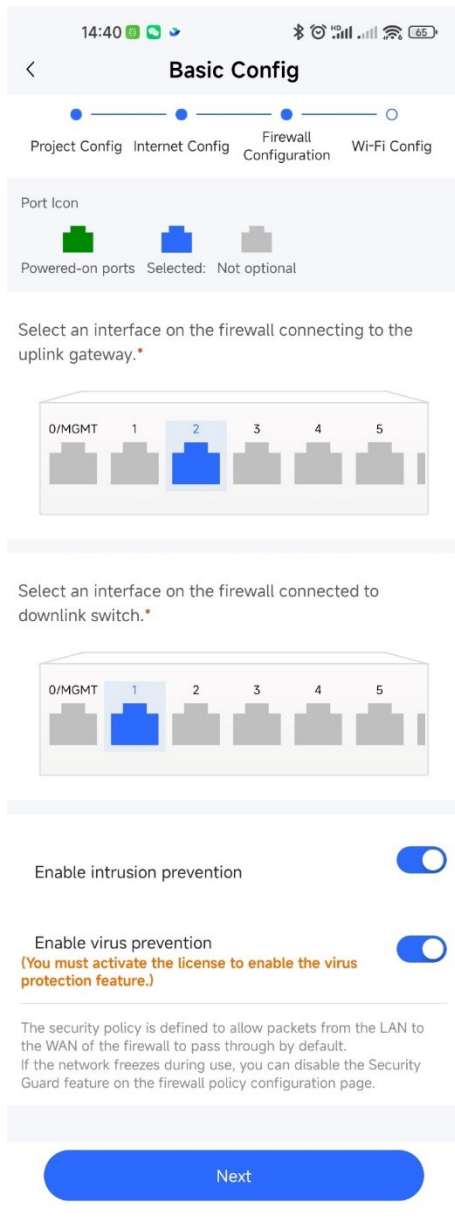
To ensure project security, ensure that the password meets the following requirements:

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

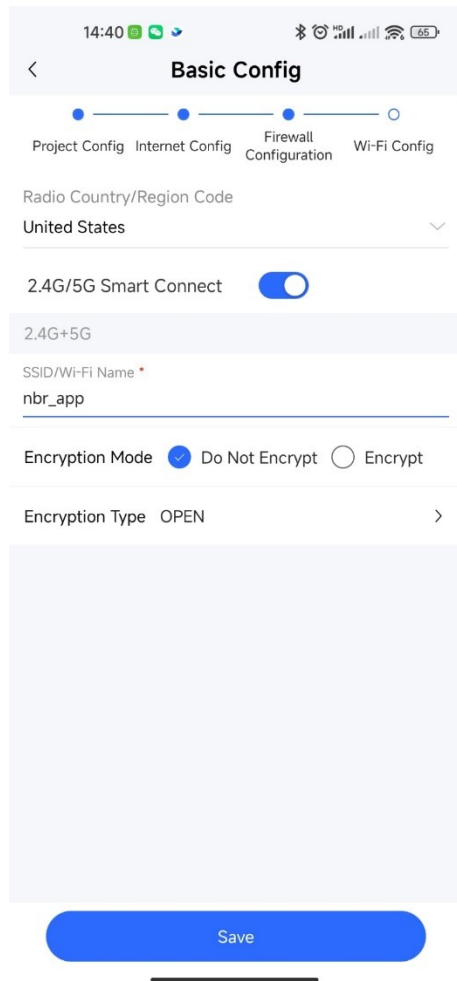
Scenario * Office >

Next

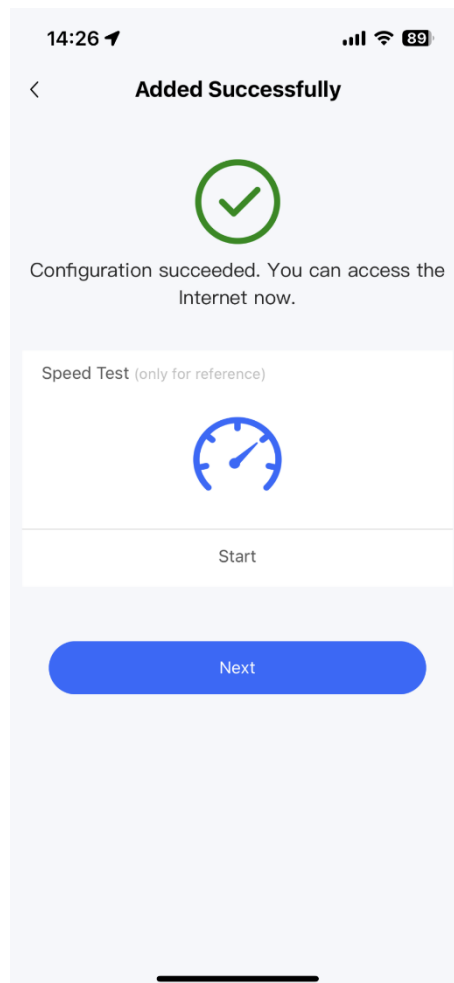
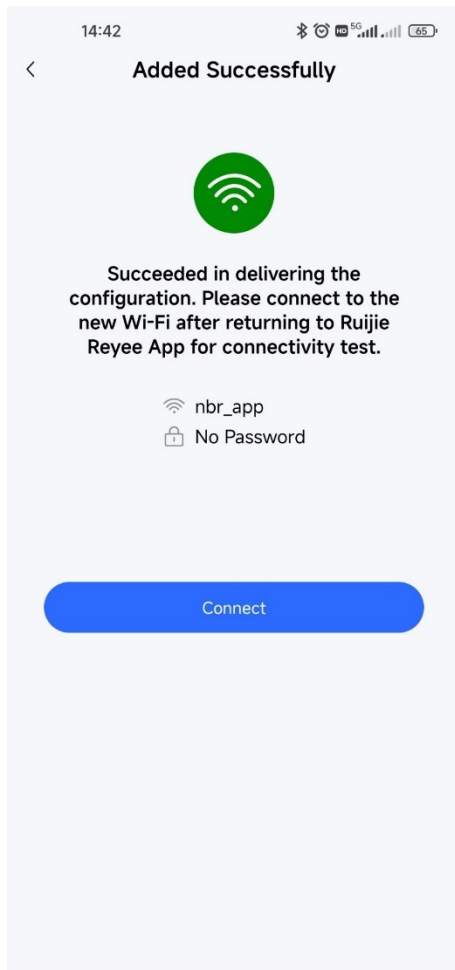
(6) Select the firewall interfaces connected to the router and switch, and tap **Next**.



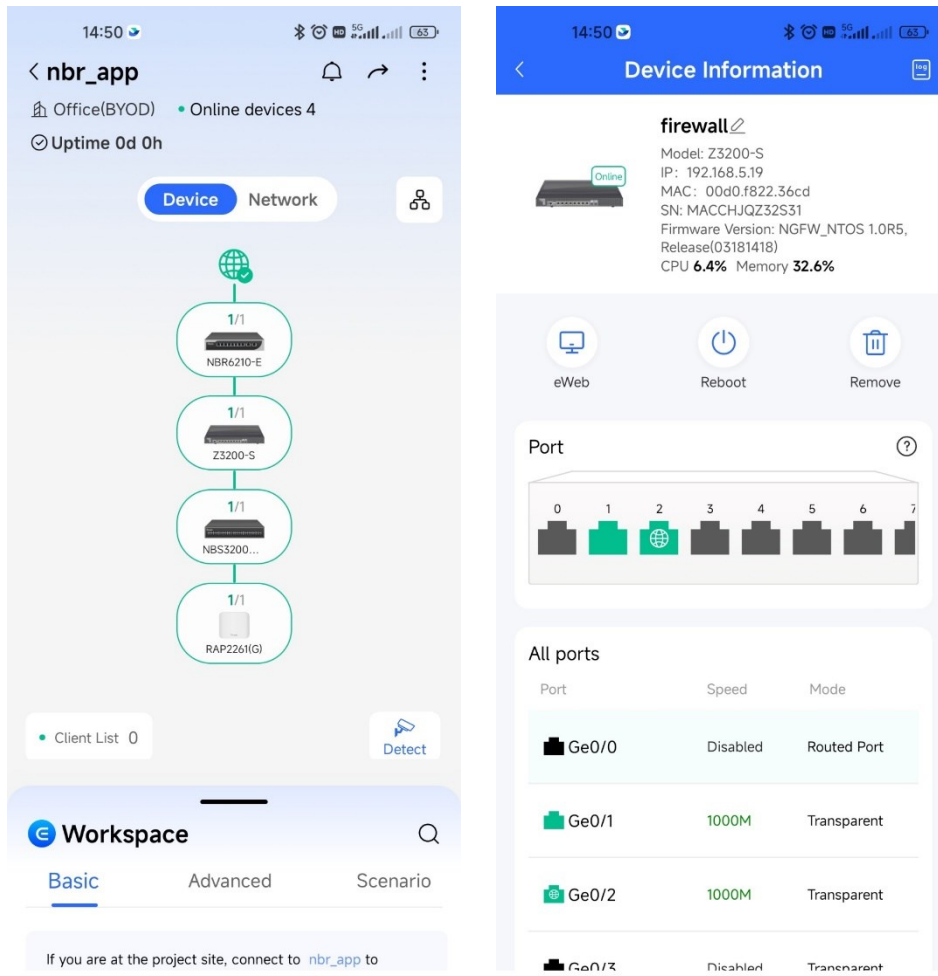
(7) Set the Wi-Fi name and password and tap **Save**.



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



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



7.2 Transparent Mode

7.2.1 Preparations

Confirm the following information before performing the configuration:

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

Method	Path
Official website	https://www.rujiienetworks.com/ Choose Support > Download > Reyee and find the latest version of the Z-S series firewall under RG-WALL 1600-Z-S series cloud management firewalls.

Method	Path
Web management page of the firewall	Choose System > System Maintenance > System Upgrade > Online Upgrade > Recommended Version to upgrade to the latest version (recommended) in online mode.
Ruijie Cloud	After the device goes online on the Ruijie Cloud, you can remotely upgrade the device in online mode on the Ruijie Cloud (without the need for local upgrade). Choose Monitoring > Device > Firewall , select a device, select a version, and click Upgrade .

⚠ Caution

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

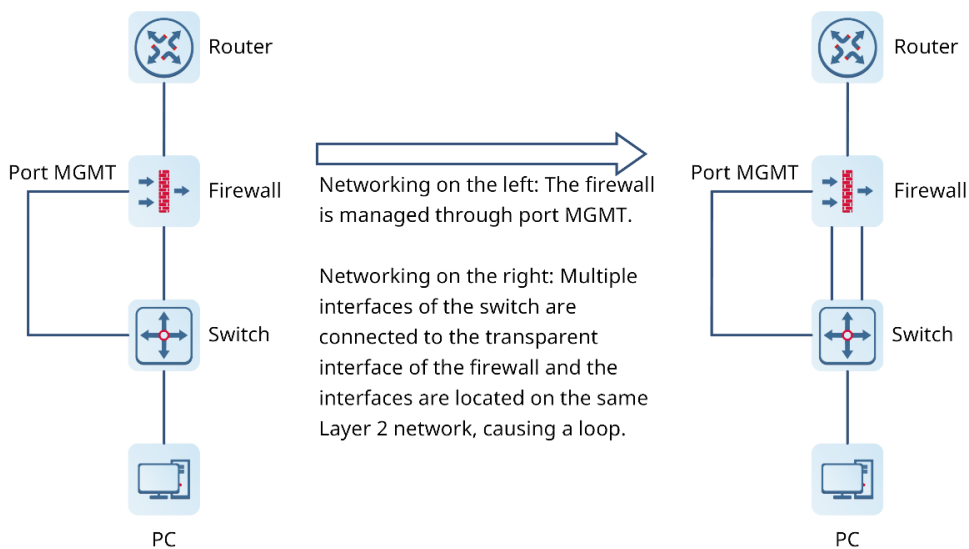
7.2.2 Deployment in Transparent Mode (Quick Deployment)

Network Requirements

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

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

Network Topology



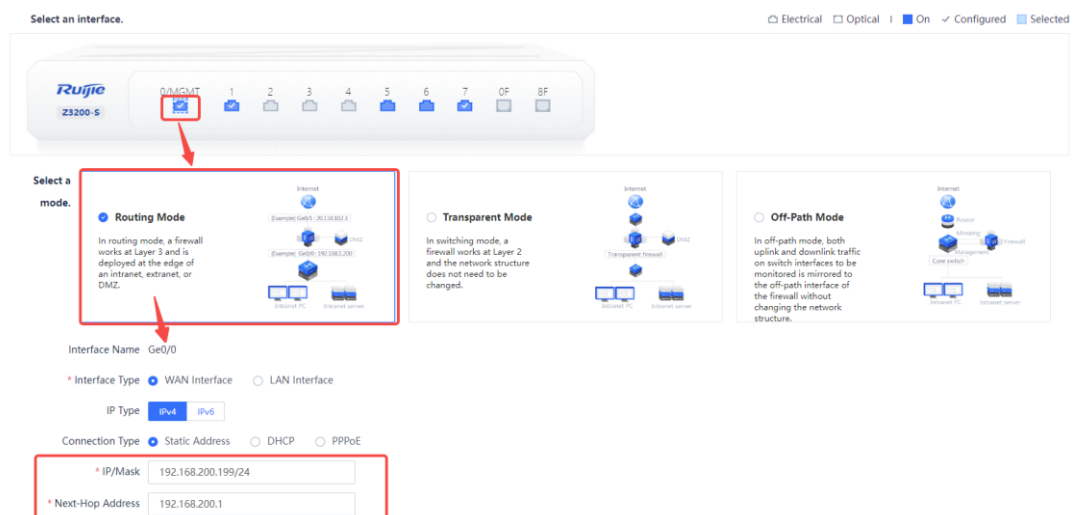
In this example, the firewall connects to the egress router through the WAN interface and connects to the core switch through the LAN interface. Port 0/MGMT (Ge0/0) of the firewall is used as the management interface to connect to the core switch (with management interface address set to 192.168.200.199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

Configuration Points

- (1) Implement quick onboarding. Select a deployment mode (transparent mode) and configure a WAN interface and a LAN interface to complete Internet access. Configure an IP address and the next hop for the management interface (0/MGMT) to ensure successful connection to the Internet.
 - WAN interface: Applicable to **connect to the egress device**. The WAN interface directly connects the firewall to an egress router or another device.
 - LAN interface: Applicable for **connection to LAN** devices, such as servers, PCs, switches, and printers.
- (2) (Optional) Check the connectivity. The system automatically checks whether the firewall is connected to the Internet.
- (3) Complete the quick onboarding configuration.
- (4) (Optional) Implement remote O&M on the cloud.

Procedure

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

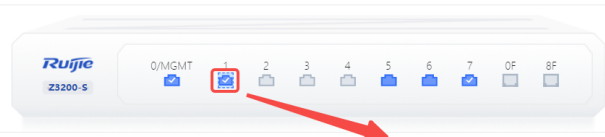


- b Configure the WAN interface and LAN interface and set the mode to transparent mode.

Note

The management interface cannot be set to the transparent mode.

Select an interface. Electrical Optical | On Configured Selected



Select a mode.

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

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

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

Interface Name Ge0/1

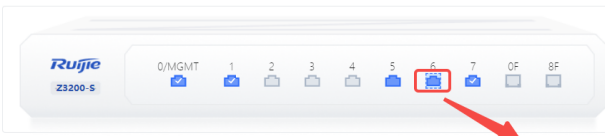
* Interface Type WAN Interface LAN Interface

* Bridge Interface [Add Bridge Interface](#)

Member Interface

* Connection Type Static Address DHCP

Select an interface. Electrical Optical | On Configured Selected



Select a mode.

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

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

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

Interface Name Ge0/6

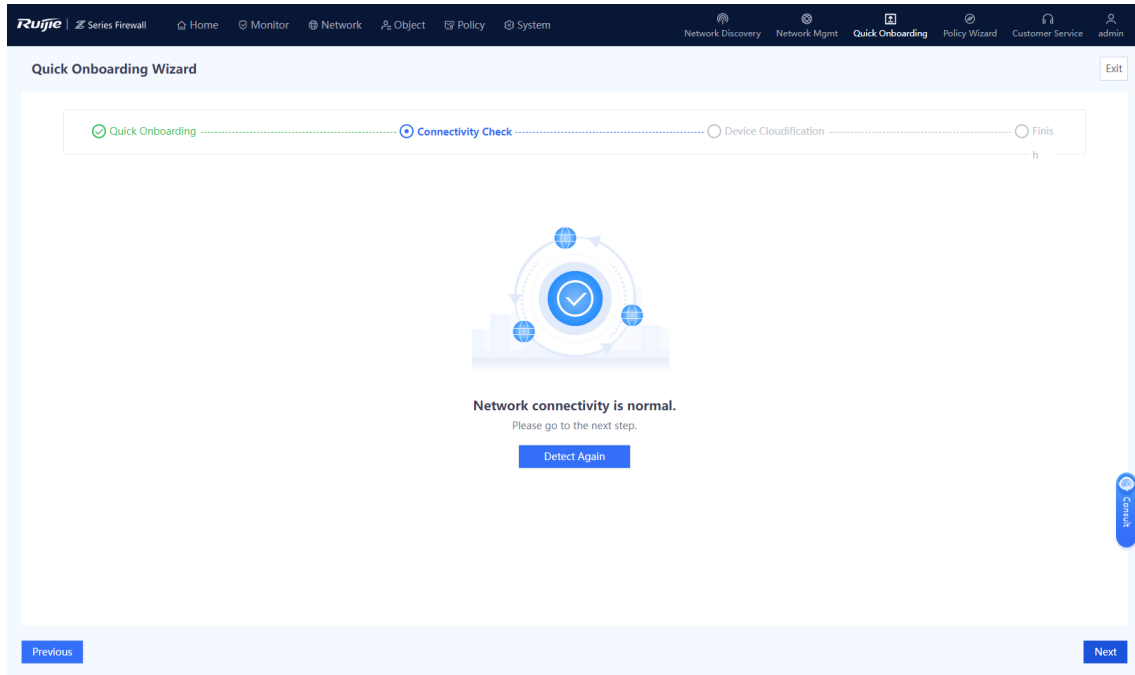
* Interface Type WAN Interface LAN Interface

* Bridge Interface [Add Bridge Interface](#)

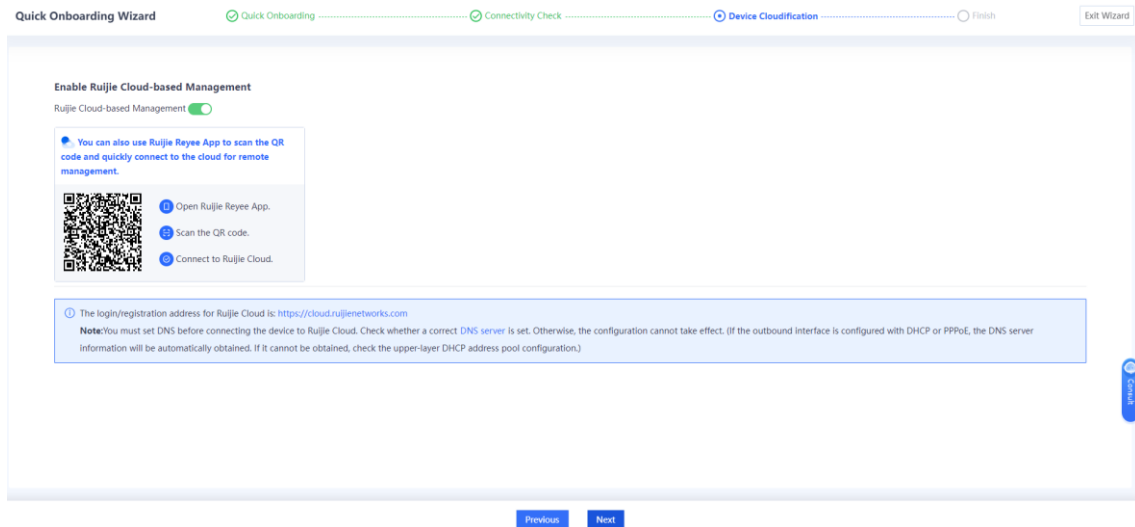
Member Interface

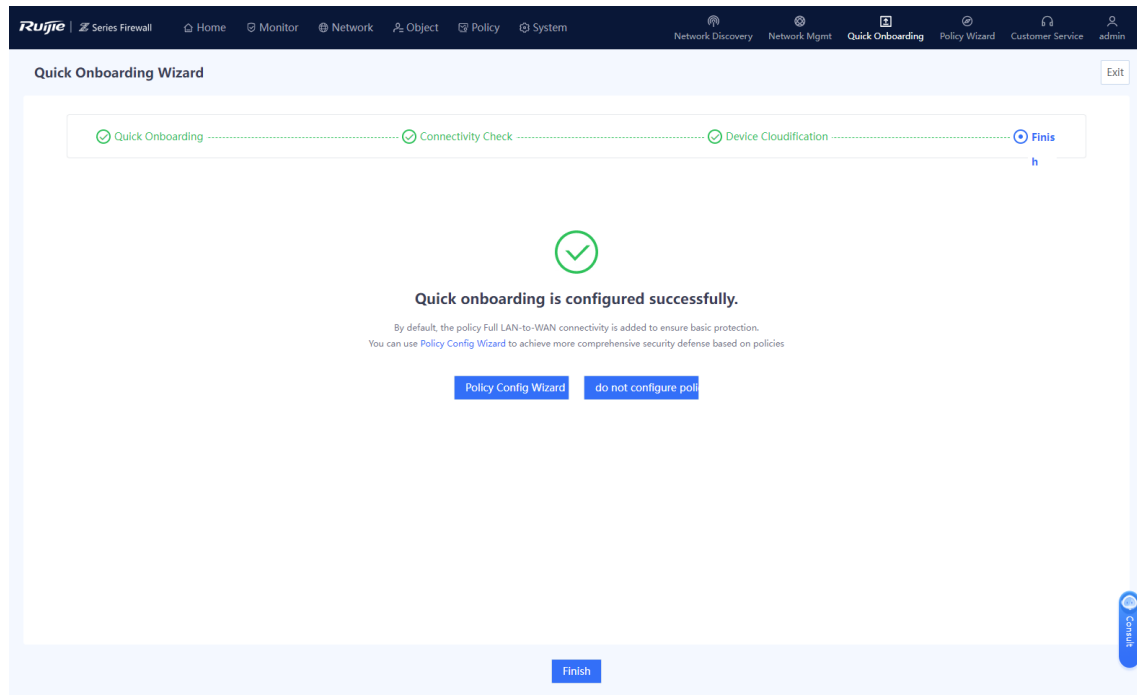
* Connection Type Static Address DHCP

(2) (Optional) Check the connectivity.



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





Configuration Verification

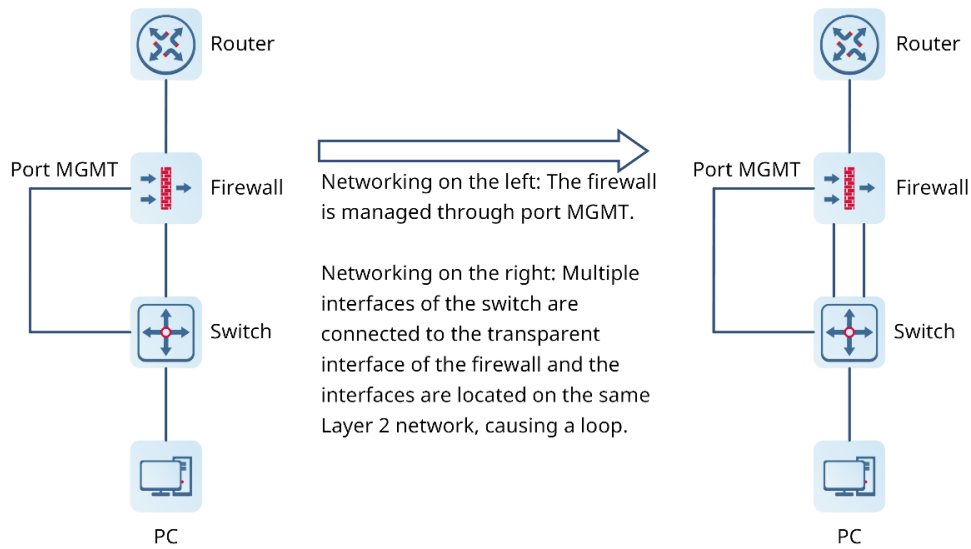
In transparent mode, the firewall can access the Internet without the need to modify the network environment, including the client IP address and gateway IP address.

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

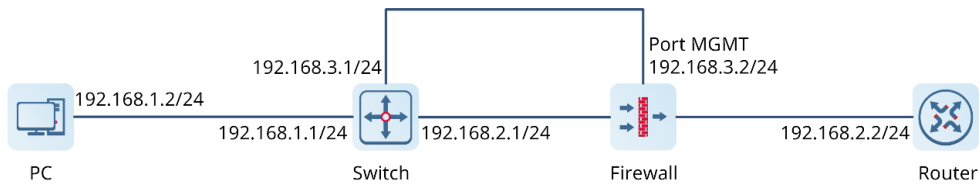
Network Requirements

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

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



Network Topology



Configuration Points

- Configure a management IP address and an access method for the management interface.
- Ensure network connectivity between the PC and the management interface.

Procedure

- (1) Configure the management interface Ge0/0.
 - a Choose **Network > Interface > Physical Interface**.
 - b Select **Ge0/0** and click **Edit**.
 - c Configure attributes of Ge0/0 and click **Save**.

< Back

Edit Physical Interface

Basic Info

Interface Name

Description

Connection Status Enable Disable

Mode Routing Mode Transparent Mode Off-Path Mode

* Zone [+ Add Security Zone](#)

Interface Type WAN Interface LAN Interface

Address

IP Type IPv4 IPv6

Connection Type Static Address DHCP PPPoE

* IP/Mask

* Next-Hop Address

Default Route

Line Bandwidth

Uplink

Downlink

Item	Description
Interface Type	Type of the Ge0/0 interface. As a management interface, Ge0/0 needs to connect to the Internet. As a result, you need to set the interface type to WAN interface.
IP/Mask	Set a valid IP address without conflicts that complies with requirements. 192.168.3.2/24
Next-Hop Address	192.168.3.1

Caution

The management interface cannot be converted to the transparent mode.

- (2) Convert other interfaces to the transparent mode.
 - a Choose **Network > Interface > Physical Interface**.

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

Edit Physical Interface

Basic Info

Interface Name:

Description:

Connection Status: Enable Disable

Mode: Routing Mode **Transparent Mode** Off-Path Mode

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

* Zone: [Add Security Zone](#)

Interface Type: WAN Interface **LAN Interface**

Advanced

MTU:

MAC: [Restore Default MAC](#)

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

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

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

< Back

Edit Physical Interface

Basic Info

Interface Name

Description

Connection Status Enable Disable

Mode Routing Mode Transparent Mode Off-Path Mode

* Bridge Interface [Add Bridge Interface](#)

* Zone [Add Security Zone](#)

Interface Type WAN Interface LAN Interface

Advanced

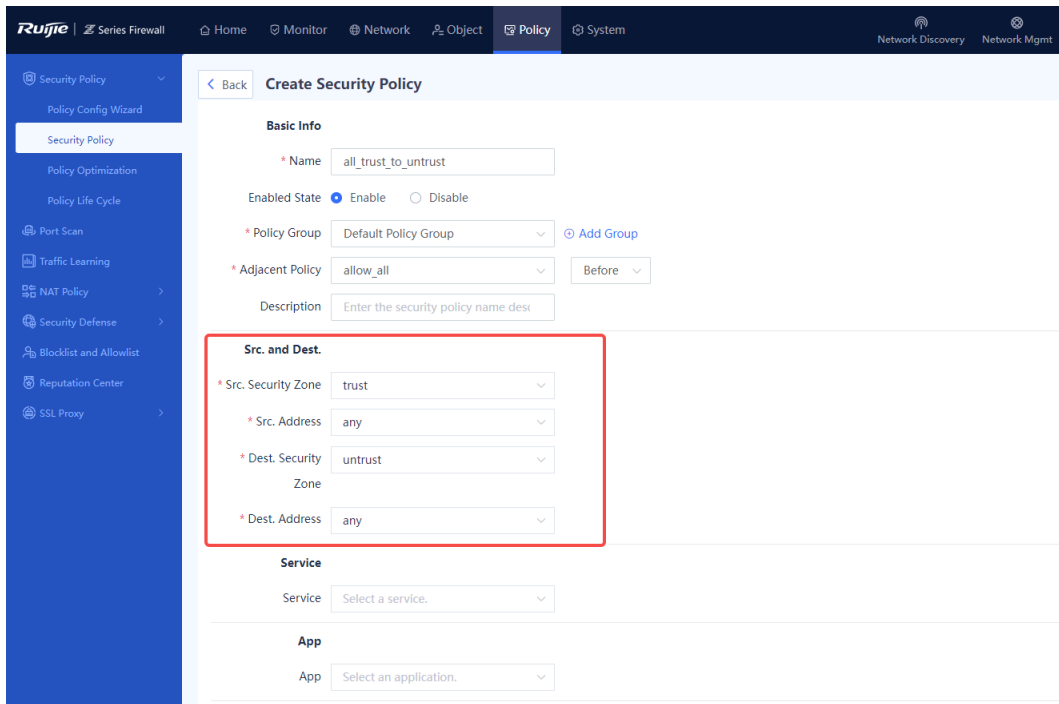
MTU

MAC [Restore Default MAC](#)

The following figure shows the configuration result.

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

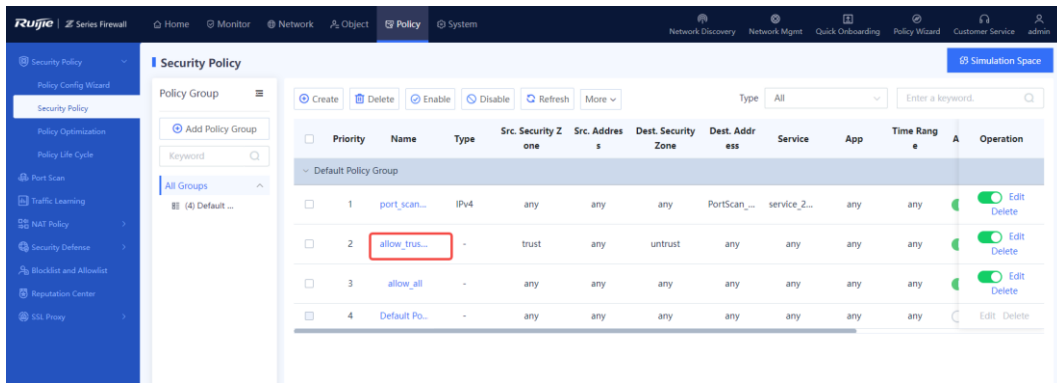
- (3) Configure a permit policy for traffic from zone **trust** to **untrust**.
 - a Choose **Policy > Security Policy > Security Policy**.
 - b Click **Create**.



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

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

The following figure shows the configuration result.



⚠ Caution

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

Configuration Verification

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

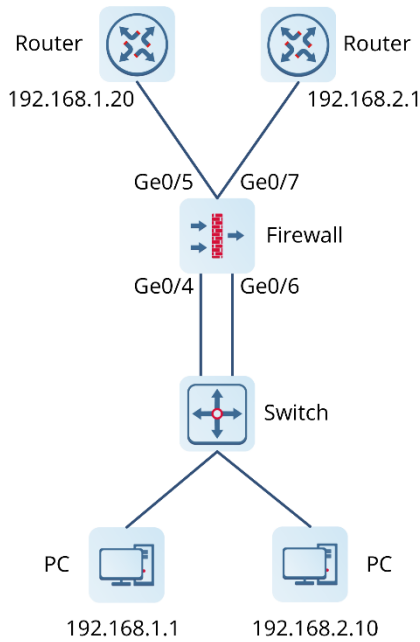
- You can successfully log in to the web management page to configure and manage the firewall.
- The PC on the same network segment as the management IP address can normally access the network.

7.2.4 Multi-bridge Deployment Mode

Application Scenario

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

Network Topology



Configuration Points

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

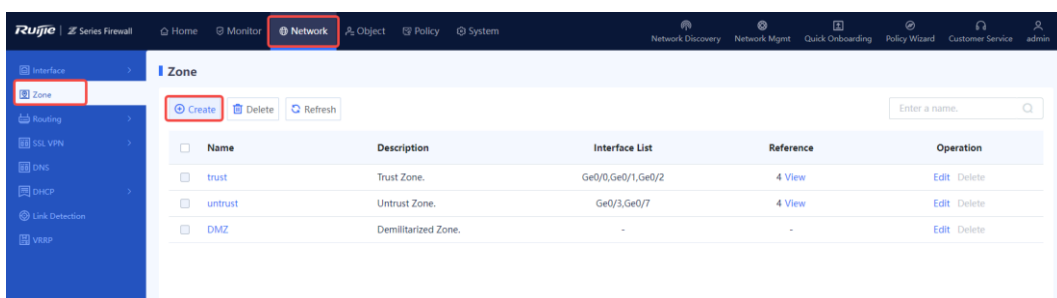
Caution

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

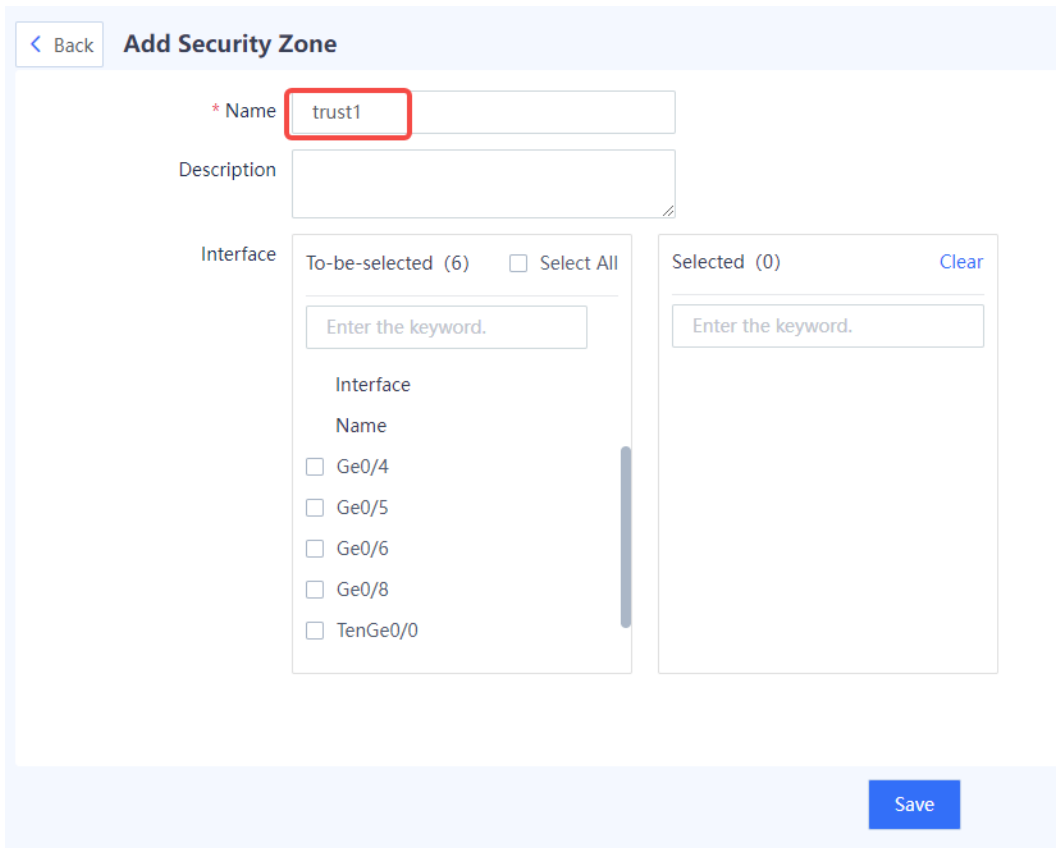
Procedure

(1) Create security zones.

a Choose **Network > Zone**.



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



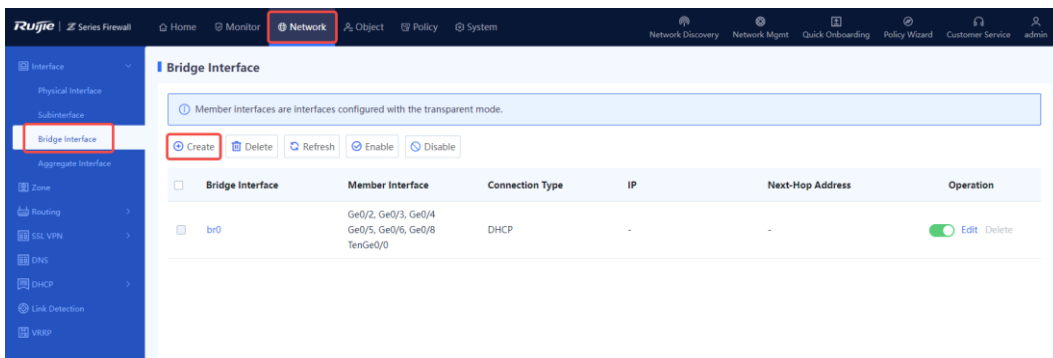
- c Configure parameters for the security zone **trust1** and click **Save**.
- d Repeat the preceding steps to create other security zones.

Caution

The security zone name must be unique.

(2) Create bridge interfaces.

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



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

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

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

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

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

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

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

< Back

Edit Physical Interface

Basic Info

Interface Name

Description

Connection Status Enable Disable

Mode Routing Mode **Transparent Mode** Off-Path Mode

* Bridge Interface + Add Bridge Interface

* Zone + Add Security Zone

Interface Type WAN Interface LAN Interface

Advanced

MTU

MAC Restore Default MAC

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

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

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

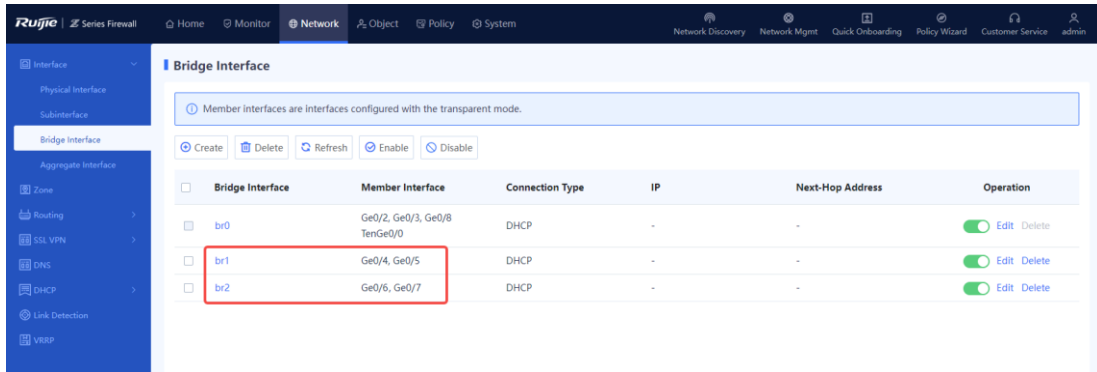
The following figure shows the configuration result.

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

Caution

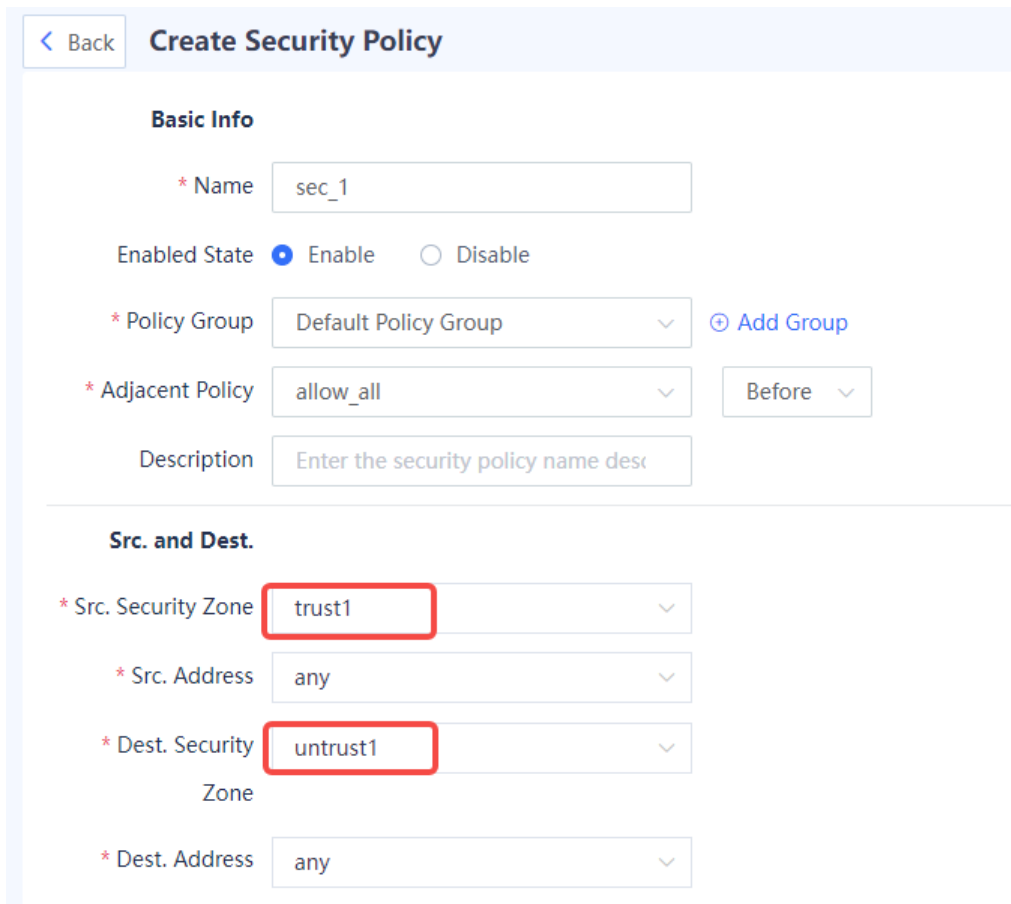
When all interfaces except Ge0/0 are set to transparent mode, the management interface must be configured with an IP address and the next hop to ensure device access through the management interface.

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



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

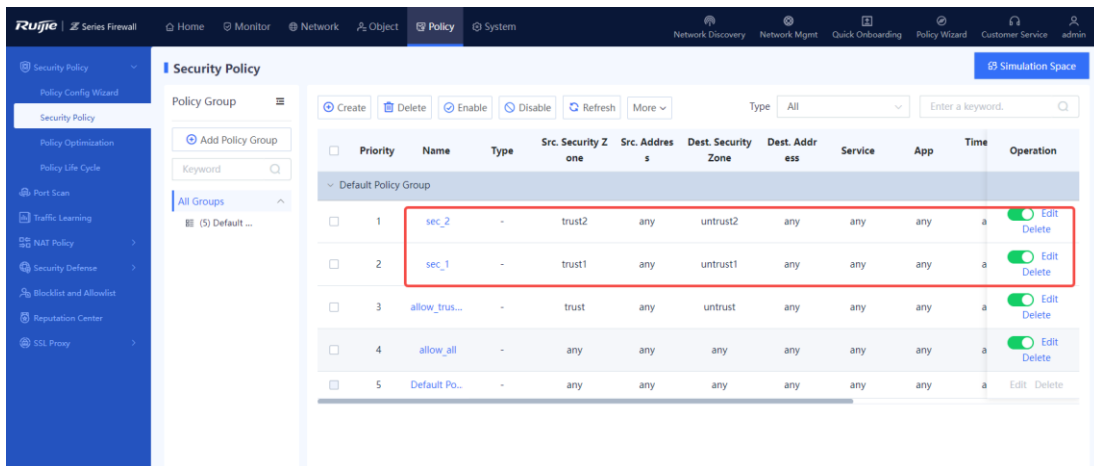
- a Choose **Policy > Security Policy**.
- b Click **Create** and create security policy 1.



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

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

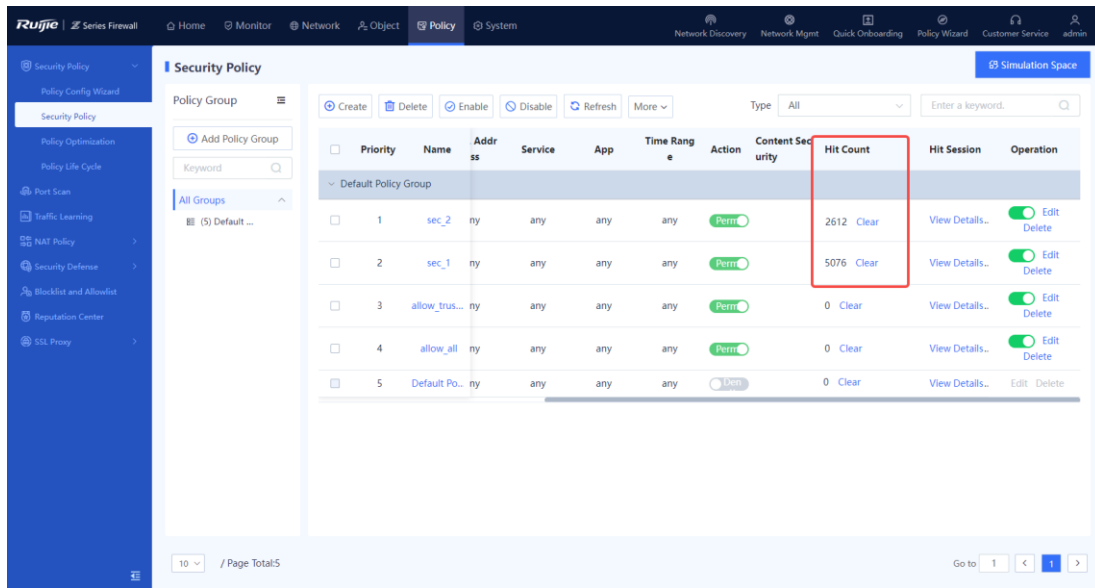
d Repeat the preceding steps to create security policy 2 and associate it with zones **trust2** and **untrust2**.



Configuration Verification

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

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



- (2) PC1 can normally access 192.168.2.1.
- (3) PC2 can normally access 192.168.1.20.

7.2.5 Precautions for Deploying Transparent Bridge Mode

Suggestions

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

Precautions

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

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

Function Restrictions

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

7.2.6 Configuring a Bridge Interface

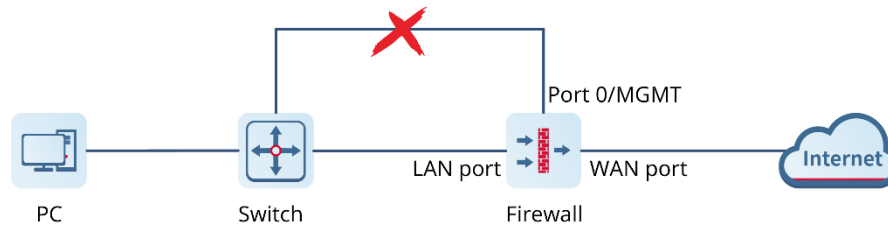
Application Scenario

Bridge interfaces are applicable to firewall deployment in transparent mode.

A bridge interface is a logical virtual interface composed of physical interfaces in transparent mode. You need to correctly configure an IP address and gateway to enable the firewall to forward traffic at Layer 3 through the

bridge interface. The firewall supports multiple groups of bridge interfaces, and traffic of the bridge groups is isolated from one another.

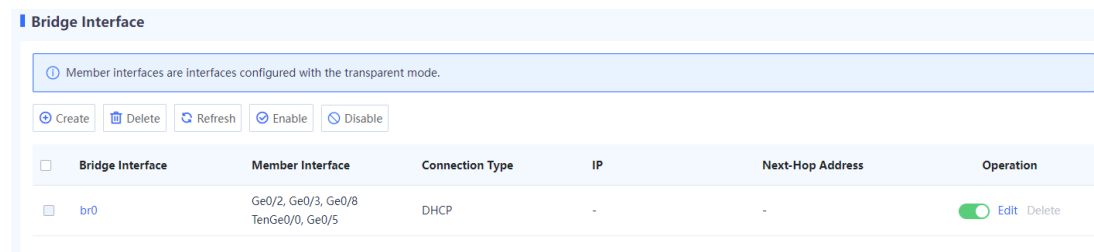
In actual networking, you do not need to separately connect port 0/MGMT to devices such as switch. Remote O&M can be implemented through the bridge interface, which is easy to implement.



Procedure

(1) Choose Network > Interface > Bridge Interface.

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



Note

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

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

- If a new physical interface works in transparent mode, click **Refresh** to obtain the latest member interface information.
- Click to enable or disable the bridge interface.
- Click **Delete** to delete the bridge interface.

Caution

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

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

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

< Back

Add Bridge Interface

Basic Info

* Interface Name

Connection Status Enable Disable

Member Interface

Address

Connection Type Static Address DHCP

Src. MAC Consistency

Check

① Src. MAC Consistency

Check

Access Management

Permit HTTPS PING SSH

Item	Description	Remarks
Interface Name	Name of a bridge interface.	<ul style="list-style-type: none"> Characters such as `~!#%^&*+ \ {};:"'<>?` and spaces are not allowed. The name is specified when you create a bridge interface and cannot be modified in later steps. <p>[Example]</p> <p>br1</p>
Connection Status	Whether to enable the bridge interface.	[Example] Enable

Item	Description	Remarks
Member Interface	<p>Member interface in the bridge interface.</p> <p>Members of the bridge interface are interfaces set to transparent mode. One bridge interface can contain multiple transparent interfaces, but each transparent interface can belong to only one bridge interface.</p>	<p>To add a member to the bridge interface, set Bridge Interface to the current bridge interface when you configure the corresponding member interface (such as physical interface or aggregate interface).</p> <p>[Example] Ge0/2</p>
Address		
Connection Type	<p>Connection type of the bridge interface. The options are as follows:</p> <ul style="list-style-type: none"> ● Static Address: Applicable when the network administrator specifies an IP address for the device based on the predefined IP address planning. This connection type requires the network administrator to possess certain network knowledge. When this option is selected, you need to set IP/Mask and Next-Hop Address. ● DHCP: Applicable when the network administrator is not professional. The bridge interface automatically obtains an IP address from the upper-layer DHCP server for Internet access. 	<p>[Example] Static Address</p>
IP/Mask	<p>IP address and mask of the interface.</p>	<p>You need to set this parameter when Connection Type is set to Static Address.</p> <p>[Example] 192.168.20.1/24</p>
Next-Hop Address	<p>Next router address to reach the router with the destination address.</p>	<p>You need to set this parameter when Connection Type is set to Static Address.</p> <p>[Example] 192.168.20.2/24</p>
Default Route	<p>Whether to enable the default route.</p>	<p>[Example] Enable</p>

Item	Description	Remarks
Src. MAC Consistency Check	Whether to enable source MAC address consistency check. If you select Enable , the firewall checks the source MAC address of the packet with the source MAC address in the session. If they are different, the firewall does not check the session status of the packet but transparently forwards the packet over the bridge network directly.	[Example] Enable
Access Management	Whether the bridge interface supports HTTPS, ping, and SSH.	The configuration takes effect when local defense is enabled on the device. [Example] Select HTTPS .

7.3 Routing Mode

7.3.1 Preparations

Confirm the following information before performing the configuration:

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

Note

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

- Software version obtaining methods

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

⚠ Caution

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

7.3.2 Single-Line Onboarding (Quick Deployment)

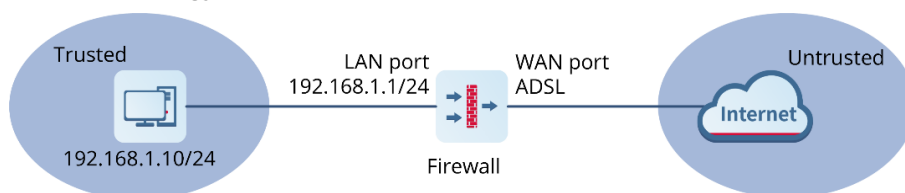
Network Requirements

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

i Note

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

Network Topology



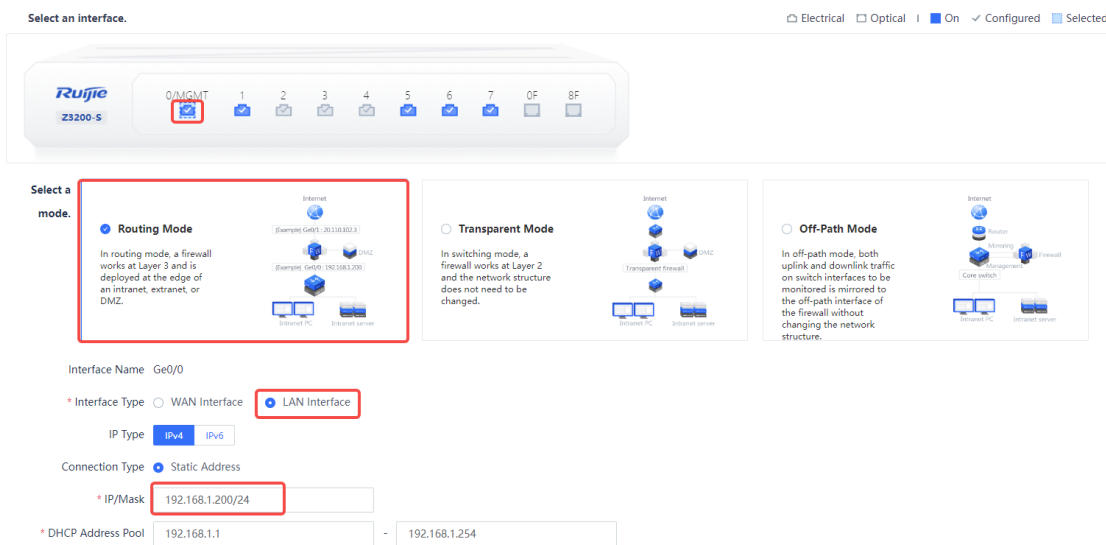
Assume that the username and password allocated by the ISP are **admin** and **ruijie@123**.

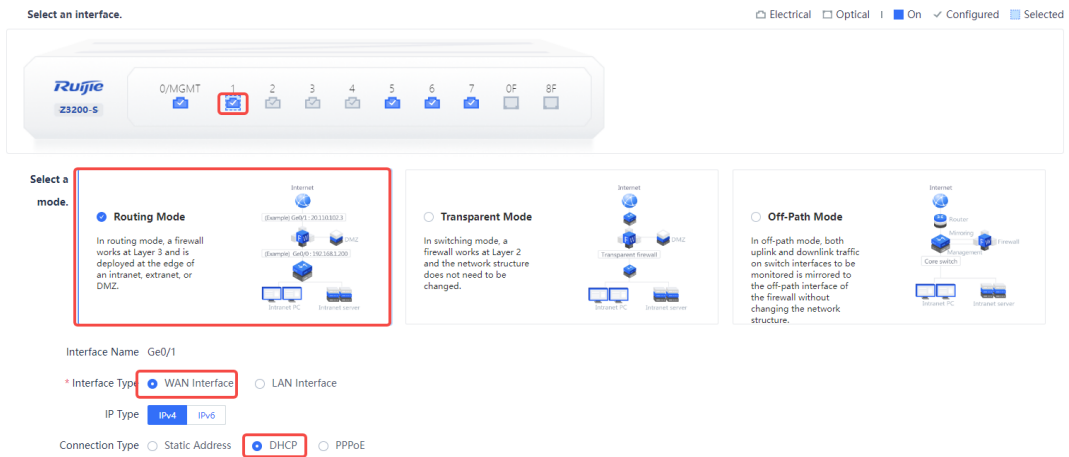
Configuration Points

- (1) Implement quick onboarding. Select a deployment mode (routing mode) and configure a WAN interface and a LAN interface to complete Internet access.
 - WAN interface: Applicable to Internet access to connect the firewall to the Internet. Generally, the WAN interface is directly connected to the FTTH ONU of the ISP. The following connection types are supported based on the interface type:
 - Static address: Applicable when the network administrator specifies an IP address for the device based on the predefined IP address planning. This connection type requires the network administrator to possess certain network knowledge. The IP address/mask and next-hop address must be configured.
 - DHCP: Applicable when no professional network administrator is available. The user terminal automatically obtains an IP address to access the Internet after the terminal is connected to the firewall.
 - ADSL dialup: Applicable for dialup access to the ISP network. The account and password of the dialup user must be configured.
 - LAN interface: Applicable for **connection to LAN** devices, such as PCs, switches, and printers.
- (2) (Optional) Check the connectivity. The system automatically checks whether the firewall is connected to the Internet.
- (3) Complete the quick onboarding configuration.
- (4) (Optional) Implement remote O&M on the cloud.

Procedure

- (1) Implement quick onboarding.
 - a Configure the IP addresses of the PC and the 0/MGMT management interface to be on the same network segment. Visit <https://192.168.1.200> (default address) to log in to the device using the default account and password (**admin** and **firewall**).
 - b Configure a WAN interface and a LAN interface to complete Internet access.
 - a In this example, Ge0/0 (port 0/MGMT by default) is used as the LAN interface and Ge0/1 (enabled with DHCP for dynamic address allocation) is used as the WAN interface.
 - c Set the mode to routing.

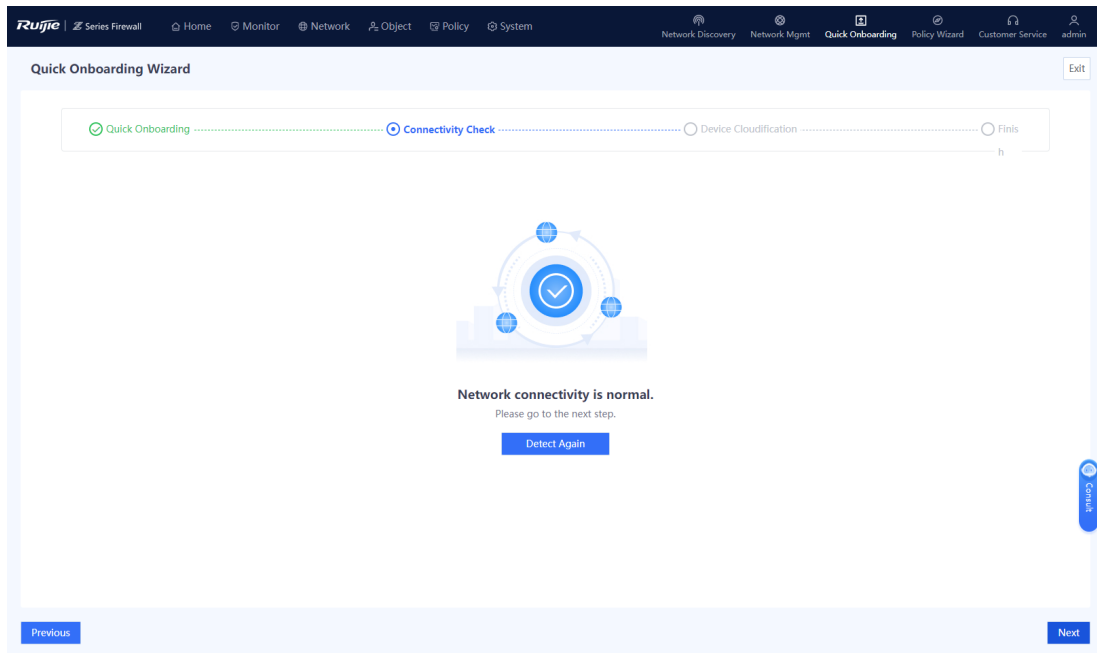




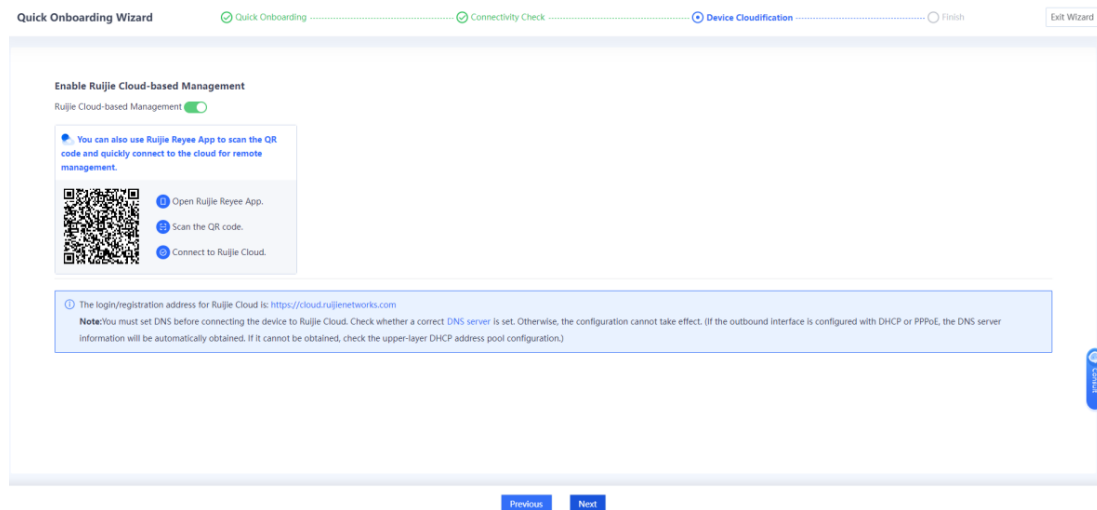
Caution

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

(2) (Optional) Check the connectivity.



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

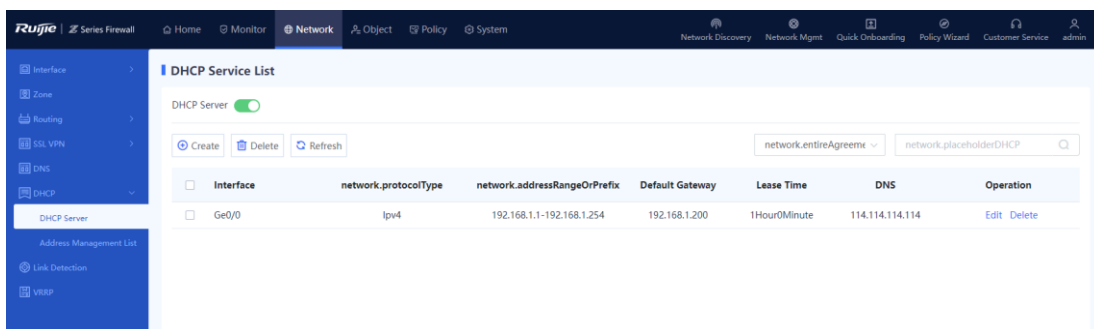


Configuration Verification

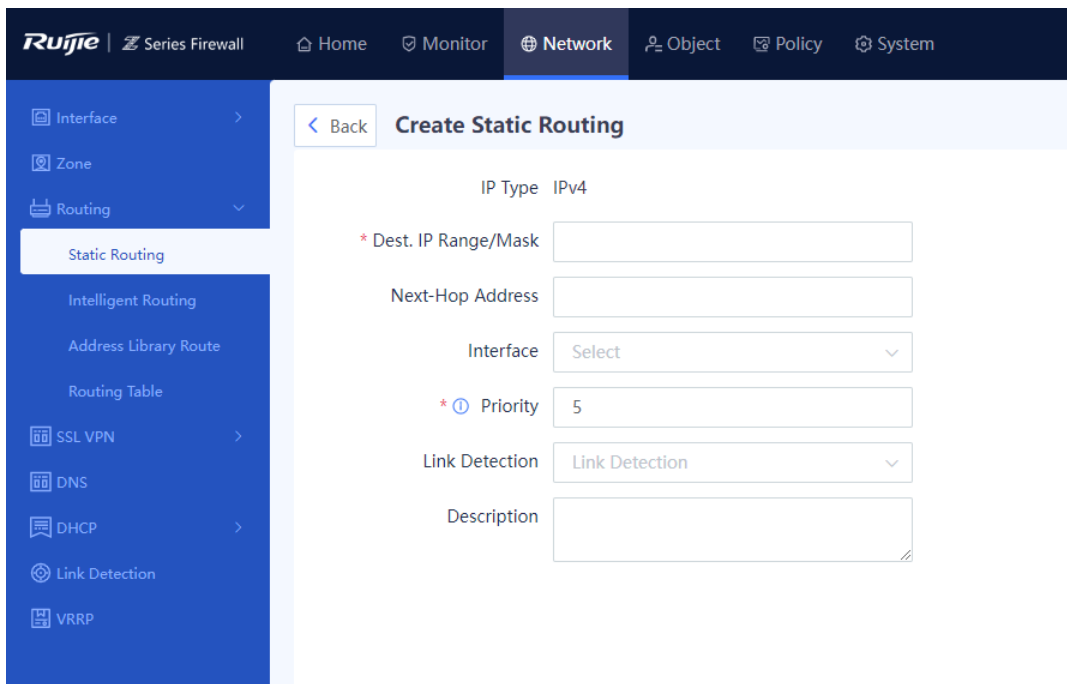
Set the IP address of the PC to 192.168.1.1/24, gateway address to 192.168.1.200, and DNS server addresses to 114.114.114.114 (primary) and 223.5.5.5 (secondary). (The address of the local DNS server must be used.) The PC can normally access the Internet.

Precautions

- By default, DHCP is disabled on the firewall interface. To allow downstream PCs to dynamically obtain IP addresses to access the Internet, choose **Network > DHCP > DHCP Server** and enable **DHCP Server**.



- The routing mode deployment in this section uses Layer 2 networking as an example to describe how to implement Internet access. If the downstream network of the firewall is a Layer 3 network, for example, the gateway of the downstream terminal is not the firewall, you need to add a static route to the LAN network segment based on the actual network planning. (In this static route, the destination network segment is the LAN service network segment and the next-hop address is the address of the interface connecting the downstream device to the firewall.)



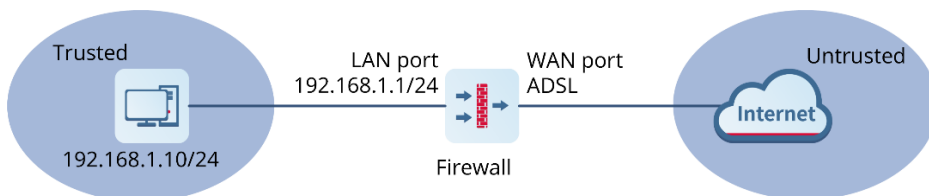
7.3.3 Single-Line Onboarding (Custom Deployment)

1. Onboarding Through Single ADSL Line

Network Requirements

The PC is located in the LAN network segment 192.168.1.0/24. The WAN interface dials up using PPPoE to obtain an IP address from the ISP. The PC wants to access the Internet through the firewall.

Network Topology



Item	Description
Ge0/6	LAN interface, which belongs to the security zone trust. The IP address is 192.168.1.1.
Ge0/7	WAN interface, which belongs to the security zone untrust. This interface dials up to obtain an IP address from the ISP. The username and password allocated by the ISP are admin and ruijie@123 .

Configuration Points

Step	Description	Key Configuration
Configure interfaces.	Select two interfaces on the device and set the interface type to WAN interface and LAN interface respectively. <ul style="list-style-type: none"> ● WAN interface: Used to connect to the Internet. ● LAN interface: Used to connect to the LAN. 	<ul style="list-style-type: none"> ● WAN interface: Set Connection Type to PPPoE and add the interface to the security zone untrust. The system automatically generates a default route. ● LAN interface: Set the IP address to 192.168.1.1/24 and add the interface to the security zone trust. You can choose to enable some management functions on the interface.
Create an address object.	To facilitate management, configure the IP address of the LAN user as an address object.	Set the name to lan and IP address to 192.168.1.10.
Create a security policy.	Create a policy to control traffic between the LAN interface and WAN interface.	<ul style="list-style-type: none"> ● Src. Security Zone: trust ● Src. Address: lan ● Dest. Security Zone: untrust ● Dest. Address: any
Configure NAT.	Configure source NAT to allow the LAN user to normally access the Internet.	<ul style="list-style-type: none"> ● Src. Security Zone: trust ● Src. Address: lan ● Dest. Security Zone: untrust ● Dest. Address: any ● Src. Address Translated to: Outbound Interface Address

Procedure

- (1) Configure the WAN interface.
 - a Choose **Network > Interface > Physical Interface**.
 - b Select the physical interface to be used as the WAN interface and click **Edit**.

< Back
Edit Physical Interface

Basic Info

Interface Name

Description

Connection Status Enable Disable

Mode Routing Mode Transparent Mode Off-Path Mode

* Zone [⊕ Add Security Zone](#)

Interface Type WAN Interface LAN Interface

Address

IP Type IPv4 IPv6

Connection Type Static Address DHCP PPPoE

* Account

* Password

c Set parameters for the interface.

Item	Description
Mode	Routing Mode
Zone	untrust
Interface Type	WAN Interface
Connection Type	PPPoE
Account	admin
Password	ruijie@123

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

Line Bandwidth

Uplink Select ▾

Downlink Select ▾

Access Management

Permit HTTPS PING SSH

Advanced

ISP Address Library ▾

MTU

MAC Restore Default MAC

Link Detection ▾

e Click **Save**.

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

Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mode	MTU	Operation
Ge0/0	-	■	Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500	Edit
Ge0/1	-	■	Routing	trust	IPv4: DHCP	-	-	1500	Edit
Ge0/2	-	■	Transparent	trust	-	-	-	1500	Edit
Ge0/3	-	■	Transparent	untrust	-	-	-	1500	Edit
Ge0/4	-	■	Routing	trust1	-	-	-	1500	Edit
Ge0/5	-	■	Transparent	untrust1	-	-	-	1500	Edit
Ge0/6	-	■	Routing	untrust	IPv4: DHCP	172.20.37.124/24	-	1500	Edit
Ge0/7	-	■	Routing	untrust	IPv4: PPPoE	192.168.99.2/32	-	1500	Edit
TenGig0/0	-	■	Transparent	-	-	-	-	1500	Edit
Ge0/8	-	■	Transparent	-	-	-	-	1500	Edit

(2) Configure the LAN interface.

- a Choose **Network > Interface > Physical Interface**.
- b Select the physical interface to be used as the LAN interface and click **Edit**.

< Back

Edit Physical Interface

Basic Info

Interface Name

Description

Connection Status Enable Disable

Mode Routing Mode Transparent Mode Off-Path Mode

* Zone [Add Security Zone](#)

Interface Type WAN Interface LAN Interface

Address

IP Type IPv4 IPv6

Connection Type Static Address DHCP PPPoE

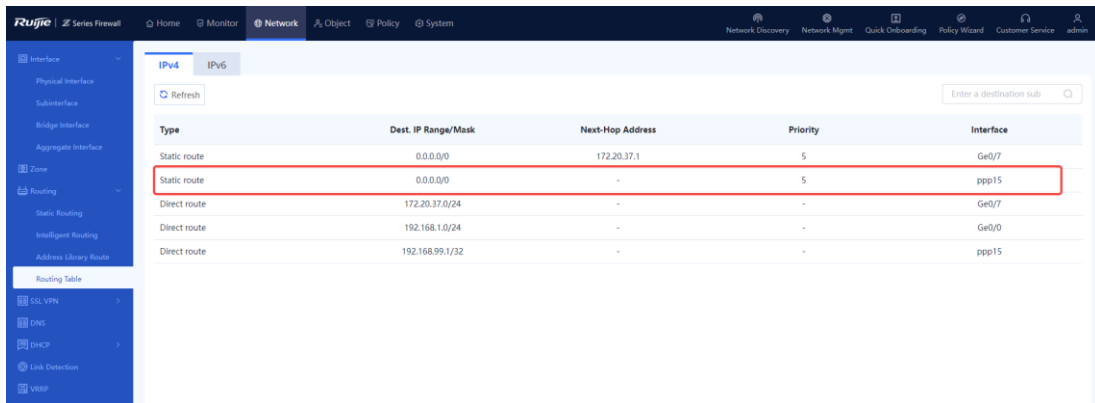
* IP/Mask

- c Set parameters for the interface.

Item	Description
Mode	Routing Mode
Zone	trust
Interface Type	LAN Interface
Connection Type	Static Address
IP/Mask	192.168.1.1/24

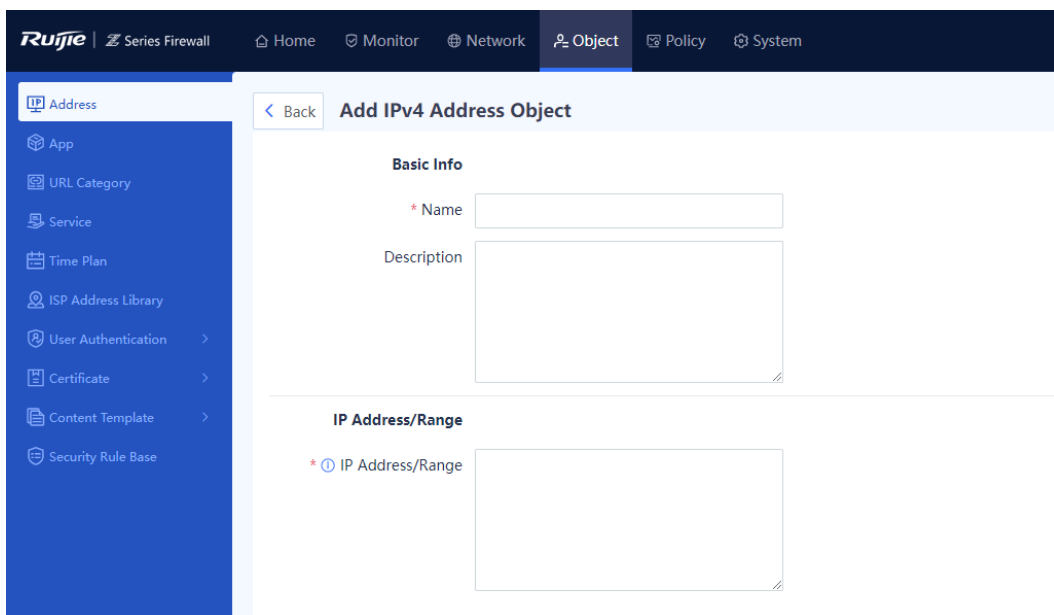
- d Enable management functions on the interface as required. You are advised to enable the HTTPS, ping, and SSH services only on the LAN interface.
- e Click **Save**.

After the WAN interface and LAN interface are successfully configured, choose **Network > Routing > Routing Table**. You can find that the device automatically generates a default route.



(3) Configure address resources.

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



c Set parameters for the address object.

Set **Name** to **lan** and **IP Address/Range** to **192.168.1.10**.

d Click **Save**.

(4) Create a security policy.

- a Choose **Policy > Security Policy > Security Policy**.
- b Click **Create** and create a security policy.

< Back
Create Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security (After being enabled, the following configurations only take effect for IPv4 traffic.)

Intrusion Prevention Enable Not Enabled [⊕ Add Intrusion Prevention Template](#)

Virus Protection Enable Not Enabled [⊕ Add Virus Protection Template](#)

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

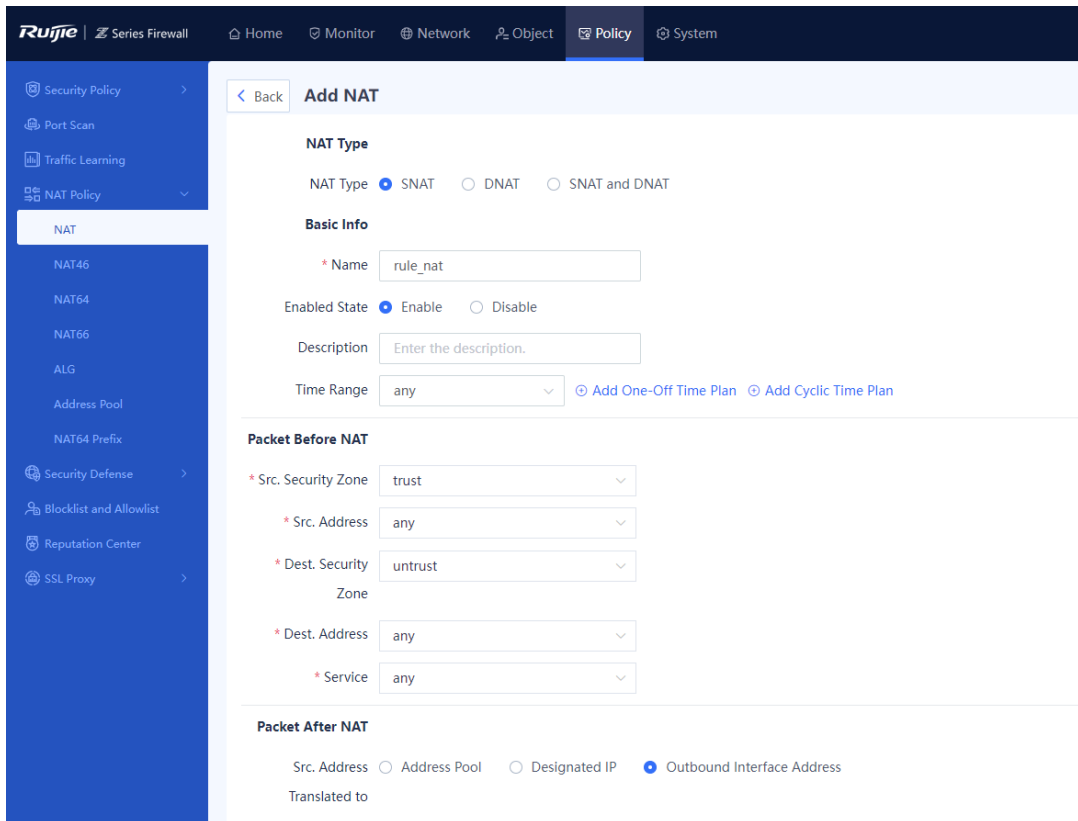
Advanced

c Set parameters for the policy.

Item	Description
Src. Security Zone	trust
Src. Address	lan
Dest. Security Zone	untrust

Item	Description
Dest. Address	any
Service	any
App	any

- d Click **Confirm**.
- (5) Configure a NAT policy.
 - a Choose **Policy > NAT Policy > NAT**.
 - b Click **Create**.
 - a Add a source NAT policy to translate the source address of traffic sent by a device in the zone **trust** and going out from a device in the zone **untrust**.



- c Set parameters for the NAT policy.

Item	Description
Src. Security Zone	trust
Src. Address	lan

Item	Description
Dest. Security Zone	untrust
Dest. Address	any
Src. Address Translated to	Outbound Interface Address

d Click **Save**.

Configuration Verification

Set the IP address of the PC to 192.168.1.10/24, gateway address to 192.168.1.1, and DNS server addresses to 114.114.114.114 (primary) and 223.5.5.5 (secondary). (The address of the local DNS server must be used.)

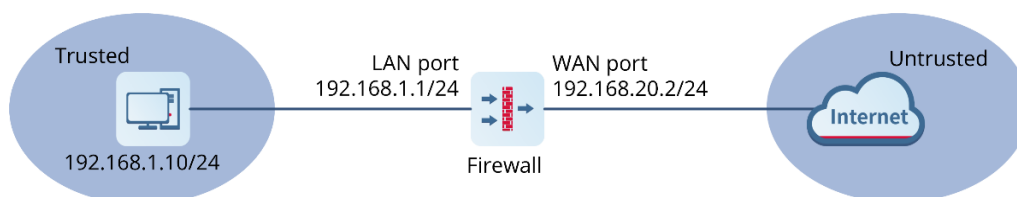
The PC can successfully ping the address 114.114.114.114.

2. Onboarding Through Static Address

Network Requirements

The computer is located in the LAN network segment 192.168.1.0/24. The WAN interface is connected to a dedicated line and specified by a static address by the ISP. The computer wants to access the Internet through the firewall.

Network Topology



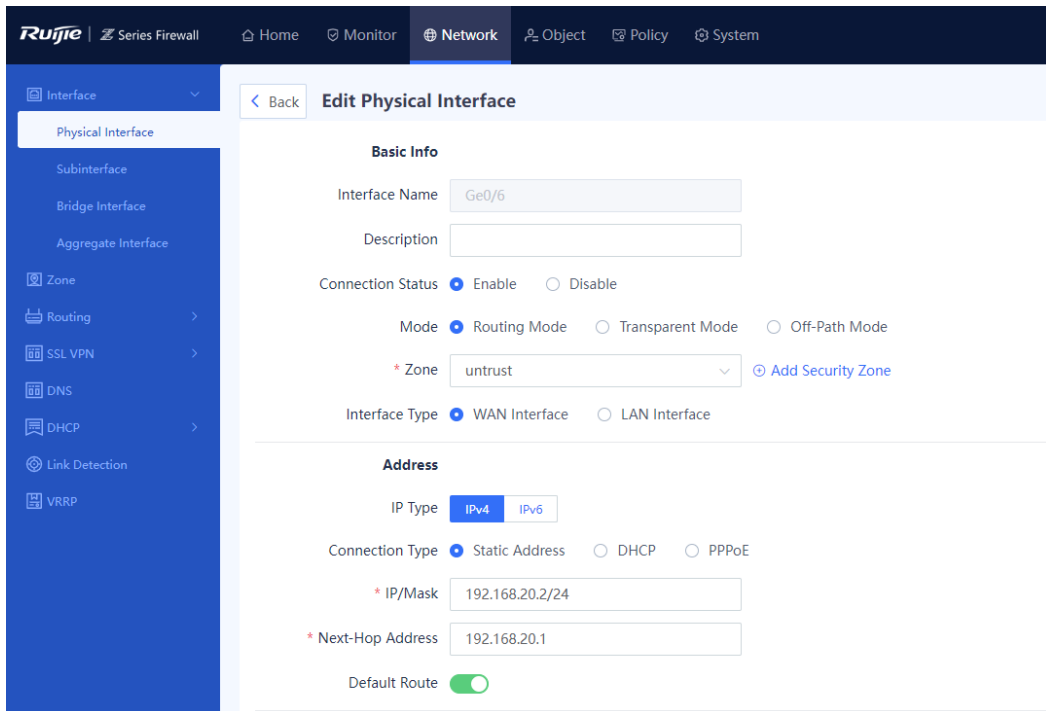
Item	Description
Ge0/1	LAN interface, which belongs to the security zone trust . The IP address is 192.168.1.1/24.
Ge0/6	WAN interface, which belongs to the security zone untrust . The fixed IP address allocated by the ISP to this interface and the gateway address are 192.168.20.2/20 and 192.168.20.1, respectively.
DNS	The DNS address is 192.168.58.110, which is obtained from the ISP.

Configuration Points

Step	Description	Key Configuration
Configure interfaces.	Select two interfaces on the device and set the interface type to WAN interface and LAN interface respectively. <ul style="list-style-type: none"> ● WAN interface: Used to connect to the Internet. ● LAN interface: Used to connect to the LAN. 	<ul style="list-style-type: none"> ● WAN interface: Set Connection Type to Static Address and configure the next-hop address. ● Add the interface to the security zone untrust. The system automatically generates a default route. ● LAN interface: Set the IP address to 192.168.1.1/24 and add the interface to the security zone trust. You can choose to enable some management functions on the interface.
Create an address object.	To facilitate management, configure the IP address of the LAN user as an address object.	Set the name to lan and IP address to 192.168.1.10.
Create a security policy.	Create a policy to control traffic between the LAN interface and WAN interface.	<ul style="list-style-type: none"> ● Src. Security Zone: trust ● Src. Address: lan ● Dest. Security Zone: untrust ● Dest. Address: any
Configure NAT.	Configure source NAT to allow the LAN user to normally access the Internet.	<ul style="list-style-type: none"> ● Src. Security Zone: trust ● Src. Address: lan ● Dest. Security Zone: untrust ● Dest. Address: any ● Src. Address Translated to: Outbound Interface Address

Procedure

- (1) Configure the WAN interface.
 - a Choose **Network > Interface > Physical Interface**.
 - b Select the physical interface to be used as the WAN interface and click **Edit**.

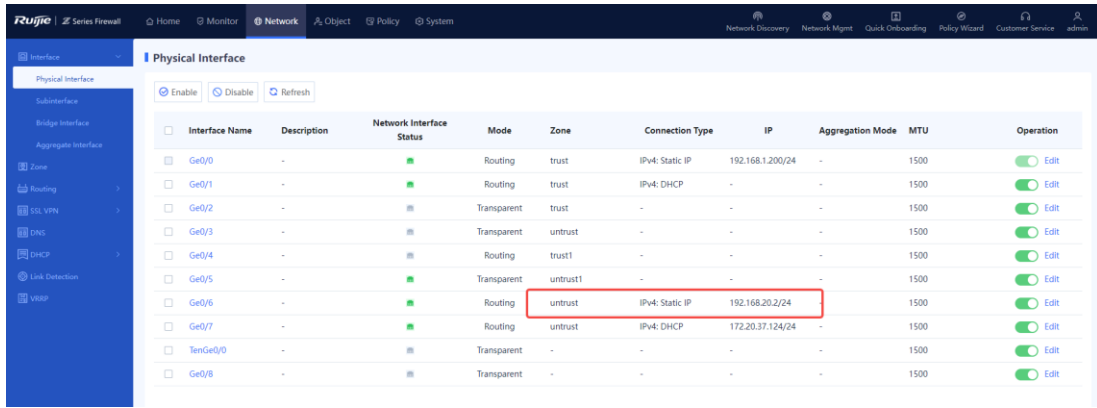


c Set parameters for the interface.

Item	Description
Mode	Routing Mode
Zone	untrust
Interface Type	WAN Interface
Connection Type	Static Address
IP/Mask	192.168.20.2/24
Next-Hop Address	192.168.20.1

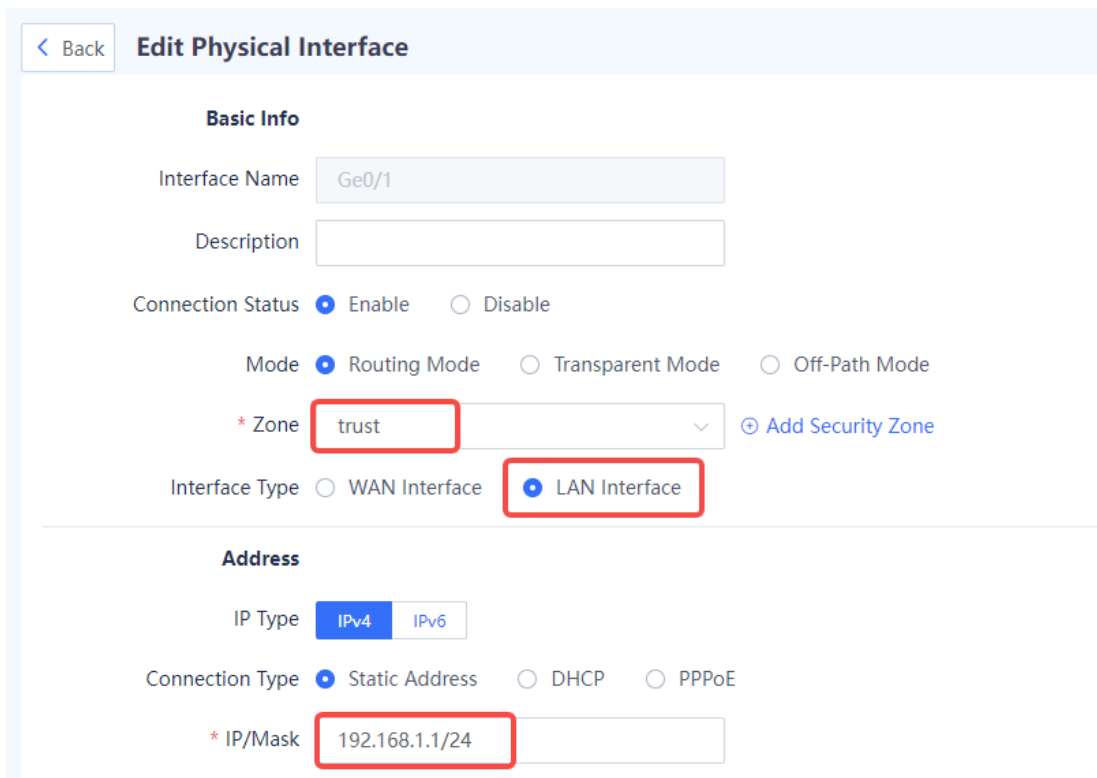
d Click **Save**.

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



(2) Configure the LAN interface.

- a Choose **Network > Interface > Physical Interface**.
- b Select the physical interface to be used as the LAN interface and click **Edit**.



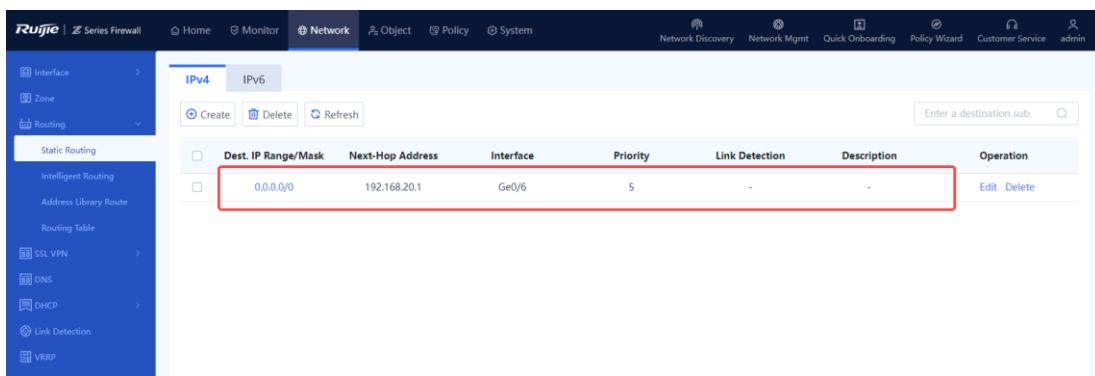
c Set parameters for the interface.

Item	Description
Mode	Routing Mode
Zone	trust
Interface Type	LAN Interface

Item	Description
Connection Type	Static Address
IP/Mask	192.168.1.1/24

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

After the WAN interface and LAN interface are successfully configured, choose **Network > Routing > Routing Table**. You can find that the device automatically generates a default route.



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

The screenshot shows the Ruijie Series Firewall configuration interface. The top navigation bar includes 'Home', 'Monitor', 'Network', 'Object', 'Policy', and 'System'. The 'Object' menu is selected, and the 'Address' sub-menu is active. The main content area is titled 'Add IPv4 Address Object' and contains two sections: 'Basic Info' and 'IP Address/Range'. In the 'Basic Info' section, the 'Name' field is set to 'lan' and the 'Description' field is empty. In the 'IP Address/Range' section, the 'IP Address/Range' field is set to '192.168.1.10'.

- c Set parameters for the address object.
 - a Set Name to lan and IP Address/Range to 192.168.1.10.
 - d Click **Save**.
- (4) Create a security policy.
 - a Choose **Policy > Security Policy**.
 - b Click **Create** and create a security policy.

< Back
Create Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security (After being enabled, the following configurations only take effect for IPv4 traffic.)

Intrusion Prevention Enable Not Enabled [⊕ Add Intrusion Prevention Template](#)

Virus Protection Enable Not Enabled [⊕ Add Virus Protection Template](#)

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

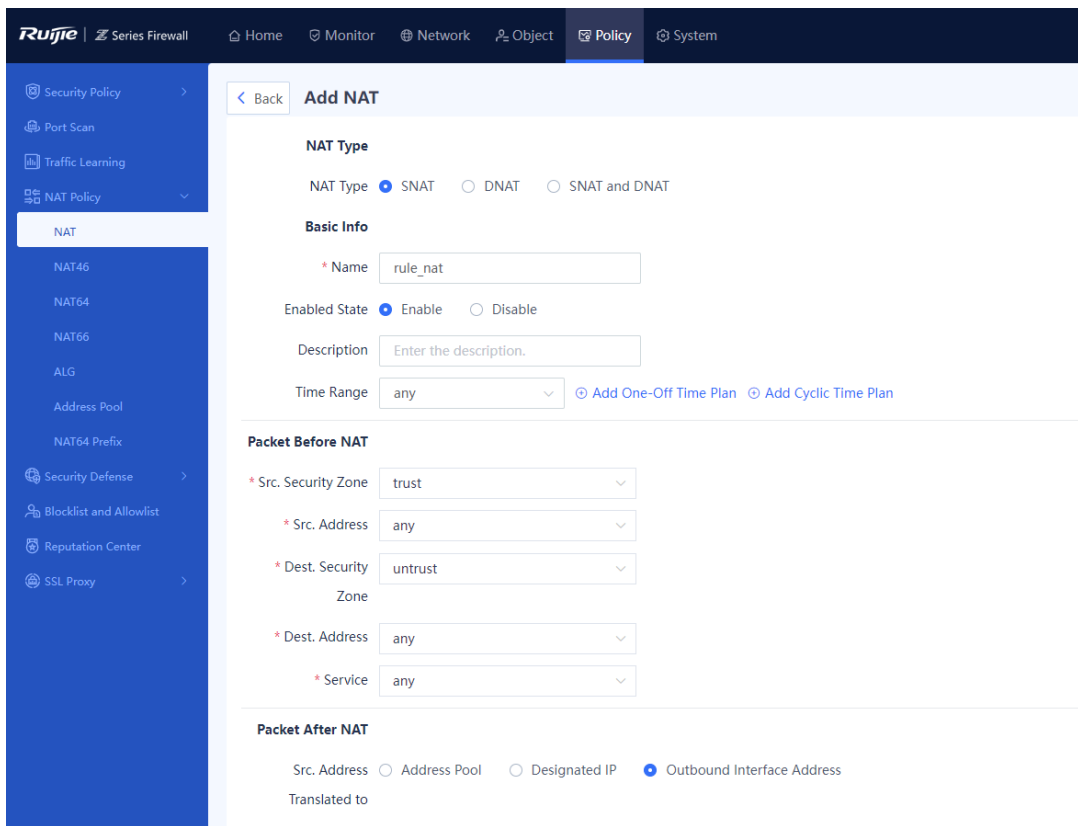
Advanced

c Set parameters for the security policy.

Item	Description
Src. Security Zone	trust
Src. Address	lan
Dest. Security Zone	untrust

Item	Description
Dest. Address	any
Service	any
App	any

- d Click **Save**.
- (5) Configure a NAT policy.
 - a Choose **Policy > NAT Policy > NAT**.
 - b Click **Create** and add a source NAT policy to translate the source address of traffic sent by a device in the zone **trust** and going out from a device in the zone **untrust**.



- c Set parameters for the NAT policy.

Item	Description
Src. Security Zone	trust
Src. Address	lan

Item	Description
Dest. Security Zone	untrust
Dest. Address	any
Src. Address Translated to	Outbound Interface Address

d Click **Save**.

Configuration Verification

Set the IP address of the PC to 192.168.1.10/24, gateway address to 192.168.1.1, and DNS server addresses to 114.114.114.114 (primary) and 223.5.5.5 (secondary). (The address of the local DNS server must be used.)

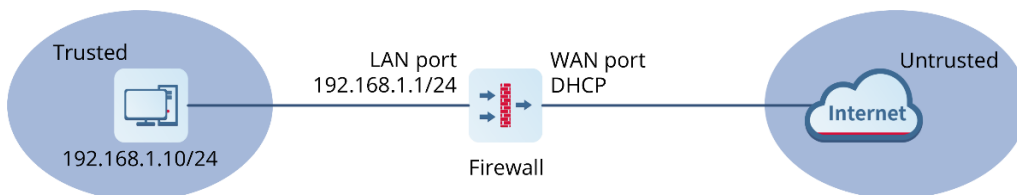
The PC can successfully ping the address 114.114.114.114.

3. Onboarding Through DHCP

Network Requirements

The PC is located in the LAN network segment 192.168.1.0/24. The WAN interface is connected to a dedicated line and specified by a static address by the ISP. The PC wants to access the Internet through the firewall.

Network Topology



Item	Description
Ge0/6	LAN interface, which belongs to the security zone trust. The IP address is 192.168.1.1/24.
Ge0/7	WAN interface, which belongs to the security zone untrust. This interface obtains an IP address through DHCP.

Configuration Points

Step	Description	Key Configuration
Configure interfaces.	<p>Select two interfaces on the device and set the interface type to WAN interface and LAN interface respectively.</p> <ul style="list-style-type: none"> ● WAN interface: Used to connect to the Internet. ● LAN interface: Used to connect to the LAN. 	<ul style="list-style-type: none"> ● WAN interface: Set Connection Type to DHCP. Add the interface to the security zone untrust. After the WAN interface obtains an IP address through DHCP, the system automatically generates a default route. ● LAN interface: Set the IP address to 192.168.1.1/24 and add the interface to the security zone trust. You can choose to enable some management functions on the interface.
Create an address object.	To facilitate management, configure the IP address of the LAN user as an address object.	Set the name to lan and IP address to 192.168.1.10.
Create a security policy.	Create a policy to control traffic between the LAN interface and WAN interface and enable NAT.	<ul style="list-style-type: none"> ● Src. Security Zone: trust ● Src. Address: lan ● Dest. Security Zone: untrust ● Dest. Address: any

Procedure

- (1) Configure the WAN interface.
 - a Choose **Network > Interface > Physical Interface**.
 - b Select the physical interface to be used as the WAN interface and click **Edit**.

< Back
Edit Physical Interface

Basic Info

Interface Name

Description

Connection Status Enable Disable

Mode Routing Mode Transparent Mode Off-Path Mode

* Zone [Add Security Zone](#)

Interface Type WAN Interface LAN Interface

Address

IP Type IPv4 IPv6

Connection Type Static Address DHCP PPPoE

c Set parameters for the interface.

Item	Description
Mode	Routing Mode
Zone	untrust
Interface Type	WAN Interface
Connection Type	DHCP

d Click **Save**.

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

Physical Interface

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

(2) Configure the LAN interface.

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

b Select the physical interface to be used as the LAN interface and click **Edit**.

< Back

Edit Physical Interface

Basic Info

Interface Name

Description

Connection Status Enable Disable

Mode Routing Mode Transparent Mode Off-Path Mode

* Zone [⊕ Add Security Zone](#)

Interface Type WAN Interface LAN Interface

Address

IP Type IPv4 IPv6

Connection Type Static Address DHCP PPPoE

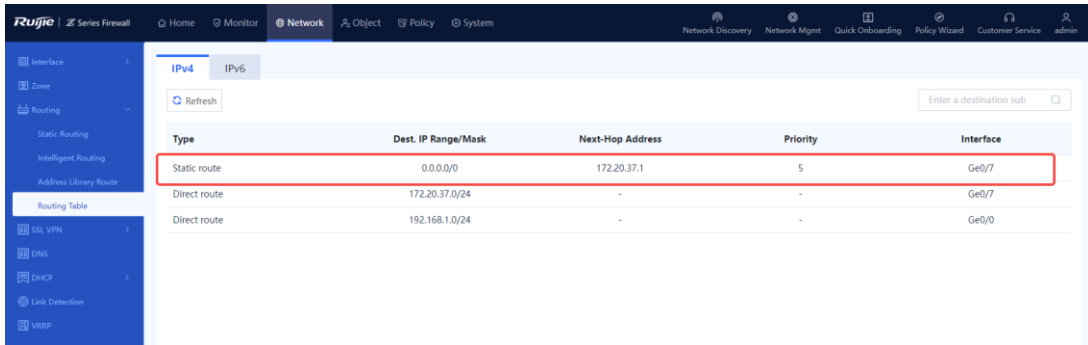
* IP/Mask

- c Set parameters for the interface.

Item	Description
Mode	Routing Mode
Zone	trust
Interface Type	LAN Interface
Connection Type	Static Address
IP/Mask	192.168.1.1/24

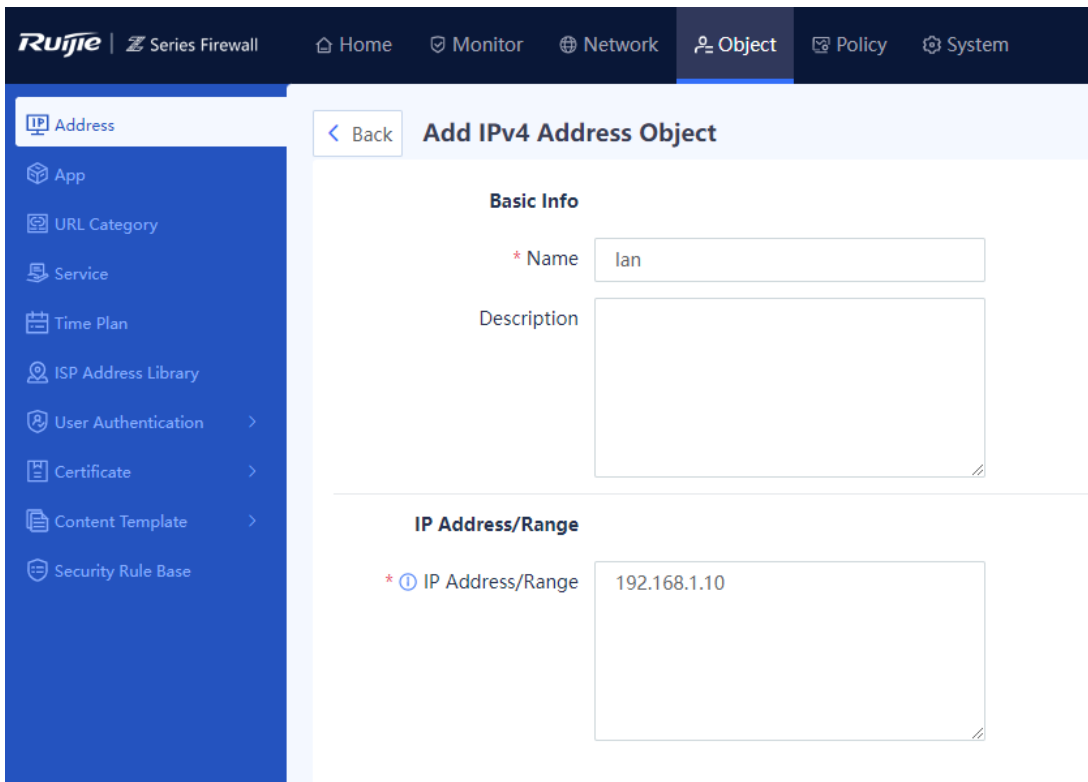
- d Enable management functions on the interface as required. You are advised to enable the HTTPS, ping, and SSH services only on the LAN interface.
- e Click **Save**.

After the WAN interface and LAN interface are successfully configured, choose **Network > Routing > Routing Table**. You can find that the device automatically generates a default route.



(3) Configure address resources.

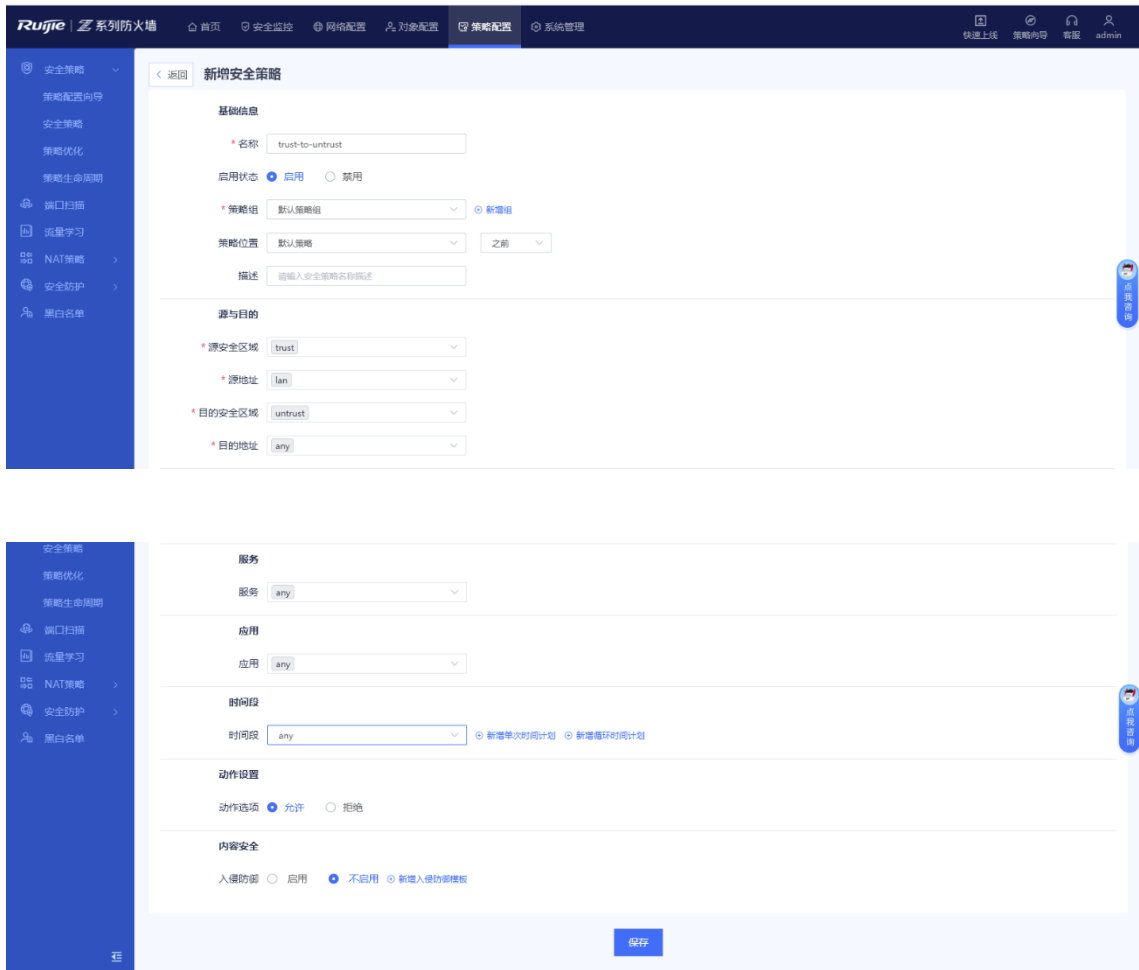
- a Choose **Object > Address > IPv4 Address**.
- b Click **Create** and add an address object with a LAN IP address.



- c Set Name to lan and IP Address/Range to 192.168.1.10.
- d Click **Save**.

(4) Create a security policy.

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



c Set parameters for the security policy.

Item	Description
Src. Security Zone	trust
Src. Address	lan
Dest. Security Zone	untrust
Dest. Address	any
Service	any
App	any

d Click **Save**.

(5) Configure a NAT policy.

a Choose **Policy > NAT Policy > NAT**.

- b Click **Create** and add a source NAT policy to translate the source address of traffic sent by a device in the zone **trust** and going out from a device in the zone **untrust**.

< Back
Create Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security (After being enabled, the following configurations only take effect for IPv4 traffic.)

Intrusion Prevention Enable Not Enabled [⊕ Add Intrusion Prevention Template](#)

Virus Protection Enable Not Enabled [⊕ Add Virus Protection Template](#)

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

Advanced

- c Set parameters for the NAT policy.

Item	Description
Src. Security Zone	trust
Src. Address	lan

Item	Description
Dest. Security Zone	untrust
Dest. Address	any
Src. Address Translated to	Outbound Interface Address

- d Click **Save**.

Configuration Verification

Set the IP address of the PC to 192.168.1.10/24, gateway address to 192.168.1.1, and DNS server addresses to 114.114.114.114 (primary) and 223.5.5.5 (secondary). (The address of the local DNS server must be used.) The PC can successfully ping the address 114.114.114.114.

7.4 Off-Path Mode

7.4.1 Preparations

Confirm the following information before performing the configuration:

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

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

⚠ Caution

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

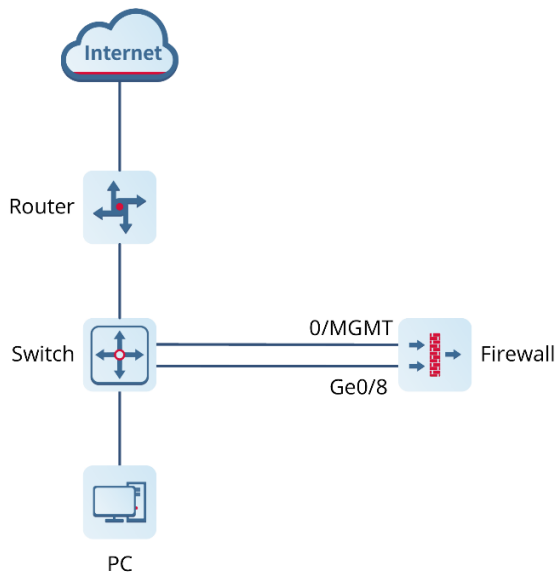
7.4.2 Deployment in Off-Path Mode (Quick Deployment)

Network Requirements

If the customer wants to use a firewall to monitor the network security information on the live network but does not want to change the physical structure of the current network, the firewall can be deployed in off-path mode. In this mode, the firewall is connected to the switch in off-path mode, and traffic of the switch is mirrored to the off-path interface for detection, providing the security protection function. This mode monitors the security of the customer network without changing the network structure and affecting data forwarding of the customer.

In off-path mode, the firewall does not forward traffic, but provides security protection for the monitored areas instead.

Network Topology



Configuration Points

- (1) Implement quick onboarding. Select a deployment mode (off-path mode) and configure an off-path interface. Configure an IP address and the next hop for the management interface (0/MGMT) to ensure successful connection to the Internet.
- (2) (Optional) Check the connectivity. The system automatically checks whether the firewall is connected to the Internet.
- (3) Complete the quick onboarding configuration.
- (4) (Optional) Implement remote O&M on the cloud.
- (5) Mirror the switch traffic to the off-path interface of the firewall. (Omitted)

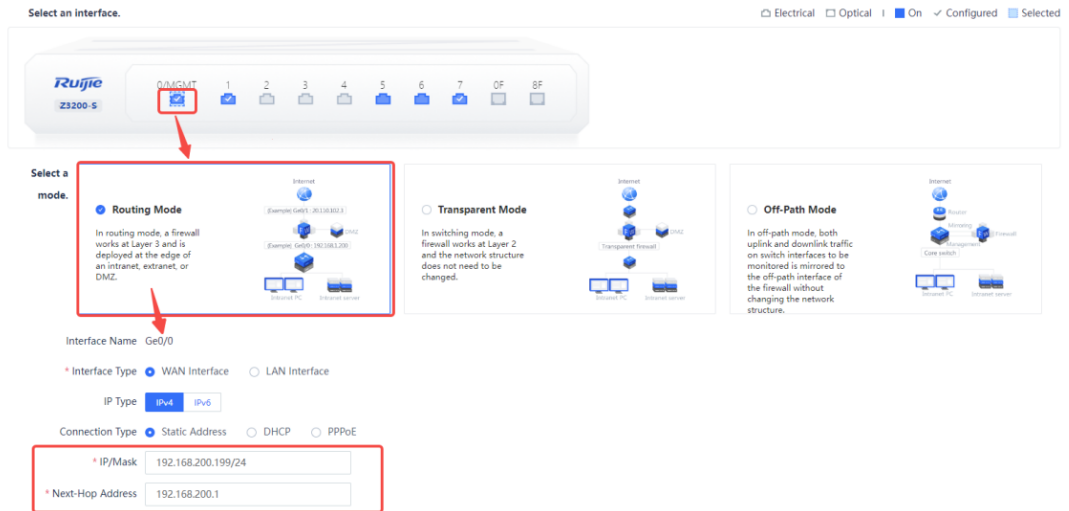
(6) Create a security policy to permit the off-path detection traffic.

Procedure

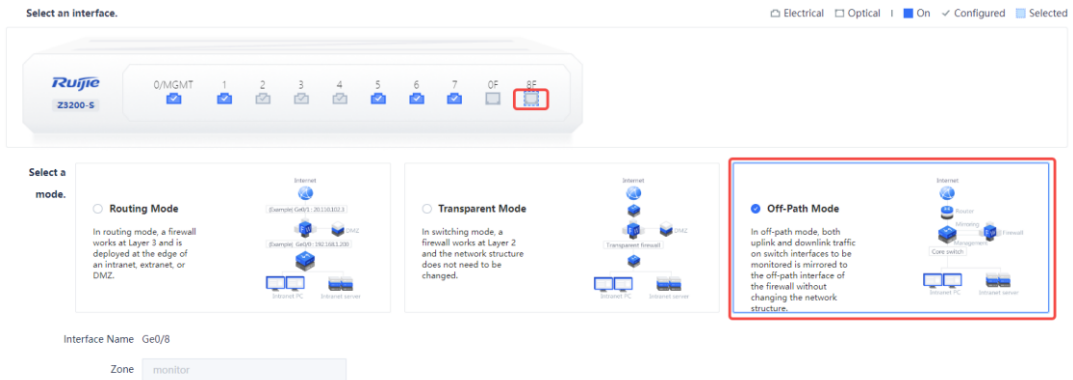
(1) Implement quick onboarding.

a Configure interfaces.

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



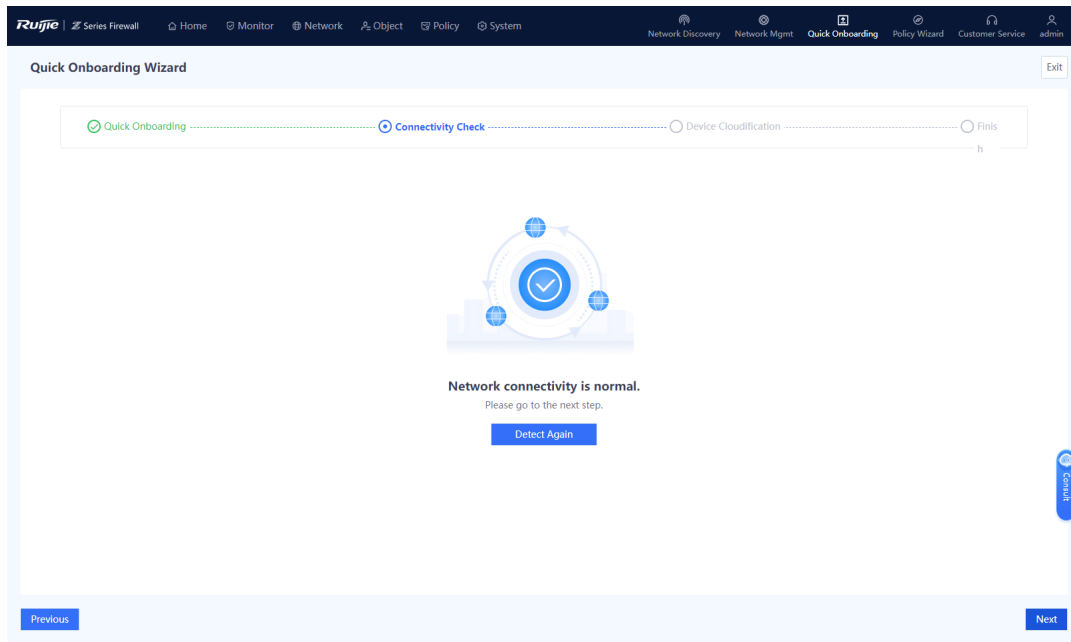
- o Configure another interface as the off-path interface. This example uses Ge0/8 as the off-path interface.



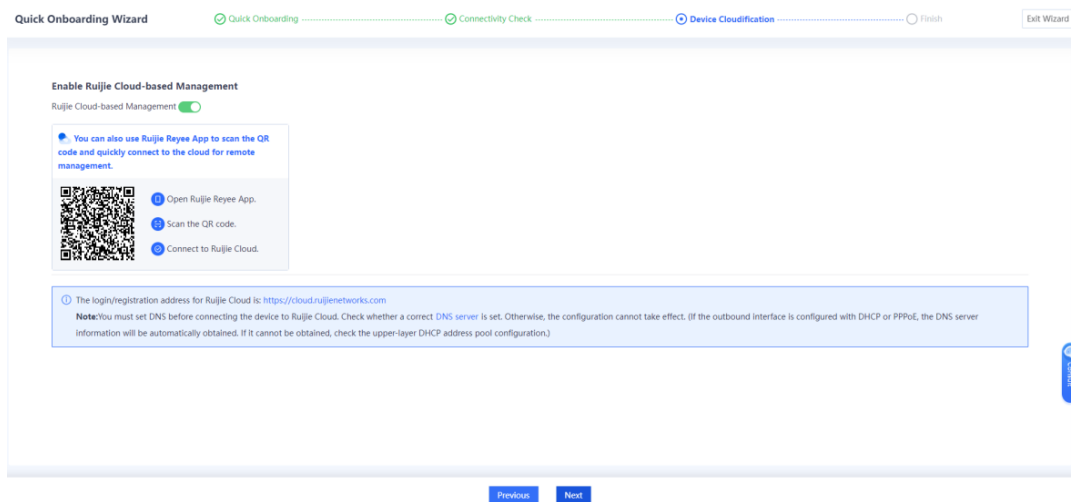
Note

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

(2) (Optional) Check the connectivity.



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



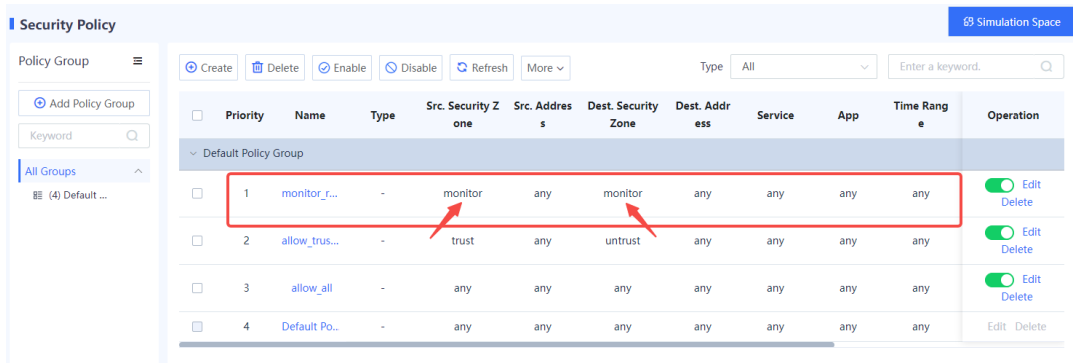
(4) Configure the switch to mirror both uplink and downlink traffic on switch interfaces to be monitored to the off-path interface Ge0/8. (Omitted)

i Note

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

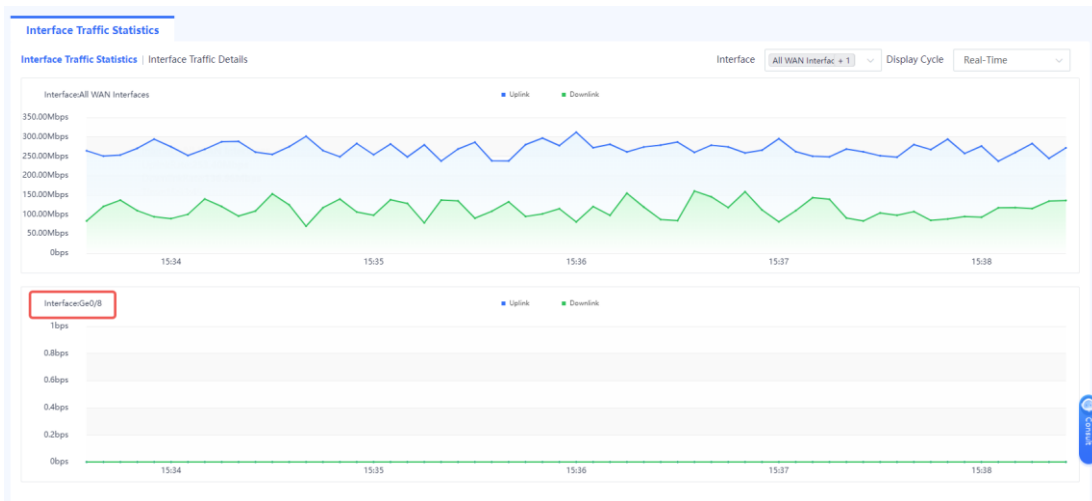
(5) Create a security policy.

After the quick deployment configuration is complete, the security policy **allow_all** is generated automatically. This security policy permits all traffic by default. To control and detect the traffic in off-path mode, you need to create a security policy in which both **Src. Security Zone** and **Dest. Security Zone** are set to **monitor**.



Configuration Verification

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



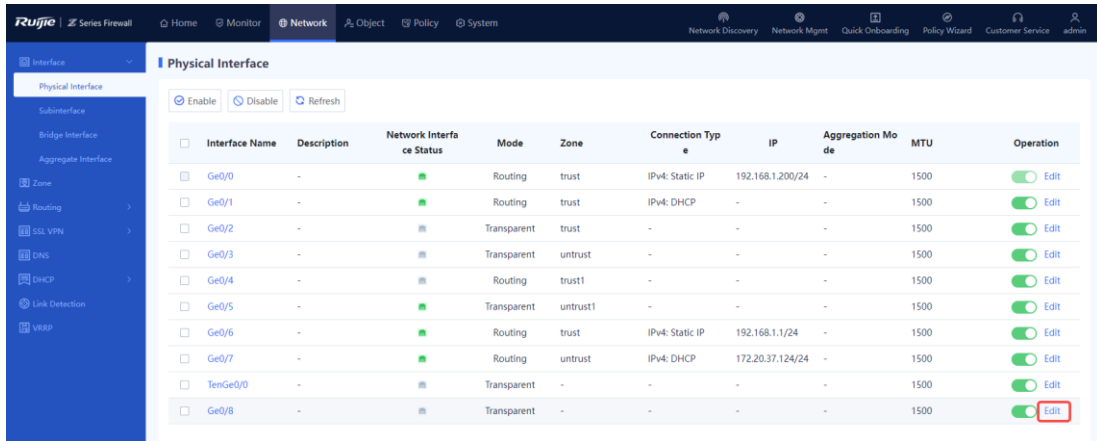
7.4.3 Configuring an Off-Path Interface (Custom Deployment)

Configuration Points

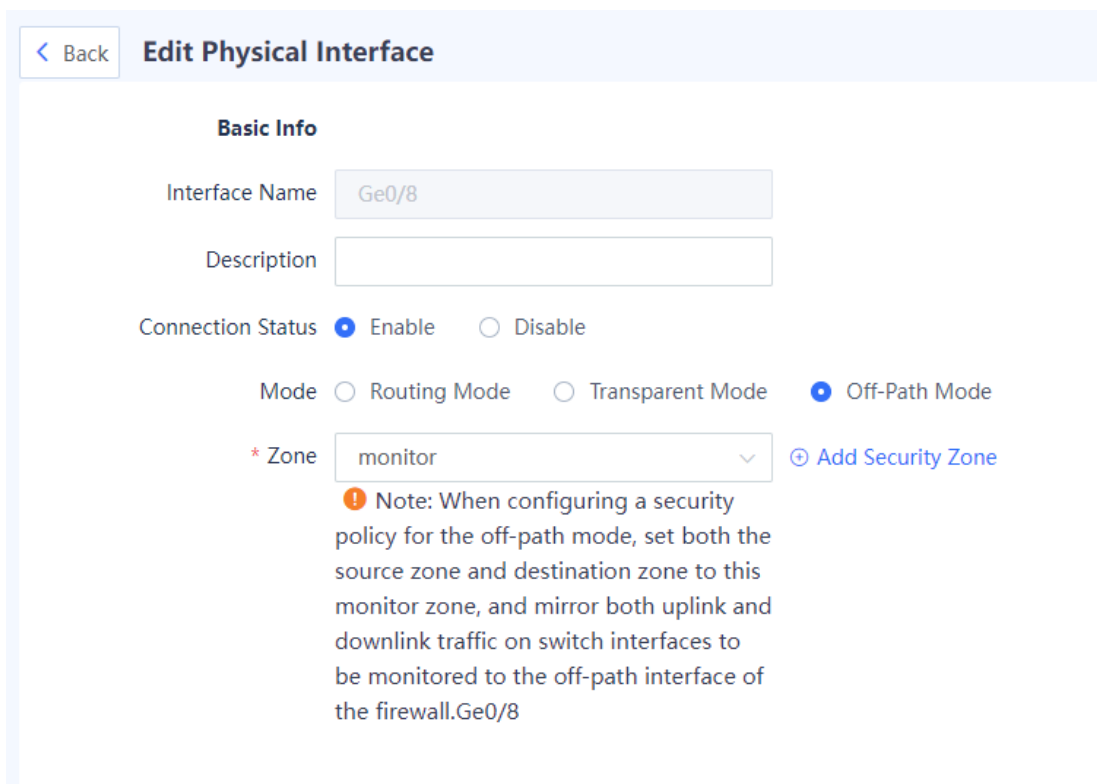
An off-path interface is an interface set to off-path mode and is used only to receive mirrored traffic but cannot forward traffic. Security zone **monitor** defines the zone traffic of which needs to be monitored, and all off-path interfaces belong to the zone **monitor**. When you create a security policy in off-path mode, you need to set both **Src. Security Zone** and **Dest. Security Zone** to **monitor**.

Procedure

- (1) Configure interfaces.
 - a Choose **Network > Interface > Physical Interface**, find the desired interface, and click **Edit** in the **Operation** column. The Ge0/8 port is used as an example.



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

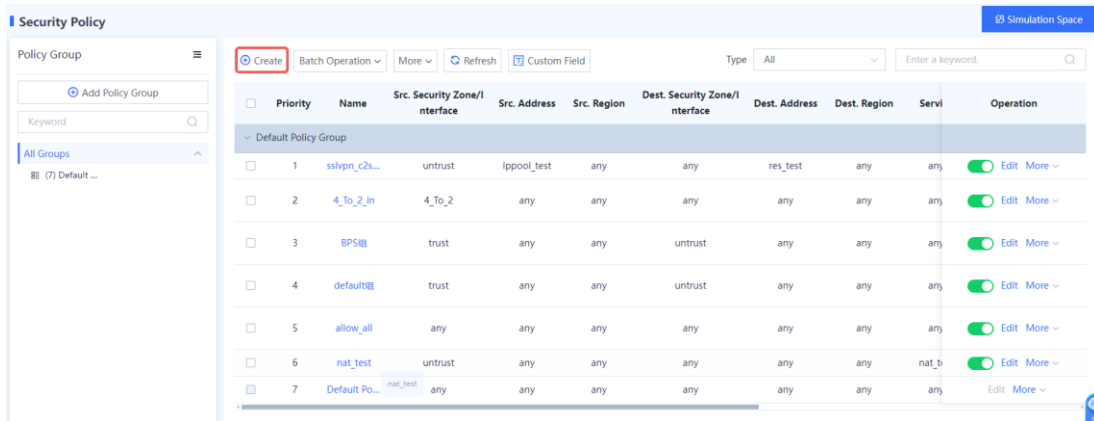


c Click **Save**.

(2) Create a security policy.

The security zone of the off-path interface is **monitor** by default. To facilitate management, you are advised to separately configure a security control policy for off-path detection traffic.

a Choose **Policy > Security Policy > Security Policy** and click **Create**.



- b Access the simulation space and run the configured security policies in advance to ensure their security, or click **Create** to apply the security policy to the firewall.

Tip



Are you sure you want to add it in the simulation space?

The policy execution process can be simulated before actual execution. The simulation helps you identify vulnerabilities and issues in policies in advance and avoid risks to services in actual execution.

Do Not Show This Again

Simulation Space Create

- c Create a security policy in which both **Src. Security Zone** and **Dest. Security Zone** are set to **monitor** to implement access control and detection on the off-path traffic based on actual needs.

< Back
Create Security Policy

Basic Info

* Name

Enabled State Enable

* Policy Group [Add Group](#)

* Priority

Description

Src. and Dest.

Src. Security
Zone/Interface

* Src. Address

Src. Region

Dest. Security
Zone/Interface

* Dest. Address

Dest. Region

Service

Action Option Permit Deny

[App, User, Effective Time](#)

Content Security

Intrusion Prevention Disable

Virus Protection Disable

URL Filtering Disable

Keyword Filtering Disable

Advanced

7.4.4 Precautions for Deploying Off-Path Mode

- When you deploy the firewall as the off-path detection device, you need to connect the interface receiving the detection traffic to the switch and configure the switch to mirror both uplink and downlink traffic on switch interfaces to be monitored to the firewall interface for detection.
- When you create a security policy in off-path mode (for access control of the off-path detection traffic), you need to set both **Src. Security Zone** and **Dest. Security Zone** to **monitor**.
- When off-path detection is enabled on the interface, the firewall detects traffic passing through the interface rather than forwarding the traffic.

8 Common Operations

8.1 NAT Policy

8.1.1 NAT Technology

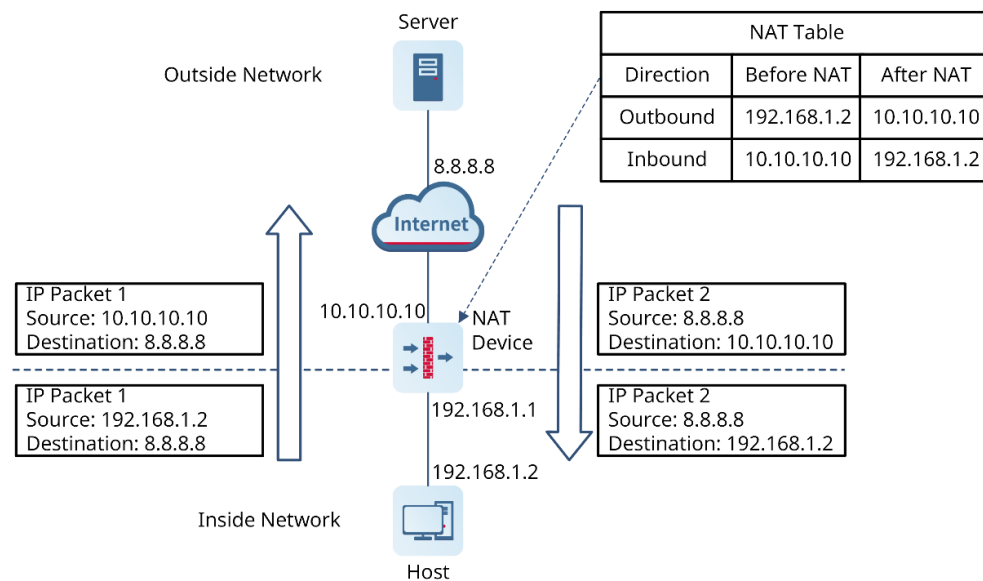
Network Address Translation (NAT) is to translate the source address (port) or destination address (port) in a packet into the desired address. NAT includes the following two steps:

- (1) Translate the original address into the mapped address.
- (2) Restore the address in the returned packet.

The advantages of NAT are:

- Private network addresses can be used on an intranet. Private network addresses are not routable on the Internet, and can only be used after being converted to public network addresses.
- NAT hides the real IP addresses so that attackers cannot know the real addresses of hosts.
- If two network addresses overlap, they can use NAT to communicate with each other.

The following figure shows a typical working process of NAT.



- (1) IP packet 1 sent by the intranet user host (192.168.1.2) to the extranet server (8.8.8.8) will pass through the NAT device.
- (2) After checking the packet header, the NAT device finds that packet 1 is destined for the Internet, so it translates the private address 192.168.1.2 in its source IP address field into a public network address 10.10.10.10 that can be routed on the Internet and sends packet 1 to the extranet server. In addition, the NAT device records the mapping relationship in the NAT table.
- (3) After reply packet 2 (whose initial destination IP address is 10.10.10.10) sent by the extranet server to the intranet host arrives at the NAT device, the NAT device checks the header again, searches the NAT table for the record of the current network address, and then replaces the initial destination IP address with the private address 192.168.1.2.

- (4) The NAT process described above is transparent to the endpoints (such as the host and server in the figure). The extranet server only knows that the IP address of intranet host is 10.10.10.10, but does not know the address 192.168.1.2. Therefore, NAT "hides" the private network of the enterprise.

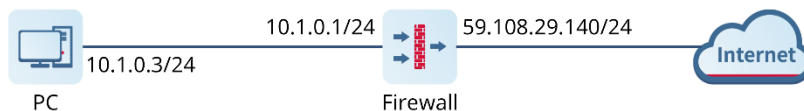
The Z-S series firewalls support multiple NAT modes to implement unidirectional and bidirectional translation between public IP addresses and private IP addresses. They are often used as specialized NAT devices. The NAT modes supported by Z-S series firewalls include:

- Static NAT
- Dynamic NAT
- PAT

1. Static NAT

Static NAT fixedly translates the original addresses into mapped addresses, regardless of inbound and outbound. As shown in [Figure 8-1](#), 10.1.0.3 and 59.108.29.187 are one-to-one mapped. Different from dynamic NAT and PAT, static NAT is a fixed translation procedure, so the destination network can also access the source network.

Figure 8-1 Static NAT Example

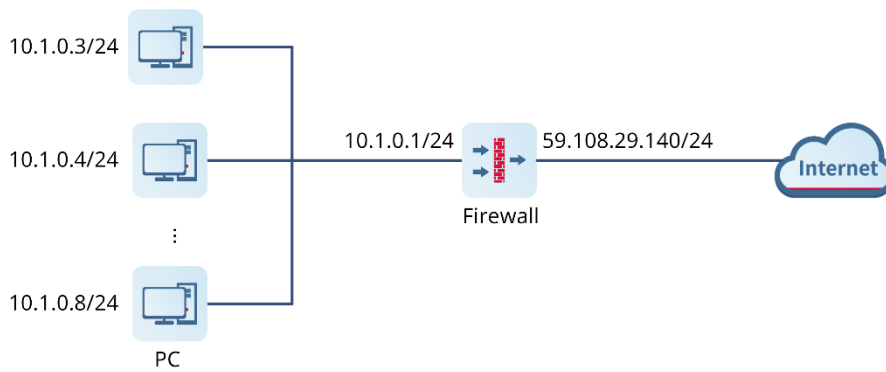


NAT Direction	Address Before NAT	Address After NAT
SNAT	10.1.0.3	59.108.29.187
DNAT	59.108.29.187	10.1.0.3

2. Dynamic NAT

Dynamic NAT translates a group of original IP addresses into a pool of mapped addresses that can be routed on the destination network. The number of addresses in the mapped address pool can be smaller than the number of original IP address. The translation process is a one-to-one mapping between the original address and the mapped address. This mapping relationship is available only when the session is valid. When the session becomes invalid, the mapping relationship is canceled. As shown in [Figure 8-2](#), addresses 10.1.0.[3-8] are translated into addresses 59.108.29.[90-99], to implement the communication between the intranet and the Internet. However, the devices on the Internet do not know the addresses 10.1.0.[3-8].

Figure 8-2 Dynamic NAT Example

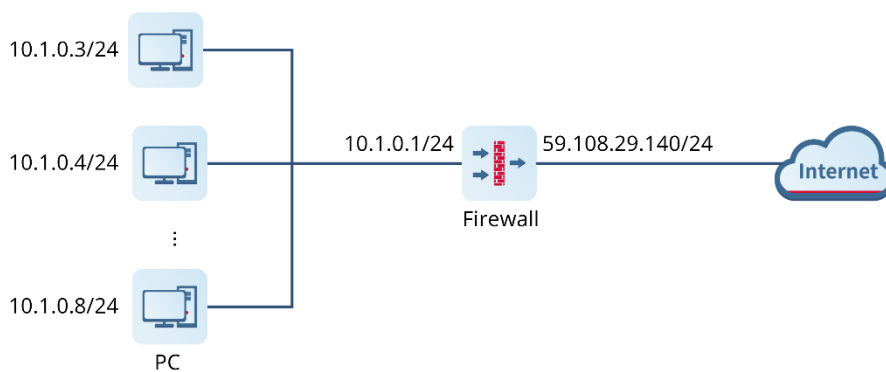


NAT Direction	Address Before NAT	Address After NAT
SNAT	10.1.0.3-10.1.0.8	59.108.29.90-59.108.29.99
DNAT	59.108.29.90-59.108.29.99	10.1.0.3-10.1.0.8

3. PAT

Port Address Translation (PAT) maps multiple IP addresses into one public IP address. In the process of address translation, the original addresses and the original ports are translated into mapped addresses and ports whose numbers are greater than 1024. Every connection requires an independent translation process because the source ports of the connections' original IP addresses are different. As shown in [Figure 8-3](#), 10.1.0.3:1025 and 10.1.0.3:1026 requires different translation processes. PAT can fully use existing public IP address resources on the Internet.

Figure 8-3 PAT Example



NAT Direction	Address Before NAT	Address After NAT
SNAT	10.1.0.3-10.1.0.8	59.108.29.140

DNAT	59.108.29.140	10.1.0.3-10.1.0.8
------	---------------	-------------------

4. Firewall Policy-based NAT

Z-S series firewalls can realize fine-grained control of the above NAT modes, so that the NAT function can fully meet the needs of customers, which is very flexible and convenient. You can perform NAT policy control from the following dimensions:

- Perform NAT for certain addresses.
- Perform NAT in the required time segments.
- Perform NAT for certain destination addresses.
- Perform NAT for certain services.
- Perform NAT from a specified port to another specified port.

8.1.2 Application Scenario

Network Address Translation (NAT) is typically used on edge devices that connect two networks. By translating an IP address in a packet header into another IP address, NAT enables mutual access between different types of networks, such as IPv4 and IPv6 networks as well as intranets and extranets.

The following table lists the translation principles and scenarios of different types of NAT.

NAT Type	Principles	Application Scenario
Destination NAT	Translate the destination address (public IPv4 address) in a packet into a private IPv4 address.	Public network users can use public network addresses to access intranet servers.
Twice NAT	Translate the source address (private IPv4 address) and destination address (public IPv4 address) in a packet to other IPv4 addresses separately.	Intranet users can use public network addresses to access intranet servers.
Static NAT-PT	Configure one-to-one static mappings between IPv6 and IPv4 addresses to translate IPv4 and IPv6 addresses.	Fixed mutual access is required between an IPv4 network and an IPv6 network. For example, a host on an IPv4 network needs to access a fixed web server on an IPv6 network.
Dynamic NAT-PT	Configure dynamic mappings between IPv6 and IPv4 addresses to translate IPv4 and IPv6 addresses.	No fixed mutual access is required between an IPv4 network and an IPv6 network. For example, a host on an IPv6 network needs to access multiple servers on an IPv4 network.

NAT Type	Principles	Application Scenario
Stateless NAT64	Configure NAT64 prefix information to translate source and destination IPv4 or IPv6 addresses using the address translation algorithms defined in RFCs.	Multipoint-to-multipoint mutual access is required between an IPv4 network and an IPv6 network.
Static NAT64	Configure static mappings between IPv6 and IPv4 addresses to translate source and destination addresses in IPv6 packets to IPv4 addresses.	Multipoint-to-point mutual access is required between IPv4 and IPv6 networks.
Dynamic NAT64	Configure dynamic mappings between IPv6 and IPv4 addresses to translate source and destination addresses in IPv6 packets to IPv4 addresses.	Dynamic NAT64 only applies to scenarios where an IPv6 host initiates a request to access an IPv4 network (for example, an IPv6 user needs to access an IPv4 server).
NAT66-source NPTv6	Translate the source IPv6 address prefix in an IPv6 packet into another IPv6 address prefix.	Intranet users proactively access an extranet.
NAT66-destination NPTv6	Translate the destination IPv6 address prefix in an IPv6 packet into another IPv6 address prefix.	Servers on an intranet provide services (for example, web services and FTP services) to an extranet.

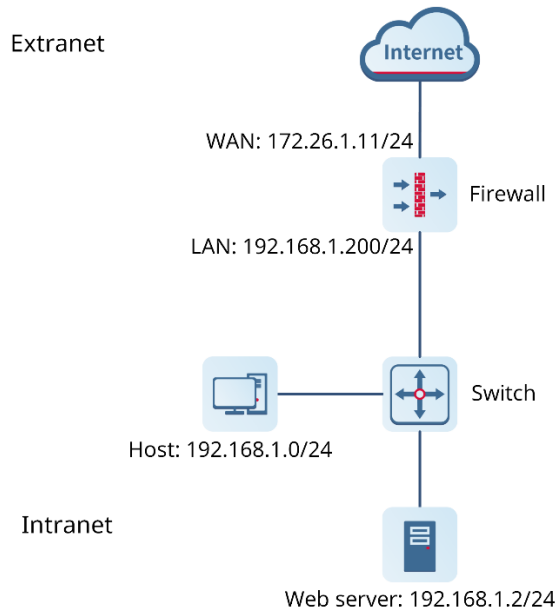
8.1.3 Configuring Destination Address Translation (One-to-One Port Mapping)

Network Requirements

After completing the basic firewall configurations, you need to map a web server (192.168.1.2) on the intranet to the address of an extranet port (172.26.1.116) so that users on the extranet can access this server.

In addition, intranet users can use the public network address to access the server.

Network Topology



Configuration Points

- (1) Complete basic network access settings.
- (2) Configure a custom service.
- (3) Configure the security policy.
- (4) Configure port mapping.

Procedure

- (1) Complete basic network access settings.

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

The interface configuration is as follows:

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

- (2) Configure a custom service.
 - a Choose **Object > Service > Custom Service**.
 - b Click **Create** and create a custom service **18080**. In the **Protocol List** area, click **Create**. In the dialog box that is displayed, set the protocol to TCP, the source port to 0-65535, and the destination port to 18080 (external port).

Add Service

Basic Info

* Service Name

Description

* Protocol List

<input type="checkbox"/>	Protocol	Src. Port	Dest. Port	Type	Code	Operation
No Data						
Total: 0						

c Click **Save**.

(3) Configure the security policy.

The policy configuration is as follows:

<input type="checkbox"/>	2	allow_trus...	-	trust	any	untrust	any	any	any	any	<input checked="" type="checkbox"/> Perm
allow_trust_to_untrust											

(4) Configure port mapping.

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

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

< Back
Add NAT

NAT Mode

NAT Mode SNAT DNAT Twice Nat

Basic Info

* Name

Enabled State Enable Disable

Description

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

Packet Before NAT

* Src. Security Zone

* Src. Address

* Dest. Address

* Service

Packet After NAT

* IP

Port

Save

Item	Description
Basic Info	
Name	WebServer
Enabled State	Enable
Packet Before NAT	
Src. Security Zone	untrust and trust
Src. Address	any
Dest. Address	WAN interface address: 172.26.1.116
Service	Select the custom service 18080 created in step (2).
Packet After NAT	
IP Address	192.168.1.2

Item	Description
Port	80 (internal port)

c Click **Save**.

Verification

Users can visit <http://172.26.1.116> from the Internet.

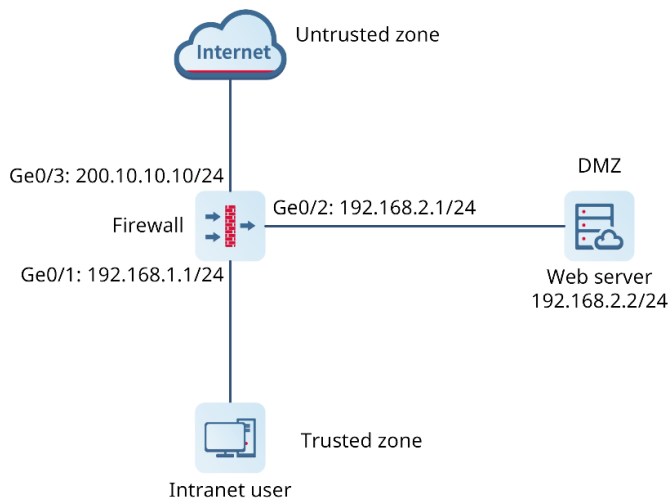
8.1.4 Configuring Bidirectional Address Translation (Allowing Intranet PCs to Access the Map Server by Using a Public Network Address)

Network Requirements

After completing the basic firewall configurations, you need to map a web server (192.168.2.2) on the intranet to the address of an extranet port (200.10.10.10) so that users on the intranet and the extranet can access this server.

- The web server is in the intranet server zone (zone: DMZ; IP address: 192.168.2.2; service: HTTPS).
- Extranet users need to access the server by accessing the extranet port address of the firewall (zone: untrust; IP address: 200.10.10.10; port 50000).
- Intranet users (zone: trust) also need to access the server by accessing the extranet port address of the firewall (zone: untrust; IP address: 200.10.10.10; port 50000), and the source address used to access the server is the extranet port of the firewall.

Network Topology



Configuration Points

- (1) Complete basic network access settings.
- (2) Configure a custom service.
- (3) Configure the security policy.
- (4) Configure bidirectional address translation.

- a Configure the destination address translation policy for extranet users.
- b Configure the twice NAT policy for intranet users.

Procedure

(1) Complete basic network access settings.

For details, see [7.3 Routing Mode](#).

(2) Configure a custom service.

- a Choose **Object > Service > Custom Service**.
- b Click **Create** and create a custom service **Server_Mapping**. In the **Protocol List** area, click **Create**. In the dialog box that is displayed, set the protocol to TCP, the source port to 0-65535, and the destination port to 50000.

Add Service ✕

Basic Info

* Service Name

Description

* **Protocol List**

<input type="checkbox"/>	Protocol	Src. Port	Dest. Port	Type	Code	Operation
<input type="checkbox"/>	TCP	0-65535	50000	-	-	Edit Delete

Total: 1

c Click **Save**.

(3) Configure the security policy.

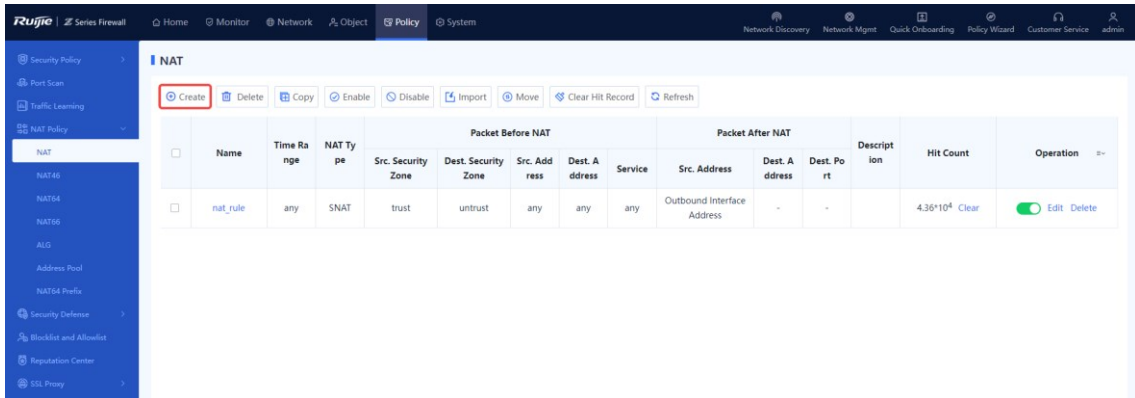
The policy configuration is as follows:

<input type="checkbox"/>	Priority	Name	Type	Src. Security Zone	Src. Addresses	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hi	Operation
▼ Default Policy Group														
<input type="checkbox"/>	1	permit_loca	IPv4	trust	lan_users	untrust	any	any	any	any	<input checked="" type="checkbox"/> Perm		0	<input checked="" type="checkbox"/> Edit Delete

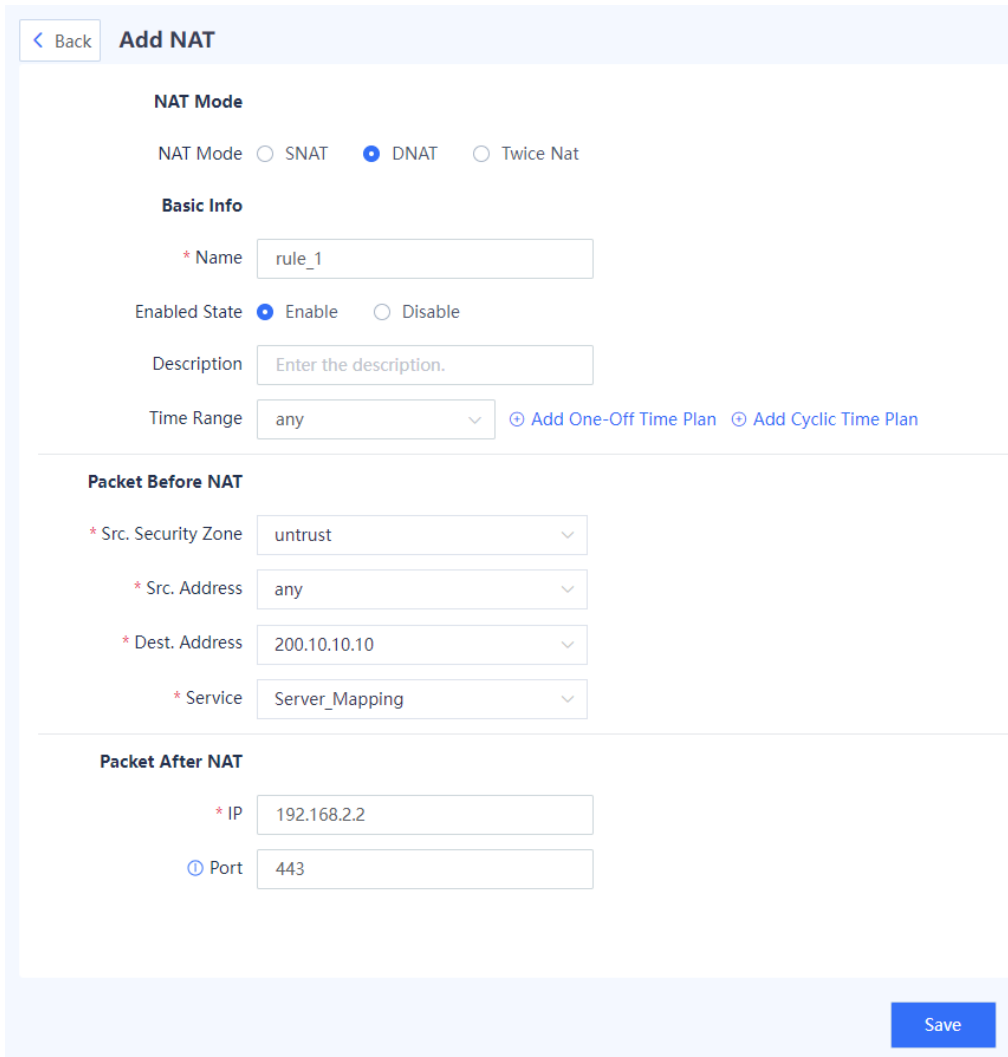
(4) Configure port mapping.

Configure the destination address translation policy for extranet users.

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



- c Set the parameters related to destination address translation.



Item	Description
Basic Info	
Name	rule_1
Enabled State	Enable
Packet Before NAT	
Src. Security Zone	untrust
Src. Address	any
Dest. Address	Extranet port IP address of the firewall: 200.10.10.10
Service	Select the custom service Server_Mapping created in step (2).
Packet After NAT	
IP Address	Set the destination address to the IP address of web server in the DMZ, 192.168.2.2.
Port	Set the destination port to 443 (web server port).

Configure the twice NAT policy for intranet users.

- a Choose **Policy > NAT Policy > NAT**.
- b Click **Create**.
- c Set the parameters for twice NAT.

< Back

Add NAT

NAT Mode

NAT Mode SNAT DNAT Twice Nat

Basic Info

* Name

Enabled State Enable Disable

Description

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

Packet Before NAT

* Src. Security Zone

* Src. Address

* Dest. Address

* Service

Packet After NAT

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

* Designated IP

* Dest. Address

Translated to

ⓘ Dest. Port Number

Translated to

Item	Description
Basic Info	
Name	rule_2
Enabled State	Enable
Packet Before NAT	
Src. Security Zone	trust
Src. Address	any
Dest. Address	Extranet port IP address of the firewall: Ge0/3:200.10.10.10.

Item	Description
Service	Select the custom service Server_Mapping created in step (2).
Packet After NAT	
Src. Address Translated to	In source address translation, configure the specified IP address 200.10.10.10 as the firewall's extranet address. If the firewall has multiple extranet addresses, you can configure an address pool as the extranet address, and then apply the address pool. Note: If the extranet address is configured as an egress interface address, the source IP address will be translated into 192.168.2.1, which does not meet requirements.
Designated IP	Firewall's extranet address, for example, 200.10.10.10
Dest. Address Translated to	Set the destination address to the IP address of web server in the DMZ, 192.168.2.2.
Dest. Port Number Translated to	Set the destination port to 443 (web server port)

d Click **Save**.

Verification

- Visit <http://200.10.10.10:50000> from the intranet.
- Visit <http://200.10.10.10:50000> from the extranet.

The NAT policy is successfully configured if the intranet web server is accessible both from the intranet and extranet.

8.1.5 Configuration Example of Static NAT-PT Networking

1. Applicable Products and Versions

Table 8-1 Products and Versions

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R5 or later

2. Service Demands

In a NAT64 networking scenario, NAT-PT policies are typically deployed on the edge devices of IPv4 and IPv6 networks to translate addresses in mutual access packets between the IPv4 and IPv6 networks.

As shown in the following figure, a company is upgrading an IPv4 network to an IPv6 network. Before the network-wide upgrade, partial network upgrade is performed first, and the network of an existing internal public server has been upgraded from IPv4 to IPv6. In this case, a NAT-PT policy needs to be configured on the firewall to translate IPv4 addresses into IPv6 addresses so that the public server can be accessed by the IPv4 network.

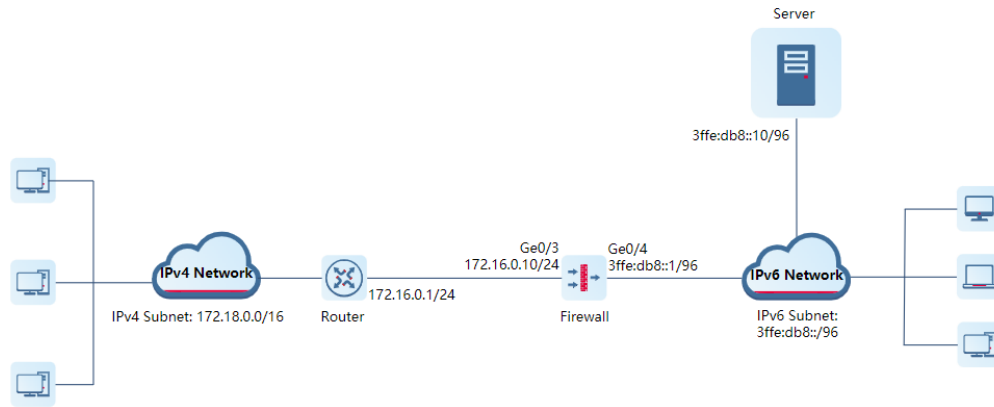


Table 8-2 Key Configuration Points in the Network Diagram

Item	Description
Pure IPv4 network	172.18.0.0/16
IPv4 network egress address	172.16.0.1/24
Public server	3ffe:db8::10/96
Pure IPv6 network	3ffe:db8::/96
NAT64 prefix information	2ffe:db8::/96, for route egress selection control
IPv4 address object	172.16.0.1, source IP address for accessing the public server 172.16.0.10, destination IP address for accessing the public server
IPv6 address object	3ffe:db8::10, for refined filtering based on security policies
Source IPv6 address after NAT	2ffe:db8::10
Destination IPv6 address after NAT	3ffe:db8::10
Firewall management port	Ge0/0, for accessing the firewall web UI and performing configurations
IP address of the firewall management port	192.168.1.200
Any IPv4 address	0.0.0.0-255.255.255.255

3. Restrictions and Guidelines

- The destination IPv4 address that matches a static NAT-PT rule cannot be a non-local interface IP address on the same network segment as the inbound interface (for example, 172.16.0.100). You are advised to configure the destination IPv4 address as the IPv4 address of the inbound interface.
- The source or destination IPv4 address object that matches a static NAT-PT rule can only contain one IP address (that is, only one IP address can be configured). This restriction can be ignored if no device on an IPv6 network proactively accesses the IPv4 network.
- The source IPv6 address after NAT must be on the same network segment as the configured NAT64 prefix. For example, if the NAT64 prefix is 2ffe:db8::/96, the source IPv6 address after NAT is 2ffe:db8::10.
- If a static NAT-PT rule needs to match any IPv4 address, you need to configure an any IPv4 address object. The default any object cannot be used, because it covers both any IPv4 address and any IPv6 address.

4. Prerequisites

You have completed basic network configurations, including interface IP address and routing information on the router and server. Pay attention to the following points during configuration:

- Ensure that the IP addresses of the router and server are fixed.
- An SNAT rule and a default route have been configured on the router to ensure that packets from the IPv4 subnet are sent out through interface 172.16.0.1/24 and the source IP addresses are replaced with the outbound interface address 172.16.0.1.

5. Procedure

(1) Configuring Interface IP Addresses and Adding Interfaces to Security Zones

- a Access the IP address of the firewall management port <https://192.168.1.200> and log in to the firewall web UI.
- b Choose **Network > Interface > Physical Interface**.
- c Click **Edit** in the **Operation** column of an interface. On the page that is displayed, configure an IP address and add the interface to a security zone.

 **Caution**

The IP address of an interface must be fixed.

(2) Configuring a Static NAT-PT Rule

- a Choose **Object > Address > IPv4 Address**. On the tab page that is displayed, click **Create** and create three IPv4 address objects according to the following figure.

IPv4 Address				
<input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/>				
<input type="checkbox"/>	Name	IP Address/Range	Address Group	Description
<input type="checkbox"/>	IPv4-all	0.0.0.0-255.255.255.255	-	-
<input type="checkbox"/>	IPv4net-dst	172.16.0.10	-	-
<input type="checkbox"/>	IPv4net-src	172.16.0.1	-	-

- b Click the **IPv6 Address** tab. On the tab page that is displayed, click **Create** and create an IPv6 address object according to the following figure.

IPv6 Address				
<input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/>				
<input type="checkbox"/>	Name	IP Address/Range	Address Group	Description
<input type="checkbox"/>	IPv6net-dst	3ffe:db8::10	-	-

- c Choose **Policy > NAT Policy > NAT64 Prefix**. On the page that is displayed, click **Create** and configure NAT64 prefix information according to the following figure.

< Back

Create NAT64 Prefix

* Name

* ? NAT64 Prefix

Prefix Length

- d Choose **NAT64** from the navigation pane. On the page that is displayed, click **Create** and configure a static NAT-PT rule according to the following figure. Configuration items with the asterisk (*) are mandatory.

< Back

Add IPv4-to-IPv6 NAT

Basic Info

* Name

Enabled State Enable Disable

Description

Packet Before NAT

* Src. Address

* Dest. Address

* Service

Packet After NAT

NAT Mode Stateless NAT64 Static NAT-PT Static NAT64

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

* Src. Address

Translated to

* Dest. Address

Translated to

[IP Address NAT Tool](#)

e After verifying the configuration, click **Save**.

(3) Configuring a Security Policy to Permit Traffic That Matches the NAT64 Rule

- a Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, click **Create**. Configure a security policy according to the following figure. Configuration items with the asterisk (*) are mandatory.

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

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

User/User Group

User/User Group

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Advanced

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

6. Verification

- Choose **Monitor > Traffic Monitoring > Session Monitoring > Session Statistics**. On the page that is displayed, locate the real-time session, and click **View Details** in the **Operation** column to view NAT64 session information.

Session Description ⊗

Basic Info

Session Creation Time:2023-08-16 14:33:12 Time Before Session Timeout:1Second

Src. and Dest.

Src. Address:172.16.0.1	Dest. Address:172.16.0.10
Src. Port:1	Dest. Port:1
NAT Src. Address:2ffe:db8::10	NAT Dest. Address:3ffe:db8::10
NAT Src. Port:1	NAT Dest. Port:1

More

Protocol:ICMP	App:Echo-request
Inbound Interface:Ge0/2	Outbound Interface:Ge0/3
Forward Packets:6	Forward Bytes:776
Reverse Packets:4	Reverse Bytes:320
Security Policy:permit-natpt	Session State:connection established

Disable

- Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, check the hit count of the security policy **permit-natpt** configured for the NAT64 rule. (The policy hit count is incremented only for the first packet of a connection that matches a policy.)

<input type="checkbox"/>	Priority	Name	Src. Address	User/User Group	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count
▼ Default Policy Group												
<input type="checkbox"/>	11	permit-nat...	IPv4net-src	any	any	IPv6net-dst	any	any	any	Permit		1 Clear
permit-natpt												

- Choose **Policy > NAT Policy > NAT46**. On the page that is displayed, check the hit count of the NAT64 rule. (The rule hit count is incremented only for the first packet of a connection that matches a rule.)

☐	Name	NAT Mode	Packet Before NAT			Packet After NAT				Hit Count
			Src. Address	Dest. Address	Service	NAT64 Prefix	Src. Address Translated to	Dest. Address Translated to	Dest. Port Number Translated to	
☐	IPv4net-to-IPv6net	Static NAT-PT	IPv4net-src	IPv4net-dst	any	natpt-src	2ffe:db8::10	3ffe:db8::10	-	1 Clear

8.1.6 Configuration Example of Dynamic NAT-PT Networking

1. Applicable Products and Versions

Table 8-3 Products and Versions

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R5 or later

2. Service Demands

A company HQ is upgrading an IPv4 network to an IPv6 network. To ensure the continuity of production and office services during the network upgrade, of the company, some servers that are frequently accessed cannot be migrated or upgraded in the early stage. Therefore, a NAT-PT policy needs to be configured on the firewall to ensure that departments that have been upgraded to an IPv6 network can access these IPv4 servers.

During network upgrade planning, fixed-mapped IPv6 addresses need to be assigned to these IPv4 servers to allow access from an IPv6 subnet.

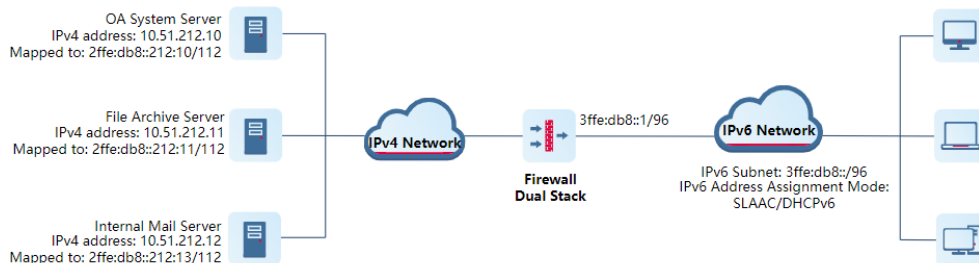


Table 8-4 Key Configuration Points in the Network Diagram

Item	Description
Firewall management port	Ge0/0, for accessing the firewall web UI and performing configurations
IP address of the firewall management port	192.168.1.200
NAT64 prefix	2ffe:db8::/96, IPv6 subnet mapped from the destination IPv4 address

Item	Description
information	
IPv6 subnet	3ffe:db8::/96
IPv6 address object 1	3ffe:db8::/96
IPv6 address object 2	2ffe:db8::212:10, mapped IPv6 address of the OA system server
IPv4 address object 1	10.51.212.10, IPv4 address of the OA system on the IPv4 network
IPv4 address pool	172.16.10.100-172.16.10.139
Port range	11001-12000
Source NAT mode	Port Address Translation (PAT), that is, reusing IP addresses
Any IPv6 address	::-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

3. Restrictions and Guidelines

- Dynamic NAT-PT does not support NAT hairpinning.
- If a dynamic NAT-PT rule needs to match any IPv6 address, you need to configure an any IPv6 address object. The default any object cannot be used, because it covers both any IPv4 address and any IPv6 address.
- If the address pool object referenced by the source NAT address pool is referenced by a NAT64 rule and the specified NAT mode is NO-PAT, the address pool object cannot be referenced by other NAT64 rules with a NAT mode of PAT.

4. Prerequisites

- (1) During network planning, you have verified that routes are available for diverting traffic from the IPv4 network to the device (firewall) where the IPv4 address pool is located.
- (2) During network planning, you have verified that routes are available for diverting traffic from the IPv6 address to the device (firewall) that performs NAT64. That is, the destination addresses are reachable from both the IPv4 and IPv6 networks.

5. Procedure

- (1) Configuring Interface IP Addresses and Adding Interfaces to Security Zones
 - a Access the IP address of the firewall management port <https://192.168.1.200> and log in to the firewall web UI.
 - b Choose **Network > Interface > Physical Interface**.
 - c Click **Edit** in the **Operation** column of an interface. On the page that is displayed, configure an IP address and add the interface to a security zone.
- (2) Configuring a Dynamic NAT-PT Rule
 - a Choose **Object > Address > IPv6 Address**. On the tab page that is displayed, click **Create** and create IPv6 address objects according to the following figure.

IPv4 Address		IPv6 Address	IPv4 Address Group	IPv6 Address Group
<div style="display: flex; gap: 10px;"> + Create 🗑️ Delete 🔄 Refresh </div>				
<input type="checkbox"/>	Name	IP Address/Range	Address Group	Description
<input type="checkbox"/>	OA-server-IPv6-mapping-a...	2ffe:db8::212:10	-	-
<input type="checkbox"/>	IPv6-subnet-1	3ffe:db8::/96	-	-

- b Choose **Object > Address > IPv4 Address**. On the tab page that is displayed, click **Create** and create an IPv4 address object according to the following figure.

IPv4 Address		IPv6 Address	IPv4 Address Group	IPv6 Address Group
<div style="display: flex; gap: 10px;"> + Create 🗑️ Delete 🔄 Refresh </div>				
<input type="checkbox"/>	Name	IP Address/Range	Address Group	Description
<input type="checkbox"/>	OA-server-IPv4-address	10.51.212.10	-	-

- c Choose **Policy > NAT Policy > NAT64 Prefix**. On the page that is displayed, click **Create** and configure NAT64 prefix information according to the following figure.

[< Back](#)

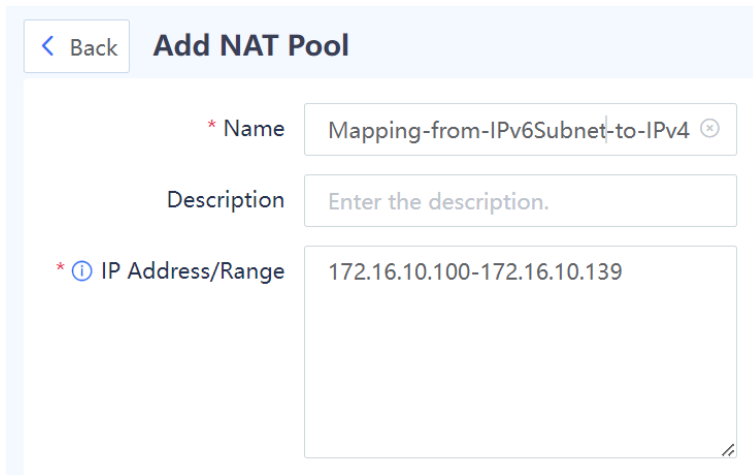
Create NAT64 Prefix

* Name

* ⓘ NAT64 Prefix

Prefix Length

- d Choose **Address Pool** from the navigation pane. On the page that is displayed, click **Create** and configure a NAT pool for the IPv6 subnet.



[< Back](#) **Add NAT Pool**

* Name

Description

* ⓘ IP Address/Range

- e Choose **NAT64** from the navigation pane. On the page that is displayed, click **Create** and configure a dynamic NAT-PT rule according to the following figure. Configuration items with the asterisk (*) are mandatory.

< Back

Add IPv6-to-IPv4 NAT

Basic Info

* Name

Enabled State Enable Disable

Description

Packet Before NAT

* Src. Address

* Dest. Address

* Service

Packet After NAT

NAT Mode Dynamic NAT-PT Dynamic NAT64

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

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

Address to Address
in Address Pool

SNAT Mode NO-PAT PAT

* **Port Number**
Range

* **Dest. Address**
Translated to

f After verifying the configuration, click **Save**.

(3) Configuring a Security Policy to Permit Traffic That Matches the NAT64 Rule

- a Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, click **Create**. Configure a security policy according to the following figure. Configuration items with the asterisk (*) are mandatory.

< Back

Create Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Advanced

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

6. Verification

- Choose **Monitor > Traffic Monitoring > Session Monitoring > Session Statistics**. On the page that is displayed, locate the real-time session, and click **View Details** in the **Operation** column to view NAT64 session information.

Session Description



Basic Info

Session Creation Time:2023-09-07 13:20:55 Time Before Session Timeout:47Second

Src. and Dest.

Src. Address:172.17.96.1	Dest. Address:10.51.212.100
Src. Port:6	Dest. Port:6
NAT Src. Address:2ffe:db8::ac11:6001	NAT Dest. Address:3ffe:db8::da64
NAT Src. Port:6	NAT Dest. Port:6

More

Protocol:ICMP	App:Echo-request
Inbound Interface:Ge0/2	Outbound Interface:Ge0/3
Forward Packets:5	Forward Bytes:500
Reverse Packets:5	Reverse Bytes:400
Security Policy:permit-access-IPv6Sever	Session State:connection established

Disable

- Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, check the hit count of the security policy **permit-IPv6net-Access-OAserver** configured for the NAT64 rule. (The policy hit count is incremented only for the first packet of a connection that matches a policy.)

Priority	Name	Address	User/User Group	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count	Hit Session	Operation
5	permit-IPv6net-Access-OAserver	any	any	any	OA-server-IP...	any	any	any	Permit		5	Clear	View Details... Edit Delete

- Choose **Policy > NAT Policy > NAT64**. On the page that is displayed, check the hit count of the NAT64 rule. (The rule hit count is incremented only for the first packet of a connection that matches a rule.)

Name	NAT Mode	Packet Before NAT			Packet After NAT					Hit Count	Description	Operation
		Src. Address	Dest. Address	Service	NAT64 Prefix	SNAT Pool	SNAT Mode	Port Range	Dest. Address Translated to			
IPv6Subnet...	Dynamic NAT-PT	IPv6-subne...	OA-server-IP...	any	Mapping-from-IPv4-to-IPv6	Mapping-from-IPv6Subnet-to-IPv4	pat	11001-12000	10.51.212.10	1	Clear	Edit

8.1.7 Configuration Example of Stateless NAT64 Networking

1. Applicable Products and Versions

Table 8-5 Products and Versions

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R5 or later

2. Service Demands

In a NAT64 networking scenario, NAT-PT policies are typically deployed on the edge devices of IPv4 and IPv6 networks to translate addresses in mutual access packets between the IPv4 and IPv6 networks.

A company is upgrading an IPv4 network to an IPv6 network. Hosts on the IPv4 network need to access the public server, and hosts on the IPv4 and IPv6 networks can access each other.

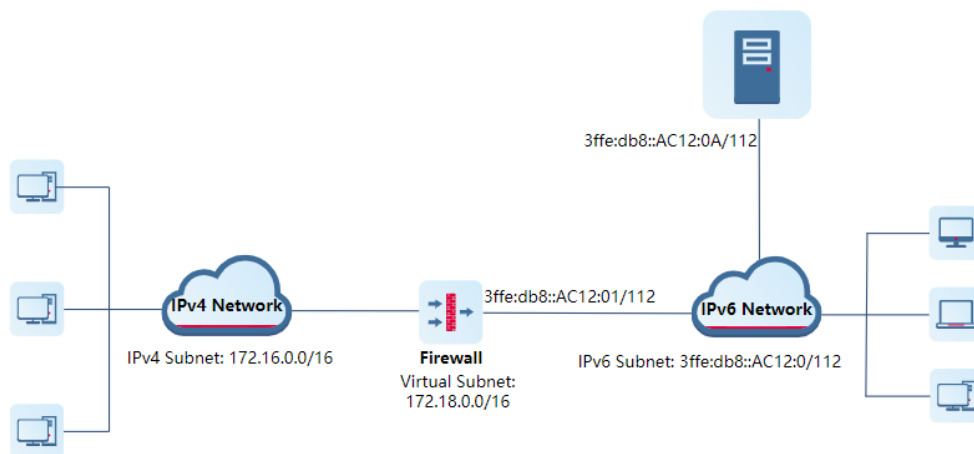


Table 8-6 Key Configuration Points in the Network Diagram

Item	Description
Firewall management port	Ge0/0, for accessing the firewall web UI and performing configurations
IP address of the firewall management port	192.168.1.200
NAT64 prefix information	3ffe:db8::/96
Virtual subnet	172.18.0.0/16, virtual subnet address mapped from an IPv6 address when a host on the IPv4 network accesses the IPv6 network

Item	Description
IPv6 subnet	3ffe:db8::AC12:0:0/112, for planning IPv6 addresses obtained by devices on an IPv6 network. The number of addresses it contains is equal to that of the virtual subnet, and the IPv4 subnet represented by the last 32 bits is the same as the virtual subnet.
IPv4 address object 1	172.16.0.0/16
IPv4 address object 2	172.18.0.0/16
IPv6 address object 1	3ffe:db8::AC12:0/112
Any IPv4 address	0.0.0.0-255.255.255.255

3. Restrictions and Guidelines


- Stateless NAT64 does not support NAT hairpinning.
- If a stateless NAT64 rule needs to match any IPv4 address, you need to configure an any IPv4 address object. The default any object cannot be used, because it covers both any IPv4 address and any IPv6 address.

4. Procedure

(1) Configuring Interface IP Addresses and Adding Interfaces to Security Zones




- Access the IP address of the firewall management port <https://192.168.1.200> and log in to the firewall web UI.
- Choose **Network > Interface > Physical Interface**.
Click **Edit** in the **Operation** column of an interface. On the page that is displayed, configure an IP address and add the interface to a security zone.

(2) Configuring a Stateless NAT64 Rule




 Caution

The address of the virtual subnet 172.18.0.0/16 does not exist on a physical network device interface.

- Choose **Object > Address > IPv4 Address**. On the tab page that is displayed, click **Create** and create IPv4 address objects according to the following figure.

IPv4 Address			
	IPv6 Address	IPv4 Address Group	IPv6 Address Group
 Create	 Delete	 Refresh	
<input type="checkbox"/> Name	IP Address/Range	Address Group	Description
<input type="checkbox"/> IPv4-all	0.0.0.0-255.255.255.255	-	-
<input type="checkbox"/> IPv4net-dst	172.18.0.0/16	-	-
<input type="checkbox"/> IPv4net-src	172.16.0.0/16	-	-

- b Click the **IPv6 Address** tab. On the tab page that is displayed, click **Create** and create an IPv6 address object according to the following figure.


IPv4 Address		IPv6 Address	IPv4 Address Group	IPv6 Address Group
 Create	 Delete	 Refresh		
<input type="checkbox"/>	Name	IP Address/Range	Address Group	Description
<input type="checkbox"/>	IPv6net-dst	3ffe:db8::ac12:0:0/112	-	-

- c Choose **Policy > NAT Policy > NAT64 Prefix**. On the page that is displayed, click **Create** and configure NAT64 prefix information according to the following figure.

< Back

Create NAT64 Prefix

* Name

*  NAT64 Prefix

Prefix Length v

- d Choose **NAT64** from the navigation pane. On the page that is displayed, click **Create** and configure a stateless NAT64 rule according to the following figure. Configuration items with the asterisk (*) are mandatory.

< Back

Add IPv4-to-IPv6 NAT

Basic Info

* Name

Enabled State Enable Disable

Description

Packet Before NAT

* Src. Address

* Dest. Address

* Service

Packet After NAT

NAT Mode
 Stateless NAT64
 Static NAT-PT
 Static NAT64

* NAT64 Prefix [Create NAT64 Prefix](#)

[IP Address NAT Tool](#)

(3) Configuring a Security Policy to Permit Traffic That Matches the NAT64 Rule

- a Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, click **Create**. Configure a security policy according to the following figure. Configuration items with the asterisk (*) are mandatory.

Configure security policy 1 to permit packets from the IPv4 network to IPv6 network. Configure the source and destination addresses to reference address objects **IPv4net-src** and **IPv6net-dst**, respectively. Set the action to **Permit**.

< Back

Create Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Advanced

Configure security policy 2 to permit packets from the IPv6 network to IPv4 network. Configure the source and destination addresses to reference address objects **IPv6net-dst** and **IPv4net-src**, respectively. Set the action to **Permit**.

< Back

Create Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Advanced

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

5. Verification

- Choose **Monitor > Traffic Monitoring > Session Monitoring > Session Statistics**. On the page that is displayed, locate the real-time session, and click **View Details** in the **Operation** column to view NAT64 session information.

Session Description ⊗

Basic Info

Session Creation Time:2023-09-07 13:20:55 Time Before Session Timeout:47Second

Src. and Dest.

Src. Address:172.17.96.1	Dest. Address:10.51.212.100
Src. Port:6	Dest. Port:6
NAT Src. Address:2ffe:db8::ac11:6001	NAT Dest. Address:3ffe:db8::da64
NAT Src. Port:6	NAT Dest. Port:6

More

Protocol:ICMP	App:Echo-request
Inbound Interface:Ge0/2	Outbound Interface:Ge0/3
Forward Packets:5	Forward Bytes:500
Reverse Packets:5	Reverse Bytes:400
Security Policy:permit-access-IPv6Sever	Session State:connection established

Disable

- Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, check the hit count of the security policy **permit-IPv6-to-IPv4** configured for the NAT64 rule. (The policy hit count is incremented only for the first packet of a connection that matches a policy.)

Priority	Name	Src	User/User Group	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count	Hit Session	Operation
6	permit-IPv...	!-src		any	IPv6net-dst	any	any	any	Permit		6	Clear	View Details... Edit Delete

- Choose **Policy > NAT Policy > NAT46**. On the page that is displayed, check the hit count of the NAT64 rule. (The rule hit count is incremented only for the first packet of a connection that matches a rule.)

Name	NAT Mode	Packet Before NAT				Packet After NAT			Hit Count	Description	Operation
		Src. Address	Dest. Address	Service	NAT64 Prefix	Src. Address Translated to	Dest. Address Translated to	Dest. Port Number Translated to			
nat64-stl	Stateless NAT64	IPv4net-src	IPv4net-dst	any	nat64stl-src	-	-	-	4	Clear	Edit Delete

8.1.8 Configuration Example of Static NAT64 Networking

1. Applicable Products and Versions

Table 8-7 Products and Versions

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R5 or later

2. Service Demands

A company HQ is upgrading an IPv4 network to an IPv6 network. A server at the HQ has been upgraded to the IPv6 network, and branches in other cities need to access this server (using a domain name). Therefore, during network planning, this server needs to be mapped to an address on the IPv4 network.

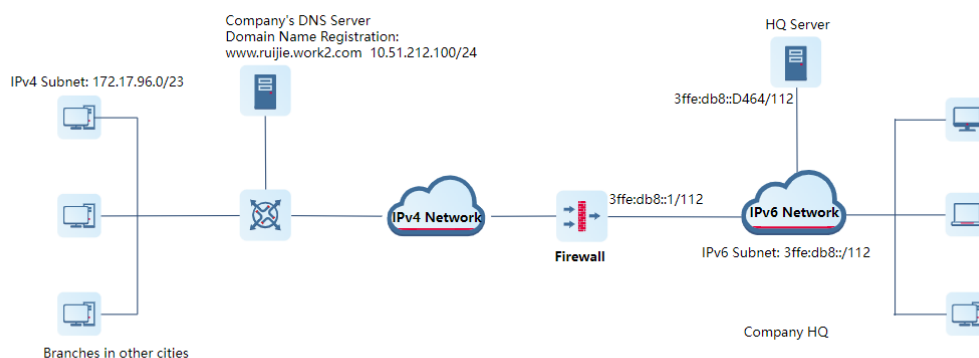


Table 8-8 Key Configuration Points in the Network Diagram

Item	Description
Firewall management port	Ge0/0, for accessing the firewall web UI and performing configurations
IP address of the firewall management port	192.168.1.200
NAT64 prefix information	2ffe:db8::/96
IPv6 subnet	3ffe:db8:: /112, for planning IPv6 addresses obtained by devices on an IPv6 network. The number of addresses it contains is equal to that of the virtual subnet, and the IPv4 subnet represented by the last 32 bits is the same as the virtual subnet.
IPv4 address object 1	172.17.96.0/23
IPv4 address object 2	10.51.212.100

Item	Description
IPv6 address object 1	3ffe:db8::D464
Any IPv4 address	0.0.0.0-255.255.255.255

3. Restrictions and Guidelines

- Static NAT64 does not support NAT hairpinning.
- If a static NAT64 rule needs to match any IPv4 address, you need to configure an any IPv4 address object. The default any object cannot be used, because it covers both any IPv4 address and any IPv6 address.

4. Prerequisites

You have registered the HQ server domain name **www.ruijie.work2.com** to be accessed by the IPv4 network on the company's DNS64 server. Traffic can be diverted to the edge firewall of the HQ based on the resolved address.

5. Procedure

(1) Configuring Interface IP Addresses and Adding Interfaces to Security Zones

- Access the IP address of the firewall management port <https://192.168.1.200> and log in to the firewall web UI.
- Choose **Network > Interface > Physical Interface**.
Click **Edit** in the **Operation** column of an interface. On the page that is displayed, configure an IP address and add the interface to a security zone.

(2) Configuring a Static NAT64 Rule

- Choose **Object > Address > IPv4 Address**. On the tab page that is displayed, click **Create** and create IPv4 address objects according to the following figure.

IPv4 Address				
	IPv6 Address	IPv4 Address Group	IPv6 Address Group	
<input type="checkbox"/>	Name	IP Address/Range	Address Group	Description
<input type="checkbox"/>	IPv4-all	0.0.0.0-255.255.255.255	-	-
<input type="checkbox"/>	IPv4net-dst	10.51.212.100	-	-
<input type="checkbox"/>	IPv4net-src	172.17.96.0/23	-	-

- Click the **IPv6 Address** tab. On the tab page that is displayed, click **Create** and create an IPv6 address object according to the following figure.

IPv4 Address		IPv6 Address	IPv4 Address Group	IPv6 Address Group
<input type="button" value="Create"/>	<input type="button" value="Delete"/>	<input type="button" value="Refresh"/>		
<input type="checkbox"/>	Name	IP Address/Range	Address Group	Description
<input type="checkbox"/>	IPv6-webServer	3ffe:db8::d464	-	-

- c Choose **Policy > NAT Policy > NAT64 Prefix**. On the page that is displayed, click **Create** and configure NAT64 prefix information according to the following figure.

Create NAT64 Prefix

* Name

* NAT64 Prefix

Prefix Length

- d Choose **NAT64** from the navigation pane. On the page that is displayed, click **Create** and configure a static NAT64 rule according to the following figure. Configuration items with the asterisk (*) are mandatory.

< Back

Add IPv4-to-IPv6 NAT

Basic Info

* Name

Enabled State Enable Disable

Description

Packet Before NAT

* Src. Address

* Dest. Address

* Service

Packet After NAT

NAT Mode Stateless NAT64 Static NAT-PT Static NAT64

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

* Dest. Address

Translated to

Dest. Port Number

Translated to

[IP Address NAT Tool](#)

e After verifying the configuration, click **Save**.

(3) Configuring a Security Policy to Permit Traffic That Matches the NAT64 Rule

- a Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, click **Create**. Configure a security policy according to the following figure. Configuration items with the asterisk (*) are mandatory.

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

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [Add Group](#)

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Advanced

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

6. Verification

- Choose **Monitor > Traffic Monitoring > Session Monitoring > Session Statistics**. On the page that is displayed, locate the real-time session, and click **View Details** in the **Operation** column to view NAT64 session information.

Session Description ⊗

Basic Info

Session Creation Time:2023-09-07 13:20:55 Time Before Session Timeout:47Second

Src. and Dest.

Src. Address:172.17.96.1	Dest. Address:10.51.212.100
Src. Port:6	Dest. Port:6
NAT Src. Address:2ffe:db8::ac11:6001	NAT Dest. Address:3ffe:db8::da64
NAT Src. Port:6	NAT Dest. Port:6

More

Protocol:ICMP	App:Echo-request
Inbound Interface:Ge0/2	Outbound Interface:Ge0/3
Forward Packets:5	Forward Bytes:500
Reverse Packets:5	Reverse Bytes:400
Security Policy:permit-access-IPv6Server	Session State:connection established

Disable

- Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, check the hit count of the security policy **permit-access-IPv6Server** configured for the NAT64 rule. (The policy hit count is incremented only for the first packet of a connection that matches a policy.)

<input type="checkbox"/>	Priority	Name	Src. Address	User/User Group	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count	Operation
Default Policy Group													
<input type="checkbox"/>	7	permit-acc...	IPv4net-src	any	any	IPv6-webSer...	any	any	any	Permit		7 Clear	🟢 Edit Delete

- Choose **Policy > NAT Policy > NAT46**. On the page that is displayed, check the hit count of the NAT64 rule. (The rule hit count is incremented only for the first packet of a connection that matches a rule.)

<input type="checkbox"/>	Name	NAT Mode	Packet Before NAT				Packet After NAT			Hit Count	Description	Operation
			Src. Address	Dest. Address	Service	NAT64 Prefix	Src. Address Translated to	Dest. Address Translated to	Dest. Port Number Translated to			
<input type="checkbox"/>	IPv4net-access-IP...	Static NAT64	IPv4net-src	IPv4net-dst	any	natpt-src	-	3ffe:db8:d464	-	4 Clear		🟢 Edit Delete

8.1.9 Configuration Example of Dynamic NAT64 Networking

1. Applicable Products and Versions

Table 8-9 Products and Versions

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R5 or later

2. Service Demands

A company HQ is upgrading an IPv4 network to an IPv6 network. To ensure the continuity of production and office services during the network upgrade, of the company, some servers that are frequently accessed cannot be migrated or upgraded in the early stage. Therefore, a NAT-PT policy needs to be configured on the firewall to ensure that departments that have been upgraded to an IPv6 network can access these IPv4 servers.

During network upgrade planning, fixed-mapped IPv6 addresses can be assigned to these IPv4 servers to allow access from an IPv6 subnet. However, fixed mappings make network maintenance difficult if device addresses on the network change. If fixed mappings exist on the firewall, a series of firewall rules need to be modified upon device address changes, posing potential security risks. In addition, the customer requests that domain names be used to access the servers.

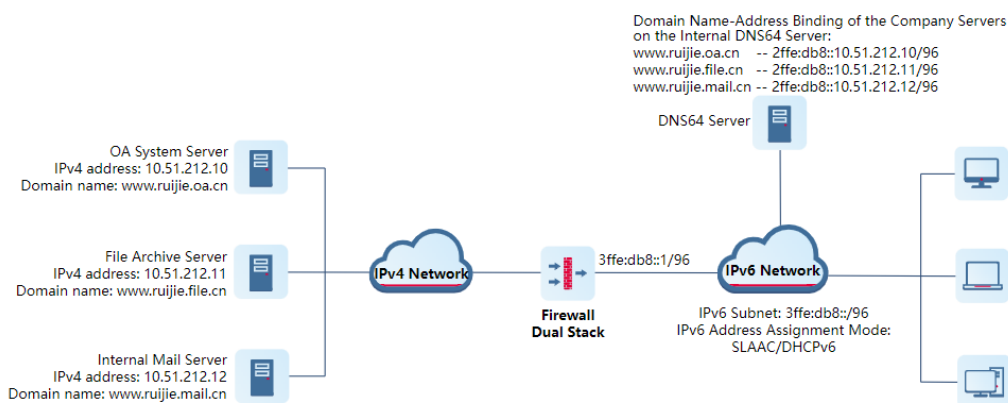


Table 8-10 Key Configuration Points in the Network Diagram

Item	Description
Firewall management port	Ge0/0, for accessing the firewall web UI and performing configurations
IP address of the firewall management port	192.168.1.200
NAT64 prefix information	2ffe:db8::/96, IPv6 address public prefix information that all IPv4

Item	Description
	servers register with the DNS64 server
IPv6 subnet	3ffe:db8::/96
IPv6 address object 1	3ffe:db8::/96
IPv6 address object 2	2ffe:db8::/96
IPv4 address object 1	10.51.212.10-10.51.212.12
IPv4 address pool	172.16.10.100-172.16.10.139
Port range	11001-12000
Source NAT mode	PAT, that is, reusing IP addresses
Any IPv6 address	::-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

3. Restrictions and Guidelines

- Dynamic NAT64 does not support NAT hairpinning.
- If a NAT64 rule needs to match any IPv6 address, you need to configure an any IPv6 address object. The default any object cannot be used, because it covers both any IPv4 address and any IPv6 address.
- If the address pool object referenced by the source NAT address pool is referenced by a NAT64 rule and the specified NAT mode is NO-PAT, the address pool object cannot be referenced by other NAT64 rules with a NAT mode of PAT.

4. Prerequisites

- (1) Destination addresses are reachable from both the IPv4 and IPv6 networks.
- (2) IPv6 hosts can access the DNS64 server without passing through the firewall. (In the preceding network diagram, the DNS64 server is deployed on the right of the firewall.)
- (3) You have correctly configured domain name-address binding information for the IPv4 servers on the DNS64 server.

5. Procedure

- (1) Configuring Interface IP Addresses and Adding Interfaces to Security Zones
 - a Access the IP address of the firewall management port <https://192.168.1.200> and log in to the firewall web UI.
 - b Choose **Network > Interface > Physical Interface**.
Click **Edit** in the **Operation** column of an interface. On the page that is displayed, configure an IP address and add the interface to a security zone.
- (2) Configuring a Dynamic NAT64 Rule
 - a Choose **Object > Address > IPv6 Address**. On the tab page that is displayed, click **Create** and create IPv6 address objects according to the following figure.

IPv4 Address		IPv6 Address	IPv4 Address Group	IPv6 Address Group
<input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/>				
<input type="checkbox"/>	Name	IP Address/Range	Address Group	Description
<input type="checkbox"/>	DNS64-public-IPv6-prefix	2ffe:db8::/96	-	-
<input type="checkbox"/>	IPv6-subnet-1	3ffe:db8::/96	-	-

- b Click the **IPv4 Address** tab. On the tab page that is displayed, click **Create** and create an IPv4 address object according to the following figure.

IPv4 Address		IPv6 Address	IPv4 Address Group	IPv6 Address Group
<input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/>				
<input type="checkbox"/>	Name	IP Address/Range	Address Group	Description
<input type="checkbox"/>	IPv4Server	10.51.212.10-10.51.212.12	-	-

- c Choose **Policy > NAT Policy > NAT64 Prefix**. On the page that is displayed, click **Create** and configure NAT64 prefix information according to the following figure.

< Back

Create NAT64 Prefix

* Name

* ⓘ NAT64 Prefix

Prefix Length

- d Choose **Address Pool** from the navigation pane. On the page that is displayed, click **Create** and configure a NAT pool for the IPv6 subnet.

< Back

Edit NAT Pool

* Name

Description

* ⓘ IP Address/Range

- e Choose **NAT64** from the navigation pane. On the page that is displayed, click **Create** and configure a dynamic NAT64 rule according to the following figure. Configuration items with the asterisk (*) are mandatory.

< Back

Add IPv6-to-IPv4 NAT

Basic Info

* Name

Enabled State Enable Disable

Description

Packet Before NAT

* Src. Address

* Dest. Address

* Service

Packet After NAT

NAT Mode Dynamic NAT-PT Dynamic NAT64

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

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

Address to Address
in Address Pool

SNAT Mode NO-PAT PAT

* Port Number [+](#)

Range

f After verifying the configuration, click **Save**.

(3) Configuring a Security Policy to Permit Traffic That Matches the NAT64 Rule

- a Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, click **Create**. Configure a security policy according to the following figure. Configuration items with the asterisk (*) are mandatory.

< Back

Create Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [+ Add Group](#)

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Advanced

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

6. Verification

- Choose **Monitor > Traffic Monitoring > Session Monitoring > Session Statistics**. On the page that is displayed, locate the real-time session, and click **View Details** in the **Operation** column to view NAT64 session information.

Session Description ⊗

Basic Info

Session Creation Time:2023-09-07 14:55:09 Time Before Session Timeout:45Second

Src. and Dest.

Src. Address:3ffe:db8::ac12:a	Dest. Address:2ffe:db8::a33:d40a
Src. Port:9121	Dest. Port:9121
NAT Src. Address:172.16.10.100	NAT Dest. Address:10.51.212.10
NAT Src. Port:11005	NAT Dest. Port:11005

More

Protocol:IP	App:Echo-RequestV6
Inbound Interface:Ge0/3	Outbound Interface:Ge0/2
Forward Packets:5	Forward Bytes:300
Reverse Packets:5	Reverse Bytes:400
Security Policy:permit-IPv6net-access-IPv4Server	Session State:connection established

Disable

- Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, check the hit count of the security policy **permit-IPv6net-access-IPv4Server** configured for the NAT64 rule. (The policy hit count is incremented only for the first packet of a connection that matches a policy.)

Priority	Name	Src. Address	User/User Group	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count	Hit	Operation
Default Policy Group													
8	permit-IPv6net-access-IPv4Server	IPv6-subnet-1	any	any	IPv4Server	any	any	any	Permit		4	Clear	View Edit Delete

- Choose **Policy > NAT Policy > NAT64**. On the page that is displayed, check the hit count of the NAT64 rule. (The rule hit count is incremented only for the first packet of a connection that matches a rule.)

Name	NAT Mode	Packet Before NAT			Packet After NAT					Hit Count	
		Src. Address	Dest. Address	Service	NAT64 Prefix	SNAT Pool	SNAT Mode	Port Range	Dest. Address Translated to		
permit-IPv6net-access-IPv4Server											
permit-IPv6net-access-IPv4Server	Dynamic NAT64	IPv6-subnet-1	DNS64-public-IPv6-prefix	any	DNS64-IPv6-prefix	Mapping-from-IPv6Subnet-to-IPv4	pat	11001-12000	-	4	Clear

8.1.10 Configuration Example of NAT66-Source NPTv6 Networking

1. Applicable Products and Versions

Table 8-11 Products and Versions

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R5 or later

2. Service Demands

A company has deployed a firewall as a security gateway at the network boundary. A source NAT policy needs to be configured on the firewall to allow intranet users to access the Internet without exposing intranet IP addresses to extranets. In this way, network security of internal users can be enhanced.

The following figure shows the network diagram, in which the router is the access gateway provided by the ISP.

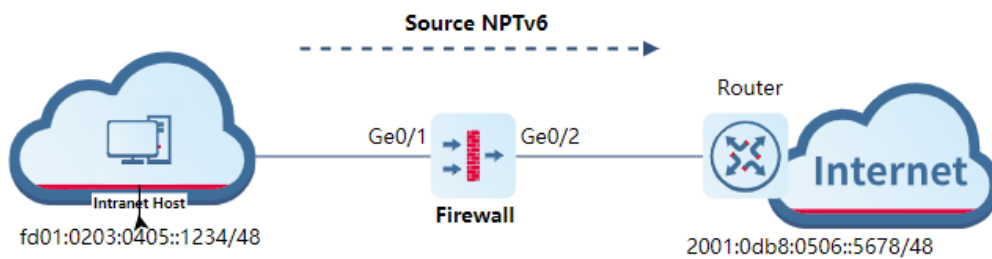


Table 8-12 Key Configuration Points in the Network Diagram

Item	Description
Firewall management port	Ge0/0, for accessing the firewall web UI and performing configurations
IP address of the firewall management port	192.168.1.200
IPv6 address object 1	fd01:0203:0405::/48, IPv6 prefix before source NAT
NPT information	2001:0db8:0001::/48, IPv6 prefix after source NPT
IPv6 address of Ge0/1	FD01:0203:0405::5678/48, trust zone
IPv6 address of Ge0/2	2001:0DB8:0506::1234/48, untrust zone
Any IPv6 address	::FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

3. Restrictions and Guidelines

- The prefix lengths before and after NPT must be the same. For example, in a source NPTv6 rule, the IPv6 subnet prefix length in the matched source address object must be the same as the prefix length in the prefix information after NPT.
- If a NAT66 rule needs to match any IPv6 address, you need to configure an any IPv6 address object. The default any object cannot be used, because it covers both any IPv4 address and any IPv6 address.
- It is recommended that the IPv6 prefix information (IPv6 prefix and prefix length) after source NAT be different from the outbound interface IPv6 prefix information used by the NAT66 device for performing NAT66. For example, if the prefix after source NAT is 2001::/48, the IPv6 prefix of the outbound interface can be 2001::10/48.

4. Prerequisites

Destination addresses before and after destination NAT are reachable. Routing and related configurations have been completed in the early stage of network planning.

5. Procedure

(1) Configuring Interface IP Addresses and Adding Interfaces to Security Zones

- Access the IP address of the firewall management port <https://192.168.1.200> and log in to the firewall web UI.
- Choose **Network > Interface > Physical Interface**.
Click **Edit** in the **Operation** column of an interface. On the page that is displayed, configure an IP address and add the interface to a security zone.

(2) Configuring a NAT66-Source NPTv6 Rule

- Choose **Object > Address > IPv6 Address**. On the tab page that is displayed, click **Create** and create IPv6 address objects according to the following figure.

<input type="checkbox"/>	Name	IP Address/Range
<input type="checkbox"/>	src-before-NATv6	fd01:203:405::/48
<input type="checkbox"/>	IPv6-all	::ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

- Choose **Policy > NAT Policy > NAT66**. On the page that is displayed, click **Create** and configure a NAT66 rule according to the following figure. Set **NAT Mode** to **Source NPTv6**. Configuration items with the asterisk (*) are mandatory.

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

NAT Mode

NAT Mode Source NPTv6 Destination NPTv6

Basic Info

* Name

Enabled State Enable Disable

Description

Packet Before NAT

* Src. Address

* Dest. Address

* Service

Packet After NAT

* NPT Info

[Save](#)

- c After verifying the configuration, click **Save**.
- (3) Configuring a Security Policy to Permit Traffic That Matches the NAT66 Rule
- a Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, click **Create**. Configure a security policy according to the following figure. Configuration items with the asterisk (*) are mandatory.

< Back

Create Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Advanced

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

6. Verification

- Choose **Monitor > Traffic Monitoring > Session Monitoring > Session Statistics**. On the page that is displayed, locate the real-time session, and click **View Details** in the **Operation** column to view NAT66 session information.

Session Description ⊗

Basic Info

Session Creation Time:2023-09-07 17:55:08 Time Before Session Timeout:41Second

Src. and Dest.

Src. Address:fd01:203:405::1234 Dest. Address:2001:db8:506::5678

Src. Port:2235 Dest. Port:2235

NAT Src. Address:2001:db8:1::1234 NAT Dest. Address:-

NAT Src. Port:2235 NAT Dest. Port:-

More

Protocol:IP App:Echo-RequestV6

Inbound Interface:Ge0/2 Outbound Interface:Ge0/3

Forward Packets:5 Forward Bytes:300

Reverse Packets:5 Reverse Bytes:300

Security Policy:permit-src-before-NPTv6 Session State:connection established

Disable

- Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, check the hit count of the security policy **permit-src-before-NPTv6** configured for the NAT66 rule. (The policy hit count is incremented only for the first packet of a connection that matches a policy.)

<input type="checkbox"/>	Priority	Name	Src. Address	User/User Group	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count
▼ Default Policy Group												
<input type="checkbox"/>	9	permit-src...	src-before-...	any	any	IPv6-all	any	any	any	Permit		1 Clear
			permit-src-before-NPTv6									

- Choose **Policy > NAT Policy > NAT66**. On the page that is displayed, check the hit count of the NAT66 rule. (The rule hit count is incremented only for the first packet of a connection that matches a rule.)

<input type="checkbox"/>	Name	NAT Mode	Packet Before NAT			Packet After NAT	Hit Count	Status
			Src. Address	Dest. Address	Service	NPT Info		
<input type="checkbox"/>	src-fd01-NPTv6	Source NPTv6	src-before-NATv6	IPv6-all	any	2001:db8:1:/48	1 Clear	Normal

8.1.11 Configuration Example of NAT66-Destination NPTv6 Networking

1. Applicable Products and Versions

Table 8-13 Products and Versions

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R5 or later

2. Service Demands

A company has deployed a firewall as a security gateway at the network boundary. To enable the intranet web server to provide services to extranets, a destination NAT policy needs to be configured on the firewall to provide the IP address of the web server for public network users to access. The following figure shows the network diagram, in which the router is the access gateway provided by the ISP.

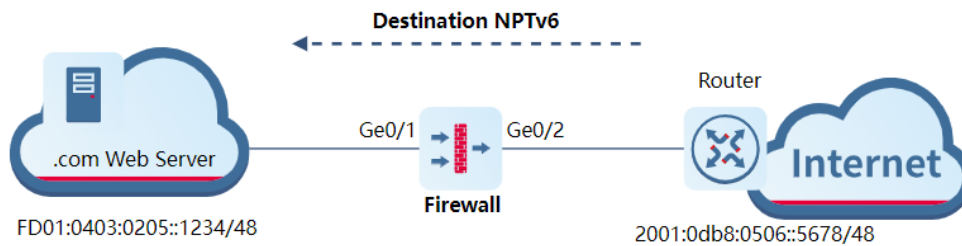


Table 8-14 Key Configuration Points in the Network Diagram

Item	Description
Firewall management port	Ge0/0, for accessing the firewall web UI and performing configurations
IP address of the firewall management port	192.168.1.200
IPv6 address object 1	2001:0DB8:0102::/48, IPv6 prefix before source NAT
NPT information	FD01:0403:0205::/48, IPv6 prefix after destination NPT
IPv6 address of Ge0/1	FD01:0403:0205::5678/48, trust zone
IPv6 address of Ge0/2	2001:0DB8:0506::1234/48, untrust zone
Any IPv6 address	::FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

3. Restrictions and Guidelines

- The prefix lengths before and after NPT must be the same. For example, in a source NPTv6 rule, the IPv6 subnet prefix length in the matched source address object must be the same as the prefix length in the prefix information after NPT.
- If a NAT66 rule needs to match any IPv6 address, you need to configure an any IPv6 address object. The default any object cannot be used, because it covers both any IPv4 address and any IPv6 address.
- The destination address after destination NPT must be the address of a physical device interface on the network.

4. Prerequisites

Destination addresses before and after destination NAT are reachable. Routing and related configurations have been completed in the early stage of network planning.

5. Procedure

(1) Configuring Interface IP Addresses and Adding Interfaces to Security Zones

- Access the IP address of the firewall management port `https://192.168.1.200` and log in to the firewall web UI.
- Choose **Network > Interface > Physical Interface**.
Click **Edit** in the **Operation** column of an interface. On the page that is displayed, configure an IP address and add the interface to a security zone.

(2) Configuring a NAT66-Destination NPTv6 Rule

- Choose **Object > Address > IPv6 Address**. On the tab page that is displayed, click **Create** and create IPv6 address objects according to the following figure.

<input type="checkbox"/>	Name	IP Address/Range
<input type="checkbox"/>	dst-prefix-after-NPTv6	fd01:403:205::/48
<input type="checkbox"/>	dst-prefix-before-NPTv6	2001:db8:102::/48
<input type="checkbox"/>	IPv6-all	::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

- Choose **Policy > NAT Policy > NAT66**. On the page that is displayed, click **Create** and configure a NAT66 rule according to the following figure. Set **NAT Mode** to **Destination NPTv6**. Configuration items with the asterisk (*) are mandatory.

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

NAT Mode

NAT Mode Source NPTv6 Destination NPTv6

Basic Info

* Name

Enabled State Enable Disable

Description

Packet Before NAT

* Src. Address

* Dest. Address

* Service

Packet After NAT

* [?](#) NPT Info

- c After verifying the configuration, click **Save**.
- (3) Configuring a Security Policy to Permit Traffic That Matches the NAT66 Rule
- a Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, click **Create**. Configure a security policy according to the following figure. Configuration items with the asterisk (*) are mandatory.

< Back

Create Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [+ Add Group](#)

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Advanced

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

6. Verification

- Choose **Monitor > Traffic Monitoring > Session Monitoring > Session Statistics**. On the page that is displayed, locate the real-time session, and click **View Details** in the **Operation** column to view NAT66 session information.

Session Description ⊗

Basic Info

Session Creation Time:2023-09-07 15:55:08 Time Before Session Timeout:47Second

Src. and Dest.

Src. Address:2001:db8:506::5678 Dest. Address:2001:db8:102::1234

Src. Port:1424 Dest. Port:1424

NAT Src. Address:- NAT Dest. Address:fd01:403:205::1234

NAT Src. Port:- NAT Dest. Port:1424

More

Protocol:IP App:Echo-RequestV6

Inbound Interface:Ge0/3 Outbound Interface:Ge0/2

Forward Packets:5 Forward Bytes:300

Reverse Packets:5 Reverse Bytes:300

Security Policy:permit-IPv6-access-WebServer Session State:connection established

Disable

- Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, check the hit count of the security policy **permit-IPv6-access-WebServer** configured for the NAT66 rule. (The policy hit count is incremented only for the first packet of a connection that matches a policy.)

<input type="checkbox"/>	Priority	Name	Src. Address	User/User Group	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count
▼ Default Policy Group												
<input type="checkbox"/>	10	permit-IPv6...	IPv6-all	any	any	dst-prefix-aft...	any	any	any	Permit <input checked="" type="checkbox"/>		8 Clear
			permit-IPv6-access-WebServer									

- Choose **Policy > NAT Policy > NAT66**. On the page that is displayed, check the hit count of the NAT66 rule. (The rule hit count is incremented only for the first packet of a connection that matches a rule.)

<input type="checkbox"/>	Name	NAT Mode	Packet Before NAT			Packet After NAT	Hit Count	Status
			Src. Address	Dest. Address	Service	NPT Info		
<input type="checkbox"/>	dst-NPTv6-access-WebServer	Destination NPTv6	IPv6-all	dst-prefix-before-NPTv6	any	fd01:403:205::/48	8 Clear	Normal

8.2 Port Mapping Policy

8.2.1 Overview

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

8.2.2 Configuring a Port Mapping Policy

Application Scenario

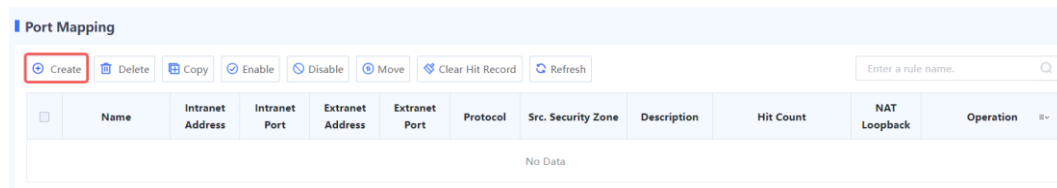
Typically, port mapping is used for extranet users to access intranet servers, for intranet users to access intranet servers using extranet IP addresses, and for mutual access between two intranets.

Precautions

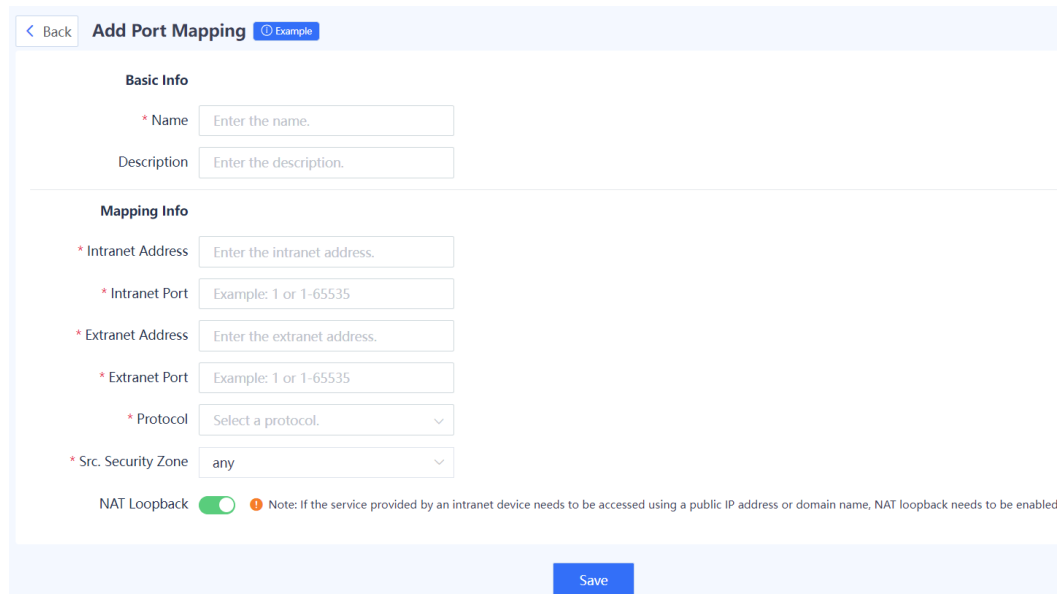
A port mapping policy takes precedence over a NAT policy. That is, if traffic matches a port mapping policy, NAT policies will not be matched.

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		
Intranet Address	Intranet 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
Intranet Port	Intranet 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 intranet ports must be the same as that of the configured extranet ports. [Example] 80 or 2-80
Extranet Address	Extranet IP address used to receive requests from an extranet.	[Example] 200.10.10.10
Extranet Port	Extranet port number used to receive requests from an extranet.	Enter a single port number or port number range. The number of configured extranet ports must be the same as that of the configured intranet 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.	[Example] any
NAT Loopback	If intranet users need to access intranet services using extranet 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.

Tip



To enable the device to perform mapping properly, the system automatically creates an associated security policy after the configuration is complete.

([portmap_aaa](#))

Yes

Add Without Creating Security Policy

Follow-up Procedure

- 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.

8.3 Security Defense

8.3.1 Principle and Application Scenario

1. Local Defense

When traditional devices in a complex network undergo network attacks or heavy traffic, the following situations may occur:

- Extra high CPU utilization.
- Slow CLI response or no response.
- Loss of link or network control protocol packets, causing link or network jitter.
- Processing bandwidth occupied by illegal packets, resulting in a failure to process important protocol packets.

There are two reasons for these problems. One reason is that the processing capabilities of the traditional devices' control planes and forwarding planes are different. The other reason is that there is a lack of protection mechanism for the control plane. Z-S series firewalls can classify, filter, and limit the rate of data packets to be processed at the control layer, thus protecting key resources at the control layer. Z-S series firewalls support flexible combinations of associated various objects (region objects, address objects, and service objects) to formulate various local defense policies suitable for actual network security needs, accurately controlling the access rights of devices, and ensuring device security.

2. Security Defense

There may be many forms of attacks in customers' network environment, such as traffic-targeted DDoS attacks and packet- or protocol-targeted attacks (such as teardrop, smurf, and redirect). The target may be a user on the intranet or the device itself. Therefore, you can configure policies to help intranet users and devices defend against attacks. Local defense provides default policies to ensure the normal operation of the device. For ARP attacks on the intranet, security defense provides static ARP configuration, proxy ARP, and anti-ARP spoofing functions.

- Protocol attacks (malformed packet attack)

Protocol attacks exploit the implementation vulnerabilities of protocol stack on the target device to send specific traffic or packets (malformed packets), to cause exceptions on the target device and achieve the purpose of denial of service. Common protocol attacks include land, smurf, fraggle, teardrop, WinNuke, ICMP redirect, ICMP unreachable, and large ICMP packet.

- Land

Attack principle/characteristics: The source address and destination address in the packet used for the land attack are the same. When a user device receives such packets, it may not know how to deal with the situation that the source address and destination address of the communication in the stack are the same, or it may send and receive the packets repeatedly, consuming a lot of system resources. As a result, the system may crash.

- Smurf

Attack principle/characteristics: This attack sends a packet with a specific request (such as an ICMP request) to the broadcast address of a subnet, and fills in the attacked host's address as the source address. Then all hosts on the subnet respond to a broadcast packet request and send packets to the attacked host. The host is attacked. Attackers can generate heavy attack traffic to the attacked host with a small cost.

- Fraggles

Attack principle/characteristics: By making a simple modification of the smurf attack, fraggle uses UDP reply packets instead of ICMP packets (attack ports 7 (echo) or 19 (chargen)).

- Teardrop

Attack principle/characteristics: This attack is mainly carried out by exploiting vulnerabilities in the system during IP packet reassembly. Teardrop is a UDP-based attack using malformed fragments. It sends multiple overlapping IP fragments to the attacked device (IP fragments include information such as which packet the fragment belongs to and the position in the packet). The attacker deliberately makes these fragments overlap. Some operating systems will crash and restart when they receive forged fragments with overlapping offset.

- WinNuke

Attack principle/characteristics: WinNuke attack, also known as out-of-band transmission attack, attacks the destination ports, which are usually ports 53, 113, 137, 138, and 139. The URG bit is set to 1, that is, emergency mode.

- ICMP redirect

Attack principle/characteristics: The attacker sends an ICMP redirect packet to the attacked host as a gateway, telling the host "the next hop to the next destination is me", so the attacked host modifies the routing table. The host's traffic is redirected to the attacker, and the attacker can sniff and hijack the traffic.

- ICMP unreachable

Attack principle/characteristics: The attacker sends a forged ICMP unreachable packet to the attacked host, making the target host unable to access the destination host, port, or network segment and cutting off the connection between the host and the destination.

- Large ICMP packet

Attack principle/characteristics: Attack the target system by sending large ICMP packets. Some systems may crash or restart after receiving the large ICMP packet due to improper processing.

- Flood (flow-based attack)

Flood attacks mainly consume limited resources such as connection, bandwidth, and CPU of the attacked host to achieve deny of service of the target host. Common resource-consuming attacks include various types of flow-based flood attacks, including syn-flood, udp-flood, and icmp-flood.

- Scan

Scan attack is usually the first step in the attacker's attempt to the target host/network. By scanning ports/IP addresses, the attacker discovers the ports, services, and OS types in the target host/network, which is the basic information for further penetration or attack. By traffic analysis, you will find that a specific host initiates a large number of connections to the consecutive ports at an IP address (attempt to detect open services) or consecutive IP addresses on a network segment (attempt to detect active hosts) in a short time.

3. Intrusion Prevention

Intrusion Prevention System (IPS) is a security product that performs in-depth inspection of traffic in real time to find threats and defend against them.

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

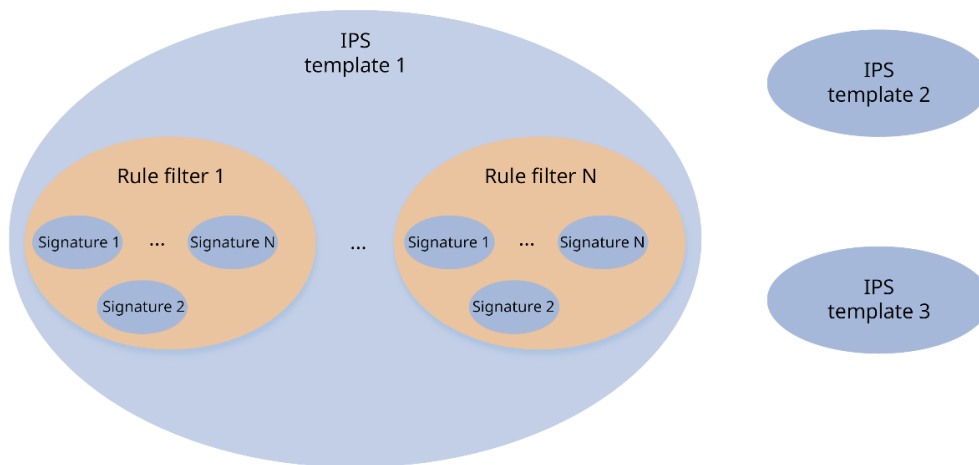
The IPS function of Z-S series firewalls is implemented using templates. Different templates can correspond to different signatures. You can customize the templates according to your needs. In addition, the device is delivered with a built-in "predefined template" that has been strictly verified.

- Custom template

The custom template is the basic configuration of Ruijie firewall IPS. A configuration template is composed of multiple "rule filters", and each rule filter consists of several signatures. You can combine specific rules into a configuration template according to your needs.

[Figure 8-4](#) shows the relationships between configuration template, rule filter, and signature.

Figure 8-4 Relationships Between Configuration Template, Rule Filter, and Signature

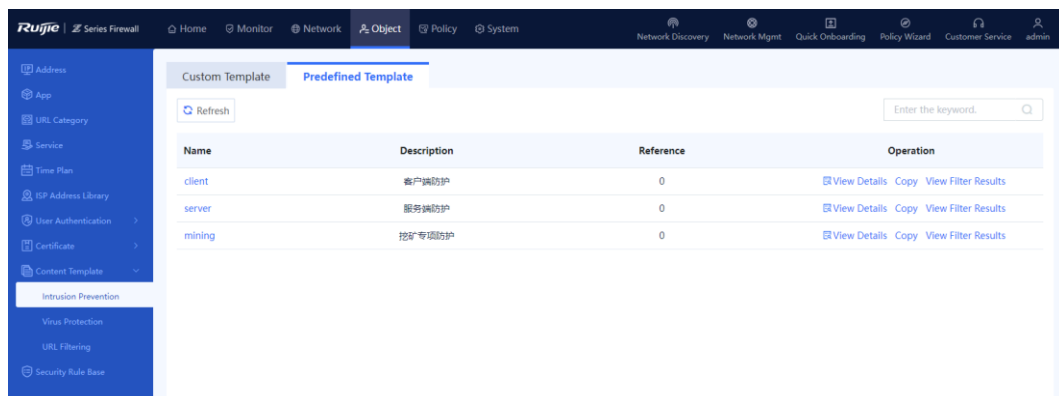


IPS supports multiple templates. An IPS template supports multiple rule filters. Each rule filter supports multiple signatures.

- Predefined template

The elements contained in predefined templates are consistent with those in custom templates. Their differences lie in:

- Predefined templates are a series of market-proven templates defined by Ruijie according to different usage scenarios. They can be directly used without modification or commissioning.
- The predefined templates will be updated automatically, and Ruijie will update the rule sets in the predefined templates according to the feedback from the market, which can reduce the maintenance manpower.



- IPS template referenced by policy

When the template configuration is completed, the IPS function of Z-S series firewall takes effect only after you reference the IPS template on the policy page. After referencing the template, you can select the actions to be performed on the traffic that hits the template according to your needs:

- Default Action: All traffic that hits the signature is processed using the actions of the signature.
- Alarm: Alarms are reported for all traffic that hits the signature, ignoring the actions of the signature.
- Block: All traffic that hits the signature is blocked, ignoring the actions of the signature.

Content Security (After being enabled, the following configurations only take effect for IPv4 traffic.)

Intrusion Prevention	<input checked="" type="radio"/> Enable	<input type="radio"/> Not Enabled	mining	Action:	Default A	Add Intrusion Prevention Template
Virus Protection	<input checked="" type="radio"/> Enable	<input type="radio"/> Not Enabled	default	Action:	Block	Add Virus Protection Template
URL Filtering	<input type="radio"/> Enable	<input checked="" type="radio"/> Not Enabled	Add URL Filtering			

4. Virus Protection

Caution

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

Virus protection is a security detection technology that analyzes network traffic and files in real time to identify hidden viruses, and reports alarms or blocks the traffic to protect the security of intranet data.

This function supports virus detection for video files, audio files, image files, executable files, documents, compressed files, web files, code files, script files, and text files transmitted by HTTPS, HTTP, FTP, SMTP, and POP3. Before detecting HTTPS traffic, you need to configure the SSL proxy function. For more information about SSL proxy, see [8.9 Configuring SSL Proxy Policies](#).

The firewall supports two virus detection modes: quick scan and deep scan. Different modes use different virus protection signature libraries:

- Quick scan: Use the **Virus Protection Signature Library (Quick Scan)**. The virus detection rate is low but the performance overhead is small.
- Deep scan: Use the **Virus Protection Signature Library (Deep Scan)**. The virus detection rate is high but the performance overhead is large.

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

When the template configuration is completed, the function takes effect only after you reference the virus protection template on the security policy page. After referencing the template, you can select the actions to be performed on the traffic that hits the template according to your needs:

- Alarm: Always report alarms when virus is detected in traffic (only alarm, no blocking)
- Block: Block all traffic with virus detected.

Content Security (After being enabled, the following configurations only take effect for IPv4 traffic.)

Intrusion Prevention Enable Not Enabled `mining` Action: [Add Intrusion Prevention Template](#)

Virus Protection Enable Not Enabled `default` Action: [Add Virus Protection Template](#)

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

5. Threat intelligence

Most of the typical security capabilities (such as AV and IPS) of firewalls are based on the analysis of traffic content. The firewalls use regularly updated signatures, rules and other information for detection, which has problems such as large detection costs and difficulty in dealing with new network threats such as Advanced Persistent Threat (APT) and zero-day vulnerabilities.

Threat Intelligence (TI) introduces real-time and global security threat knowledge to firewalls, enabling the firewalls to identify and filter malicious traffic with less computing overhead. Therefore, TI becomes an indispensable part of the multi-layer security protection system of firewalls.

The TI module can match threat intelligence based on the destination IP address of the traffic and the domain name in the DNS query, and perform blocking or alarming actions on the data that matches the threat intelligence, to block malicious IP addresses and domain names.

Data sources of threat intelligence include:

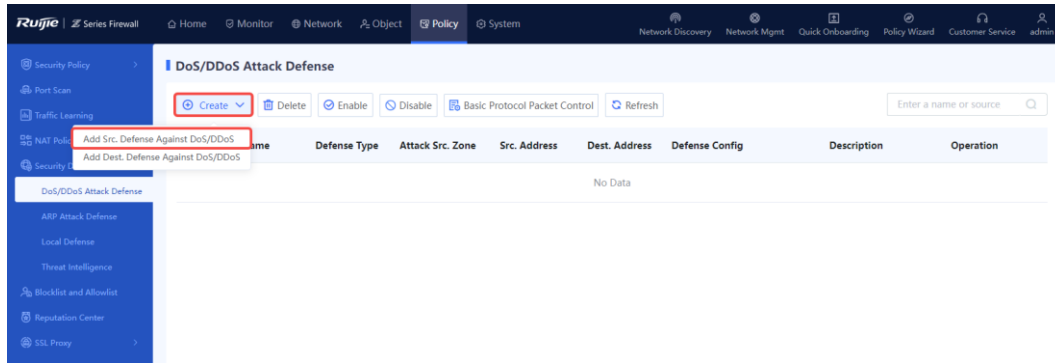
- Threat intelligence signature library: Contains a large amount of threat signature data and can be upgraded to obtain the latest data. After the TI authorization is activated, the firewall can perform security detection based on the threat intelligence signature library to enhance the capability of identifying and blocking threats. If the TI function is not authorized or authorization expires, detection based on the threat intelligence signature library is unavailable.
- Custom threat intelligence: In addition to the intelligence contained in the threat intelligence signature library, the system allows you to import malicious intelligence that you have collected. When threat is detected, the system matches the threat against the Custom Threat Intelligence first. The data matching Custom Threat Intelligence is blocked and a security log is recorded. In the unauthorized state, Custom Threat Intelligence can still be used for matching.

8.3.2 DoS/DDoS Attack Defense

1. Configuring Source Defense Against DoS/DDoS

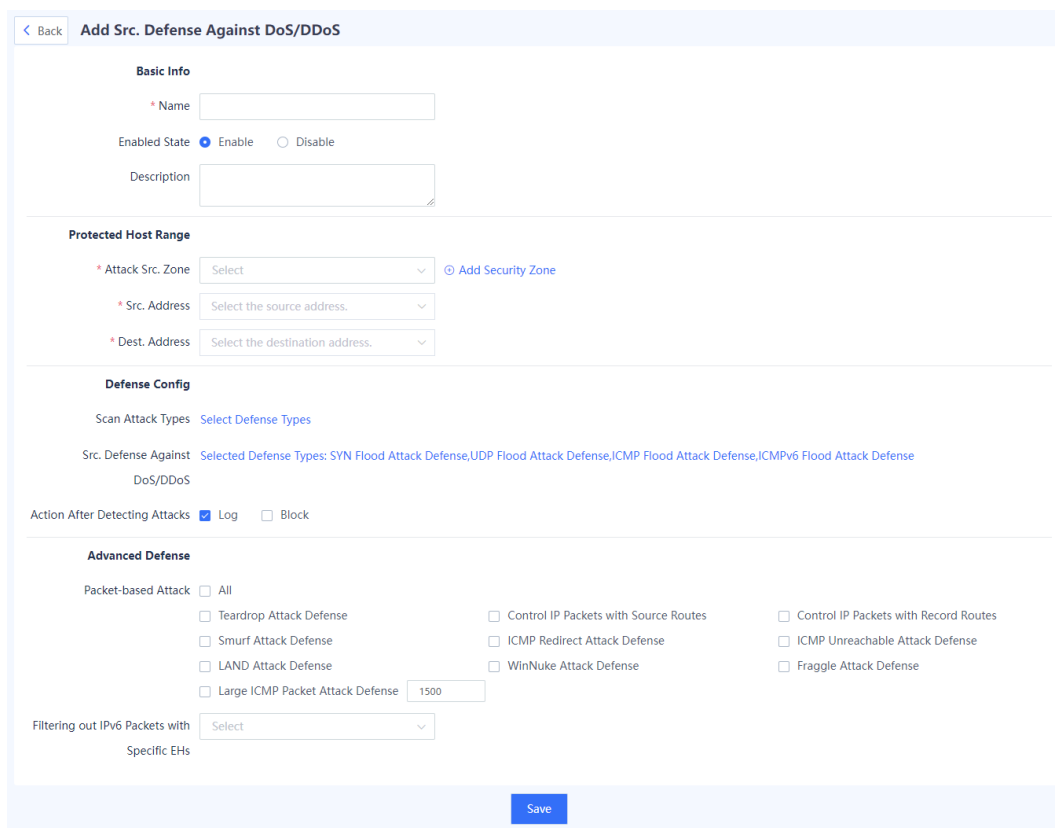
Procedure

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



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

The system displays the Add Src. Defense Against DoS/DDoS page.



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

Item	Description	Remarks
Basic Info		

Item	Description	Remarks
Name	Name of the DoS/DDoS attack defense policy.	Characters such as `~!#%^&*+ \{};:'"/<>? and spaces are not allowed. [Example] DoS_policy_1
Enabled State	Whether to enable the policy immediately after configuration is completed.	[Example] Enable
Description	Description of the DoS/DDoS attack defense policy.	Characters such as `~!#%^&*+ \{};:'"/<>? are not allowed. [Example] New policy
Protected Host Range Range of the attack source associated with the policy. The policy takes effect when matching.		
Attack Src. Zone	The policy checks the traffic from this security zone.	[Example] any
Src. Address	The policy checks the traffic from this address set.	any indicates all addresses. [Example] any
Dest. Address	The policy checks the traffic to this address set.	any indicates all addresses. [Example] any
Defense Config		
Scan Attack Types		
IP Scan Defense	Whether IP scan defense is enabled.	[Example] Enabled
Limit (pps)	Threshold for detecting an IP scan attack and triggering protection.	[Example] 10000
Blocking Duration (s)	Duration of traffic blocking after an attack is detected.	[Example] 300s

Item	Description	Remarks
Port Scan Defense	Whether port scan defense is enabled.	[Example] Enabled
Limit (pps)	Threshold for detecting a port scan attack and triggering protection.	[Example] 10000
Blocking Duration (s)	Duration of traffic blocking after an attack is detected.	[Example] 300s
DoS/DDoS Attack Defense (Based on Src. IP)		
Attack defense type.	Defense against SYN flood, UDP flood, ICMP flood, and ICMPv6 flood.	Click an attack defense type to enable defense against the specific attacks. [Example] Select SYN Flood Attack Defense .
Src. IP 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] Select Log and Block .
Advanced Defense		
Packet-based Attack	Whether defense against packet-based attacks is enabled.	[Example] All
Filtering out IPv6 Packets with Specific EHs	Filter out the IPv6 packets with the extended headers of the specified type.	[Example] Empty EHs

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

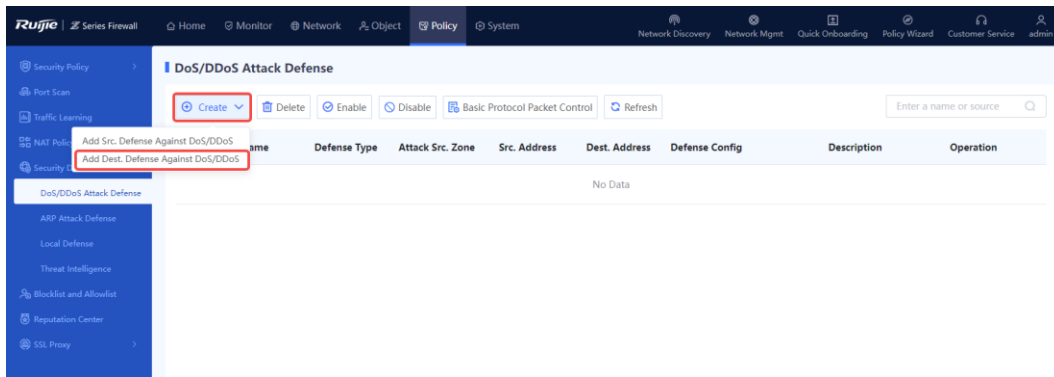
Follow-up Procedure

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

2. Configuring Destination Defense Against DoS/DDoS

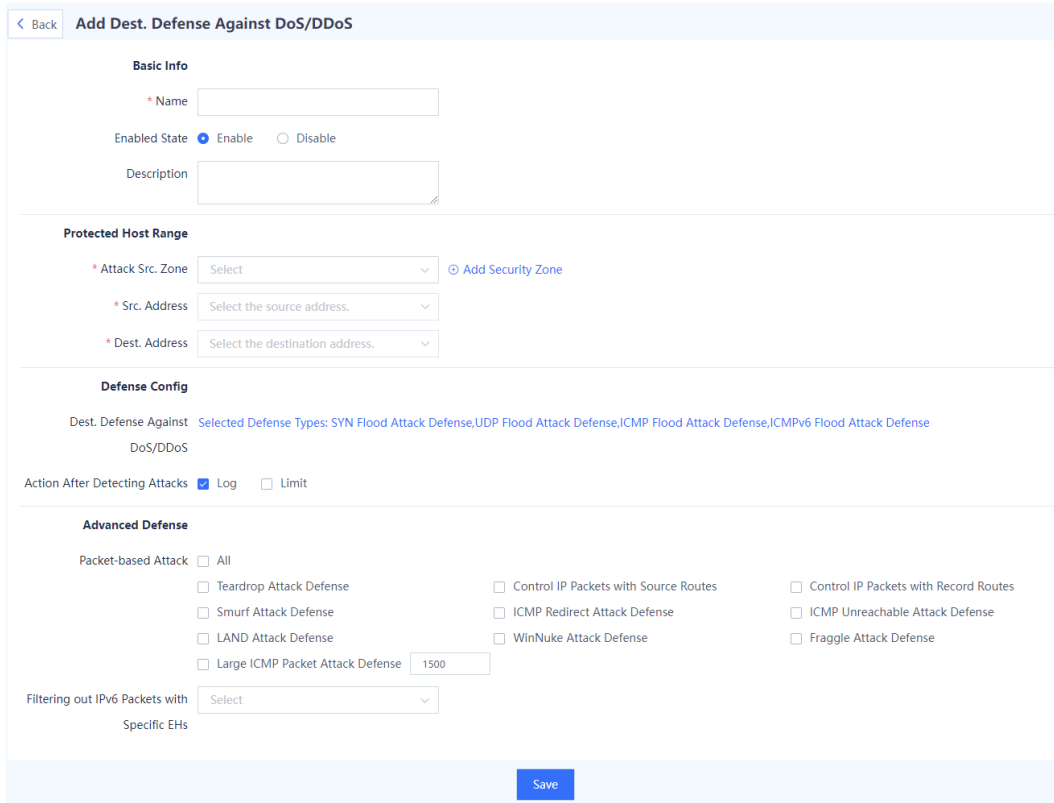
Procedure

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



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

The system displays the Add Dest. Defense Against DoS/DDoS page.



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

Item	Description	Remarks
Basic Info		
Name	Name of the DoS/DDoS attack defense policy.	Characters such as `~!#%^&*+ \{ };:'''/<>? and spaces are not allowed. [Example] DoS_policy_1
Enabled State	Whether to enable the policy immediately after configuration is completed.	[Example] Enable
Description	Description of the DoS/DDoS attack defense policy.	Characters such as `~!#%^&*+ \{ };:'''/<>? are not allowed. [Example] New policy
Protected Host Range Range of the attack source associated with the policy. The policy takes effect when matching.		
Attack Src. Zone	The policy checks the traffic from this security zone.	[Example] any
Src. Address	The policy checks the traffic from this address set.	any indicates all addresses. [Example] any
Dest. Address	The policy checks the traffic to this address set.	any indicates all addresses. [Example] any
Defense Config		
Dest. Defense Against DoS/DDoS		
Attack defense type.	Defense against SYN flood, UDP flood, ICMP flood, and ICMPv6 flood.	Click an attack defense type to enable defense against the specific attacks. [Example] Select SYN Flood Attack Defense .

Item	Description	Remarks
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] Select Log and Limit.
Advanced Defense		
Packet-based Attack	Whether defense against packet-based attacks is enabled.	[Example] All
Filtering out IPv6 Packets with Specific EHs	Filter out the IPv6 packets with the extended headers of the specified type.	[Example] Empty EHs

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

Follow-up Procedure

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

8.3.3 Intrusion Prevention

1. Creating a Custom IPS Content Template

Application Scenario

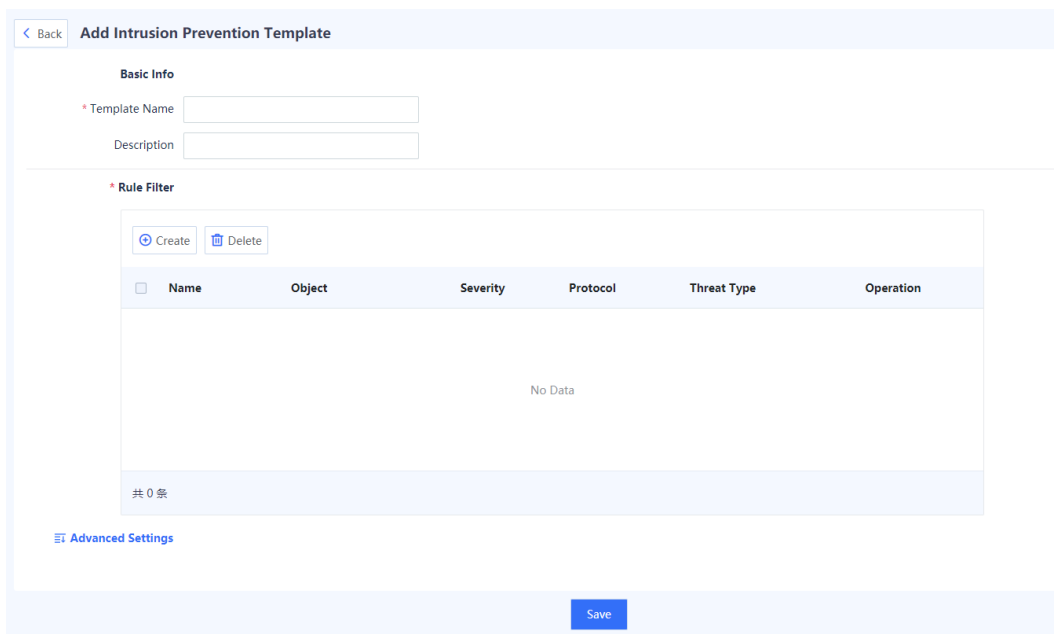
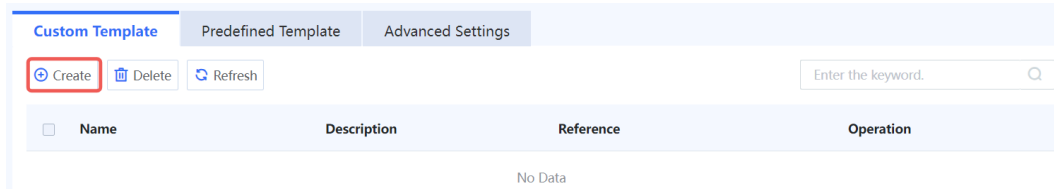
By performing in-depth detection on the traffic passing the firewall in real time, IPS can report alarms and block traffic in real time to protect user hosts from malicious traffic.

Configuration Points

- (1) Customize the intrusion prevention template.
- (2) Set the parameters of intrusion prevention template (rule filter).
- (3) Reference the IPS custom template to security policy and select actions (alarming, blocking, or default action).

Procedure

- (1) Add an intrusion prevention template.
 - a Choose **Object > Content Template > Intrusion Prevention > Custom Template**.
 - b Click **Create** to enter the Add Intrusion Prevention Template page.



- (2) Add a rule filter and set parameters.

Enter the name and description of the custom template based on the actual intrusion prevention scenario or protection requirements.

- c In the **Rule Filter** area, click **Create**, set parameters, and click **Confirm**.

[Back](#) **Add Intrusion Prevention Template**

Basic Info

* Template Name

Description

*** Rule Filter**

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

共 0 条

[Advanced Settings](#)

Add Rule Filter



* Name

* Object All Server Client

* Severity All High Medium Low Tip

Protocol

To-be-selected (5) Select All

Selected (0) [Clear](#)

Enter the keyword.

- DNS
- HTTP
- TCP
- TLS
- UDP

Threat Type

To-be-selected (93) Select All


Selected (0) [Clear](#)

Enter the keyword.

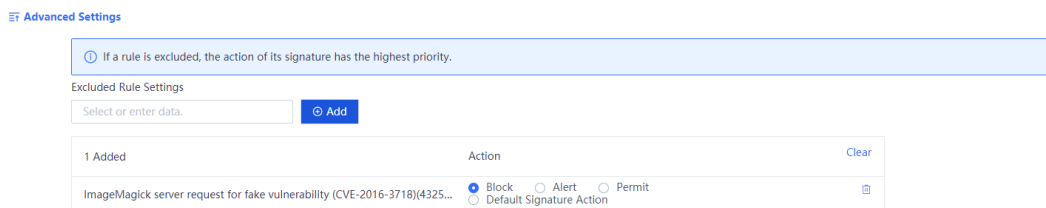
- Brute Force
- DDOS
- Deserialization
- Event Monitor
- Information Leakage
- Injection Attack

Cancel

Confirm

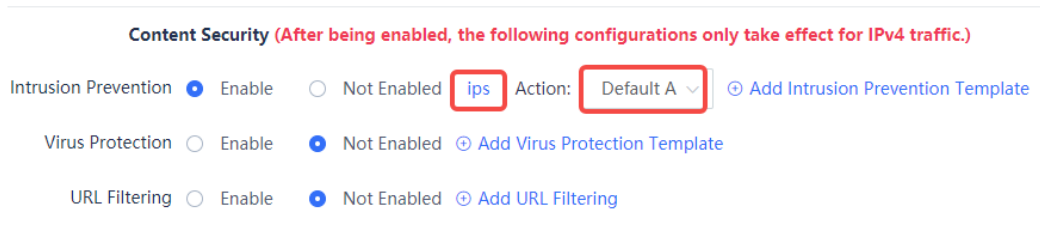
- o **Name:** Customized. You are advised to configure a name that can describe the filter function.
 - o **Object:** Objects to be protected.
 - o **Severity:** Defense severity. For example, if only **High** is selected, only the security rules with high severity can hit the filter.
 - o **Protocol:** Protocols to be detected. The protocol traffic that is not specified does not hit the filter.
 - o **Threat Type:** Types of threats to be detected. The threat traffic that is not specified does not hit the filter. If you have no special protection requirements, select all.
- d (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.



e Click **Save** to complete the configuration of intrusion prevention template.

- (3) Choose **Policy > Security Policy > Create Security Policy** to associate the security policy with intrusion prevention. Configure the template as predefined, set the action to alarming, blocking, or default (default action refers to the recommended action predefined in the system in Security Rule Base).



Content Security (After being enabled, the following configurations only take effect for IPv4 traffic.)

Intrusion Prevention Enable Not Enabled **ips** Action: **Default A** [Add Intrusion Prevention Template](#)

Virus Protection Enable Not Enabled [Add Virus Protection Template](#)

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

Rule ID	Defense Name	Threat Type	Threat Subtype	Severity	Action	Operation
4259841	D-LINK DIR-615 cross-station request for...	-	-	Medium	Alarm	<input checked="" type="checkbox"/> View Details
4259842	Western Digital mycloud NAS CSRF vuln...	-	-	High	Block	<input checked="" type="checkbox"/> View Details
4259843	Wiki Cross Site Request Forgery Attack (c...	-	-	High	Block	<input checked="" type="checkbox"/> View Details
4259844	Easy hosting control panel Cross Site Req...	-	-	Medium	Alarm	<input checked="" type="checkbox"/> View Details
4325377	ImageMagick server request for fake vul...	-	-	Medium	Alarm	<input checked="" type="checkbox"/> View Details
4325378	WordPress Print My Blog Plug-in Code Pr...	-	-	High	Block	<input checked="" type="checkbox"/> View Details
4325379	Weblogic SSRF vulnerability (cve-2014-4...	-	-	Medium	Alarm	<input checked="" type="checkbox"/> View Details
4325380	Weblogic SSRF vulnerability (cve-2014-4...	-	-	Medium	Alarm	<input checked="" type="checkbox"/> View Details
4325381	Avtech DVR device server side Request F...	-	-	Medium	Alarm	<input checked="" type="checkbox"/> View Details
4325382	VMware vrealize SSRF vulnerability(cve-2...	-	-	Medium	Alarm	<input checked="" type="checkbox"/> View Details


2. IPS Advanced Settings

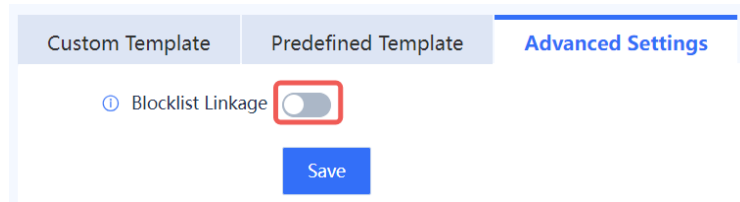
Application Scenario

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.

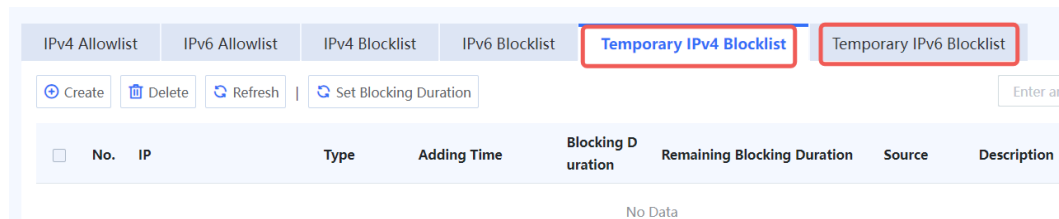
(2) Toggle on  to enable blocklist linkage.



(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.



8.3.4 Virus Protection

Application Scenario

If intranet users often download various application data from the Internet or the intranet servers often need to receive data uploaded by Internet users, you can configure virus protection policies on the firewall to detect virus in the passing traffic and configure real-time alarming and blocking to protect user hosts from malicious traffic.

Caution

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

Configuration Points

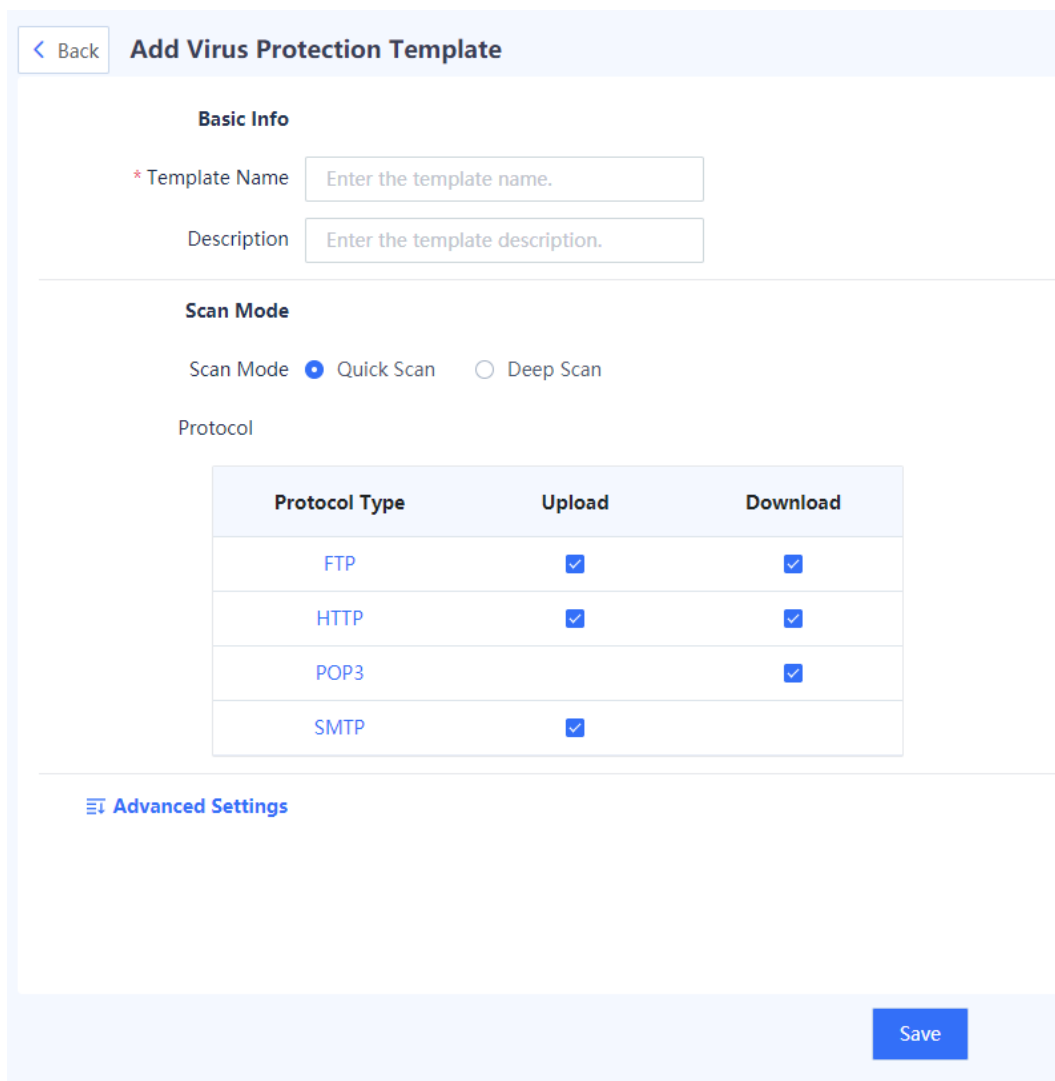
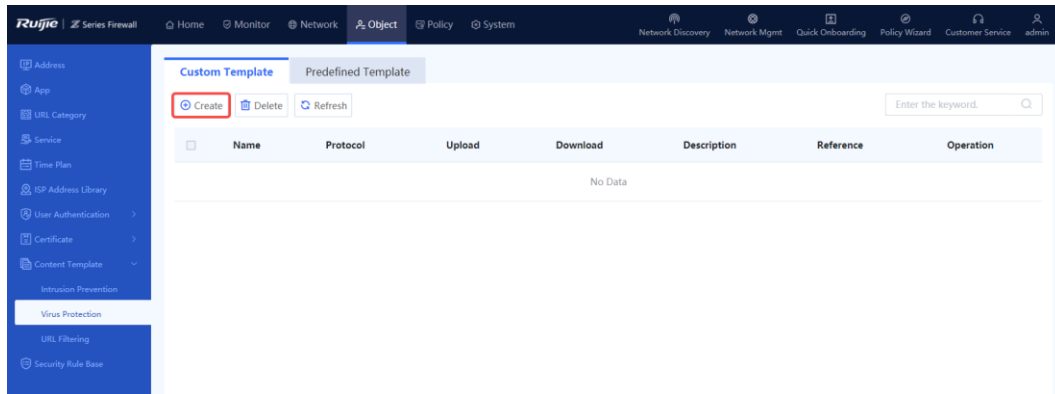
- (1) Customize the virus protection template.
- (2) Reference the virus protection template to security policy and select actions (alarming or blocking).

- (3) To detect HTTPS traffic, you need to configure the SSL proxy function. For more information about SSL proxy, see [8.9 Configuring SSL Proxy Policies](#).

Procedure

- (1) Add a virus protection template.

Choose **Object > Content Template > Virus Protection > Custom Template**. Above the operation area, click **Create**.



- **Quick Scan:** Use the **Virus Protection Signature Library (Quick Scan)**. The virus detection rate is low but the performance overhead is small.
 - **Deep Scan:** Use the **Virus Protection Signature Library (Deep Scan)**. The virus detection rate is high but the performance overhead is large.
 - **Protocol:** Detect virus for the uploaded or downloaded packets of the specified protocol. The packets of unspecified protocols are forwarded directly without virus detection.
 - If the specified MD5 value or application is configured as excluded, the firewall will directly forward the packets of the specified MD5 value or application.
- (2) Choose **Policy > Security Policy > Create Security Policy** to associate the security policy with virus protection. Select a virus protection template and set the action to Alarm or Block.

Content Security (After being enabled, the following configurations only take effect for IPv4 traffic.)

Intrusion Prevention Enable Not Enabled [Add Intrusion Prevention Template](#)

Virus Protection Enable Not Enabled Action: [Add Virus Protection Template](#)

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

8.3.5 ARP Attack Defense

1. Configuring Static ARP

Application Scenario

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

Procedure

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

The screenshot shows the 'Static ARP Entry List' configuration page. At the top, there are tabs for 'Proxy ARP', 'Anti-ARP Spoofing', and 'Anti-ARP Rate Limit'. Below the tabs, there are buttons for 'Create', 'Delete', and 'Refresh'. There are input fields for 'IP', 'MAC', and 'Interface' (with a dropdown menu). Below these fields is a table with the following columns: IP, MAC, Interface, Status, Description, and Operation. The table is currently empty, and the text 'No Data' is displayed below it.

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

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

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

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

Item	Description	Remarks
IP	IP address to be bound to the static ARP entry.	[Example] 192.168.10.3
MAC	MAC address to be bound to the static ARP entry.	Two configuration methods are supported: <ul style="list-style-type: none"> ● Fill in the information manually. ● Click Auto MAC Obtaining. The device will search for the MAC address matching the IP address according to the available ARP entry information. If no address is found, the system displays "No address is matched." [Example] 11:22:33:44:55:66
Interface	Physical interface to be bound.	Two configuration methods are supported: <ul style="list-style-type: none"> ● Fill in the information manually. ● Click Auto Interface Discovery. The device will configure the interface that may match the IP address according to the related information. If no interface is found, the system displays "No interface is matched." [Example] Ge0/1

(4) Click **Save** to complete the configuration of static ARP policy.

Follow-up Procedure

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

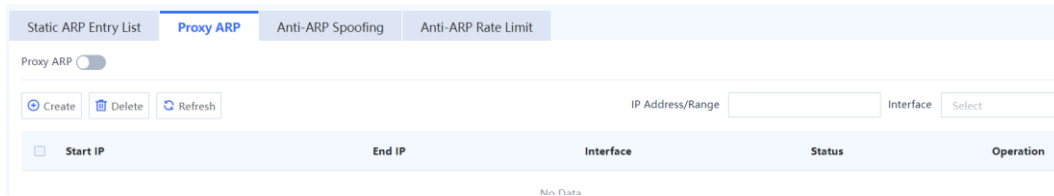
2. Configuring Proxy ARP

Application Scenario

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

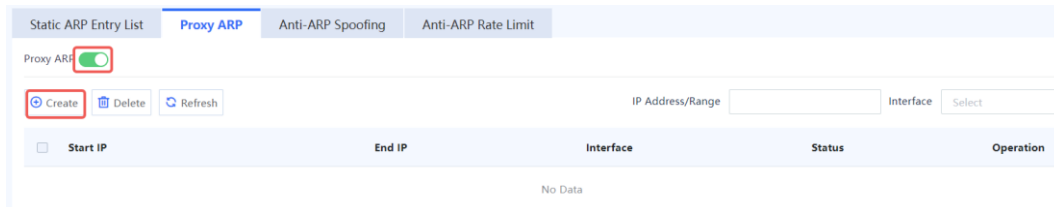
Procedure

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



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

- (2) Enable Proxy ARP.



- (3) Click **Create**.

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

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

- (5) Click **Save** to complete the configuration of proxy ARP.

Follow-up Procedure

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

3. Configuring Anti-ARP Spoofing

Application Scenario

The firewall periodically sends gratuitous ARP broadcast packets to allow terminals on the same network segment to obtain the correct MAC address of the firewall, thus preventing attackers from forging the gateway.

Procedure

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

- (2) Enable Anti-ARP Spoofing.
- (3) Modify Gateway MAC Broadcast Interval. The unit is second.
- (4) Click **Save** to save the configuration.

4. Configuring ARP Rate Limiting

Application Scenario

ARP rate limiting can be configured for networks with heavy ARP traffic. After a global rate limit is set for ARP request or reply packets, when all ARP request or reply packets (including uplink and downlink packets) exceed the rate limit and the ARP request or reply packets from a source IP address exceed 5 pps, the excessive packets are discarded. Otherwise, the packets are forwarded.

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**.

8.3.6 Local Defense

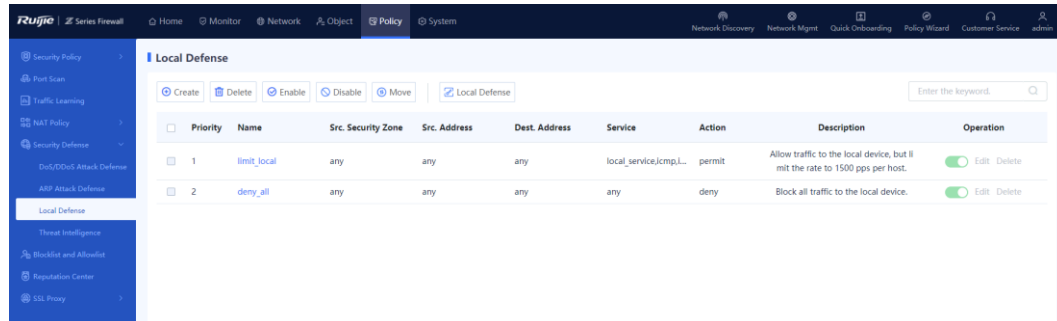
Application Scenario

The local defense function can block or restrict specified types of packets sent to the local device. For example, you can specify the ping packets in the traffic sent to the local device. Then the device directly discards the ping packets to forbid any ping operation to the local device, thus ensuring the normal running of the device.

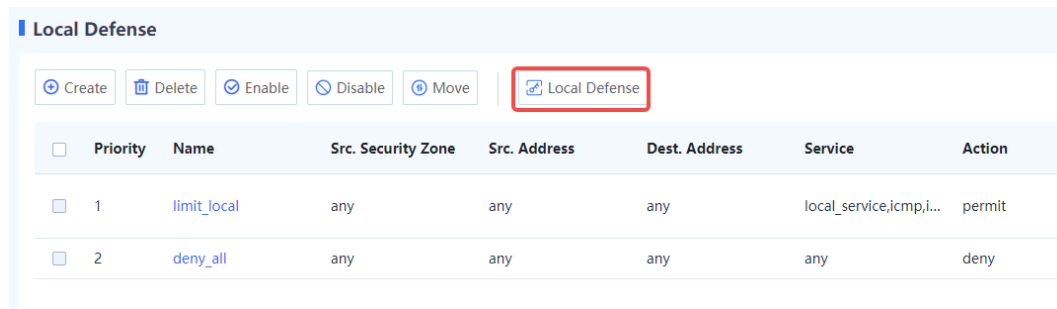
The local defense function has two default policies that cannot be modified to ensure that the device is protected from traffic attacks after this function is delivered.

Procedure

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



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



Local Defense

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

Enable Local Defense

Confirm Cancel

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

< Back
Create Local Defense Policy

Basic Info

* Name

Enabled State Enable Disable

Adjacent Policy Select a policy. ▾ Before ▾

Description

Src. and Dest.

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

Src. Address

To-be-selected (5)

Select ▾ Enter the keyword.

- 200.10.10.10 200.10.10.10
- lan_users 192.168.1.20
- 172.26.1.116 172.26.1.116
- TrafficLearn... 172.20.37.114
- PortScan_de... 172.20.37.54

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

Selected (1) Clear

Enter the keyword.

any 🗑

Dest. Address

To-be-selected (5)

Select ▾ Enter the keyword.

- any
- 200.10.10.10 200.10.10.10
- lan_users 192.168.1.20
- 172.26.1.116 172.26.1.116
- TrafficLearn... 172.20.37.114

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

Selected (1) Clear

Enter the keyword.

any 🗑

Service

Service

To-be-selected (78)

Select ▾ Enter the keyword.

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

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

Selected (1) Clear

Enter the keyword.

any 🗑

Action Settings

Action Option Permit Deny

IP-based Rate Limit

IP-based Rate Limit Disable Enable

(4) Set the parameters of local defense policy.

Item	Description	Remarks
Basic Info		
Name	Name of the local defense policy.	Characters such as `~!#%^&*+ \ {};:"'<>?` and spaces are not allowed. [Example] policy_1
Enabled State	Whether the policy is enabled in the system.	[Example] Enable
Adjacent Policy	Move the new policy before or after the specified policy. The closer a policy is to the front, the higher its priority is in matching.	-
Description	Security policy description.	Characters such as `~!#%^&*+ \ {};:"'<>?` are not allowed.
Src. and Dest. Associate the policy with source security zone, source address object, destination address object, and service object. The policy takes effect when all the four items are hit.		
Src. Security Zone	The policy checks the traffic from this zone.	any indicates traffic of all zones. [Example] any
Src. Address	The policy checks the traffic from this address set.	any indicates all addresses. [Example] any
Dest. Address	The policy checks the traffic to this address set.	any indicates all addresses. [Example] any
Service	The policy checks the traffic of this service.	any indicates all services. [Example] any
Action Settings		

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

(5) Click **Save**.

Follow-up Procedure

- To delete multiple policies in a batch, select the policies that you want to delete and click **Delete** in the above bar.
- To enable multiple policies in a batch, select the policies that you want to enable and click **Enable** in the above bar.
- To disable multiple policies in a batch, select the policies that you want to disable and click **Disable** in the above bar.
- To adjust the policy priority, click **Move**. The closer a policy is to the front, the higher its priority is in matching.
- Enter the policy names, policy associated objects, full or part of the policy description in the search box to search for the policies. Fuzzy search is supported.

8.3.7 Session Suppression

1. Configuring the Uplink Packet Rate Limit

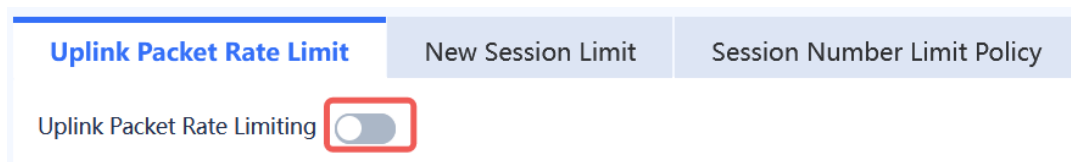
Application Scenario

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 > Security Defense > Session Suppression > 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.

The screenshot shows the configuration interface for 'Uplink Packet Rate Limit'. It includes tabs for 'New Session Limit' and 'Session Number Limit Policy'. The 'Uplink Packet Rate Limiting' toggle is turned on. Under 'Global Per-IP Rate Limiting', the 'Global Per-IP/IPv6 Uplink Limit (pps)' is set to 0, and a 'Save' button is visible. Below this, the 'Rate Limiting on Designated IP' section has 'Create', 'Delete', and 'Refresh' buttons, and a table with columns for 'IP', 'Limit (pps)', and 'Operation'. The table currently shows 'No Data'.

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**.

This screenshot is identical to the previous one, but the 'Create' button in the 'Rate Limiting on Designated IP' section is highlighted with a red box, indicating the next step in the configuration process.

b Configure rate limiting on a designated IP address.

< Back

Create Rate Limiting on Designated IP

* IP

* Uplink Limit (pps)

Item	Description	Remarks
IP	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.

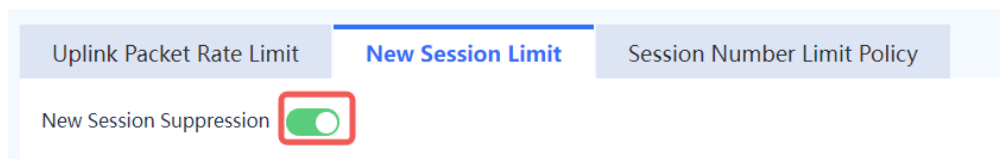
2. Configuring the New Session Limit

Application Scenario

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

Procedure

- (1) Choose Policy > Security Defense > Session Suppression > New Session Limit.
- (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	The priority of new session limiting on designated IP addresses is higher than that of global new session limiting. The default value is 0, indicating that the rate is not limited.	[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	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**.

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.


3. Configuring a Session Number Limit Policy

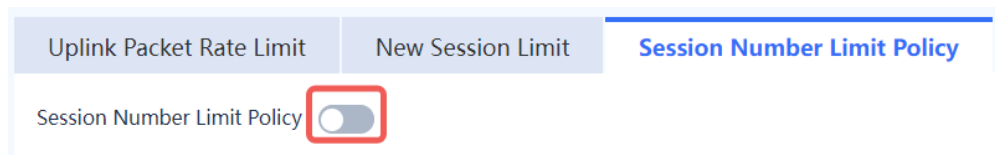
Application Scenario

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 a large number of attacks.

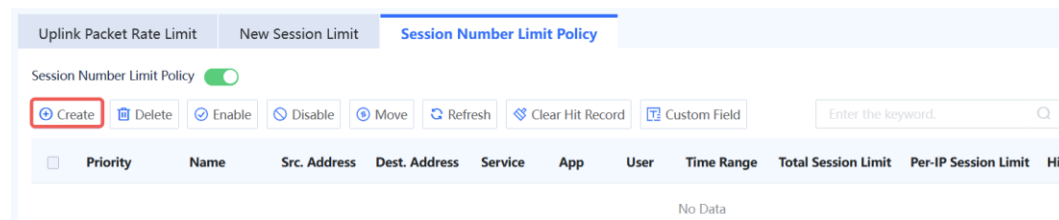
Procedure

(1) Choose Policy > Security Defense > Session Suppression > Session Number Limit Policy.

(2) Toggle on  to enable the session number limit policy function.



(3) Click Create.



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

Back

Create Session Number Limit Policy

Basic Info

* Name

* Enabled State Enable Disable

Description

Src. and Dest. Addresses

* Src. Address

* Dest. Address

Service

Service

App

App

User

User/User Group

Time Range

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

Total Session Limit

* ⓘ Total Session Limit

Per-IP Session Limit

* ⓘ Per-IP Session Limit

Action Settings

Action Option Alarm Block

Save

Item	Description	Remarks
Name	Name of the session number limit policy.	Characters such as `~!#%^\$&*+ {};:~!#%</>? and spaces are not allowed. [Example] Test
Enabled State	Enable or disable the policy.	[Example] Enable

Item	Description	Remarks
Description	Description of the session number limit policy.	Characters `~!#\$%^&*+\\ {};:"/;<>? are not allowed. [Example] Test
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	<p>If the total session limit or per-IP session limit is exceeded, the action specified in the policy is performed.</p> <p>Currently, the following modes are supported:</p> <p>Alarm: Packets are allowed to pass through, and a log is recorded.</p> <p>Block (default value): The session is blocked, and a log is recorded.</p>	<p>[Example]</p> <p>Alarm</p>

(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.


8.3.8 Threat Intelligence

1. Overview

Most of the typical security capabilities (such as AV and IPS) of firewalls are based on the analysis of traffic content. The firewalls use regularly updated signatures, rules and other information for detection, which has problems such as large detection costs and difficulty in dealing with new network threats such as Advanced Persistent Threat (APT) and zero-day vulnerabilities.

Threat Intelligence (TI) introduces real-time and global security threat knowledge to firewalls, enabling the firewalls to identify and filter out malicious traffic with less computing overhead. Therefore, TI becomes an indispensable part of the multi-layer security defense system of firewalls.

The TI module can match threat intelligence based on the destination IP address of the traffic and the domain name in the DNS query, and perform blocking or alarming actions on the data that matches the threat intelligence, to block malicious IP addresses and domain names.

 **Caution**

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

2. Enabling TI

Application Scenario

Enable the TI function on the firewall to block and alarm malicious IP traffic and malicious domain name query traffic, thus improving security defense effects.

Prerequisites

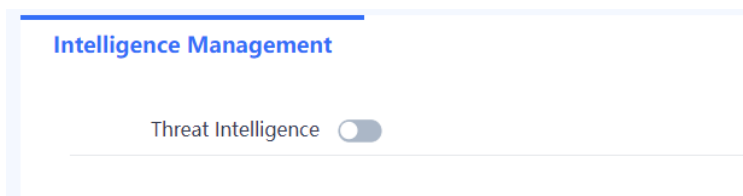
You have been authorized and activated the TI capability.

Note

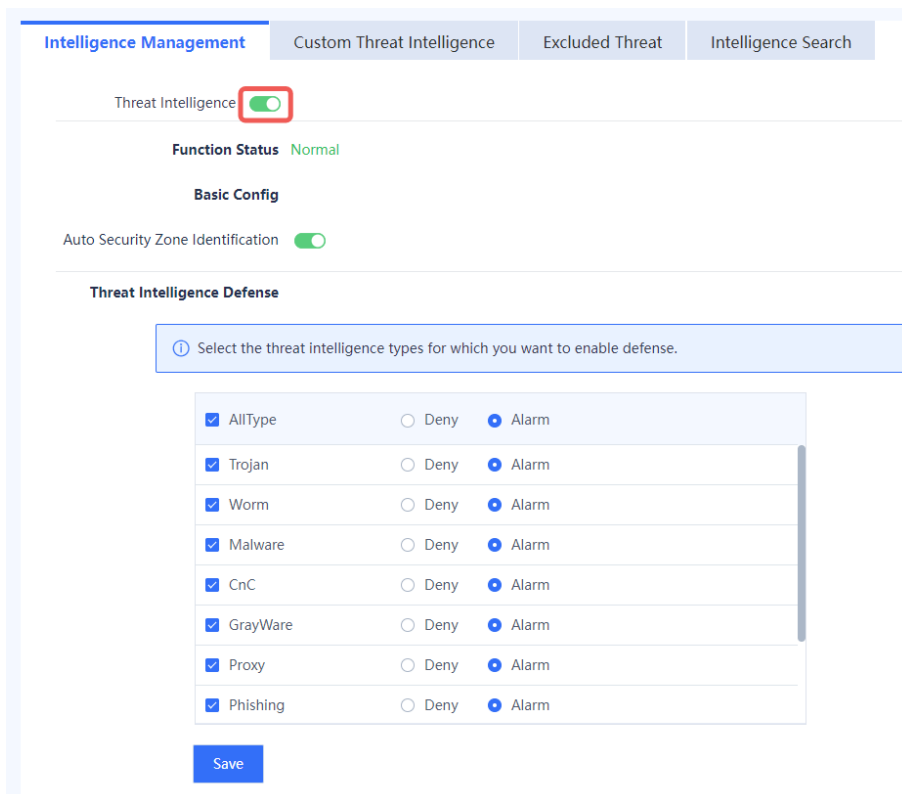
If the TI function is not authorized or authorization expires, the detection based on threat intelligence signature library is unavailable, and only the custom TI configured manually can be used. In this case, the threat intelligence signature library cannot be upgraded.

Procedure

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



- (2) Click to enable the TI function.



(1) Set the parameters of TI.

Item	Description	Remarks
Function Status	<p>Current status of the TI function</p> <ul style="list-style-type: none"> ● Unauthorized: The TI function license is not activated for the device, or the device cannot communicate with Ruijie Secure Cloud Platform. ● Normal: The TI function license is activated. The function is available and the library can be updated. ● Server Error: The TI function license is activated, but the secure cloud platform cannot connect to the threat intelligence signature library update server. The threat intelligence signature library cannot be updated. 	<p>The status is displayed automatically according to the current TI function status.</p> <p>[Example] Normal</p>
Basic Config		
Auto Security Zone Identification	<p>Whether to identify the traffic inbound and outbound security zones automatically.</p> <ul style="list-style-type: none"> ● After this function is enabled, the device automatically identifies the inbound and outbound security zones (ingress and egress) of traffic, and determines whether to perform threat signature matching for the traffic. ● If this function is disabled, you can manually specify the effective security zones for TI. 	<p>[Example] Enabled</p>
Effective Security Zone	<p>After the effective security zone is specified, the system performs TI matching and processing (block or alarm) for the traffic only when the outbound security zone of the traffic is the same as the specified zone.</p>	<p>When Auto Security Zone Identification is disabled, this parameter needs to be configured.</p> <p>[Example] untrust</p>
Threat Intelligence Defense		
Type	<p>Select the TI type to defend against.</p>	<p>Select to enable defense.</p> <p>[Example] APT</p>
Action	<p>Action to be taken on the traffic matching the TI:</p> <ul style="list-style-type: none"> ● Deny: Block traffic and record a security log. ● Alarm: Not block traffic, but record a security log. 	<p>[Example] Deny</p>

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

3. Customizing Threat Intelligence

Application Scenario

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

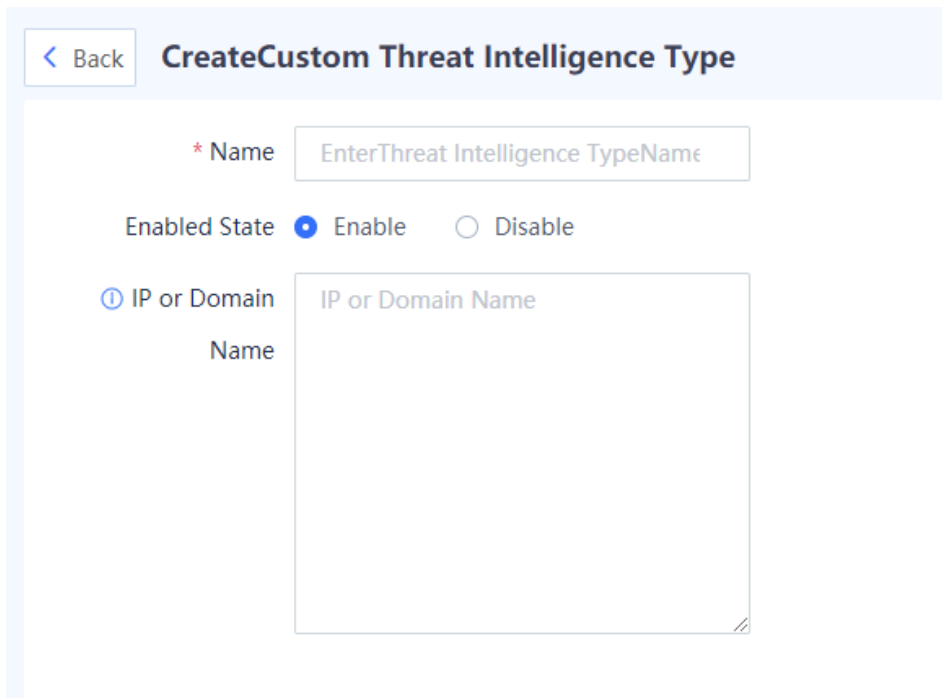
In the unauthorized state, custom threat intelligence can still be used for matching.

- Manually configure the custom TI.

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



(2) Click **Create** to enter the Create Custom Threat Intelligence Type page.



(3) Set the parameters of custom TI.

Item	Description	Remarks
Name	Name of the custom TI.	[Example] Trojan

Item	Description	Remarks
Enabled Status	Whether to enable the TI. The disabled TI will not be matched.	[Example] Enable
IP or Domain Name	IP address or DNS name to be checked and blocked.	<ul style="list-style-type: none"> If multiple IP addresses or domain names need to be configured, enter one IP address or domain name per line, and press Enter to separate lines. The domain name matching rule is full match. [Example] www.xxx.com

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

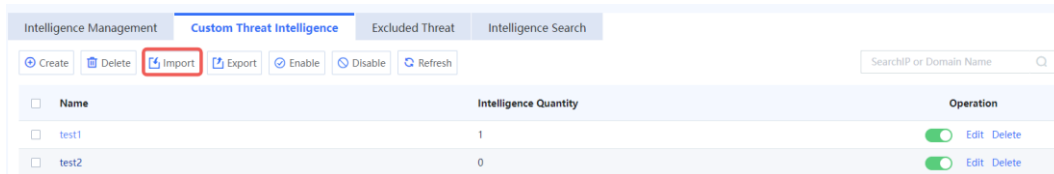
- Batch import custom TI.

Application Scenario

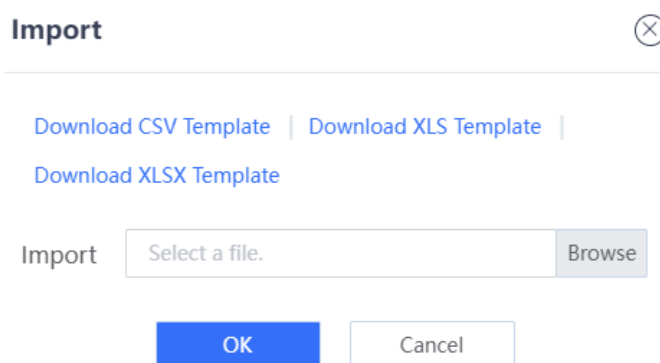
When you need to add a large number of TI types, you can fill in TI information in a template, and import them in a batch with one click.

Procedure

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



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



(3) Three formats of templates are supported. Click **Download CSV Template**, **Download XLS Template**, or **Download XLSX Template** to download the corresponding template.

- (4) Fill in the TI information in the template. Return to the web page, click **Browse**, and upload the configuration file.

Import ⊗


[Download CSV Template](#) | [Download XLS Template](#) | [Download XLSX Template](#)

Import Browse

OK
Cancel

- (5) Click **Confirm** to complete the file import.

Follow-up Procedure

- To modify the custom TI, click **Edit**.
- To delete the custom TI, click **Delete**.
- To enable or disable the custom TI, click .
- To enable or disable the TI types in a batch, select the TI types in the same status and click **Enable** or **Disable**.
- To save the custom TI to a local device, select the custom TI and click **Export**. The exported TI can be imported to other devices.

4. Configuring Excluded Threat

Application Scenario

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

Procedure

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

Intelligence Management			
Custom Threat Intelligence	Excluded Threat	Intelligence Search	
Name	Intelligence Quantity	Operation	
default	0	Edit Clear	

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

< Back

EditException Type

* Name

ⓘ IP or Domain Name

(3) Set the parameters of excluded threat.

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

Follow-up Procedure

- To modify the configuration of an excluded threat, click **Edit**.
- To delete all the IP addresses or domain names configured for an excluded threats, click **Clear**.

5. Querying Threat Intelligence

Application Scenario

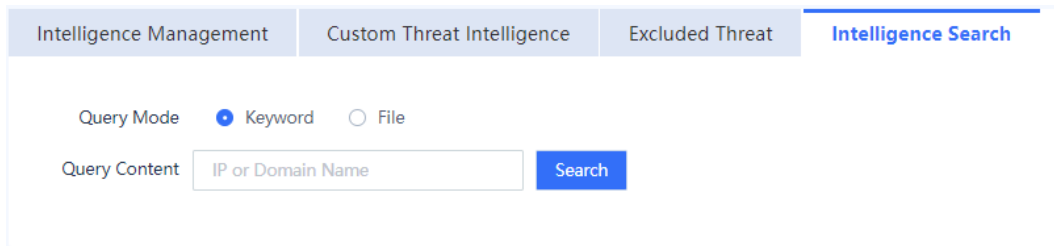
Use the threat intelligence query function to check whether a specific IP address or domain name matches threat intelligence and view the source of threat intelligence.

i Note

The query scope of threat intelligence includes available threat intelligence signature libraries and custom threat intelligence on the current device. If the threat intelligence license is not activated or has expired, the corresponding threat intelligence signature library is unavailable.

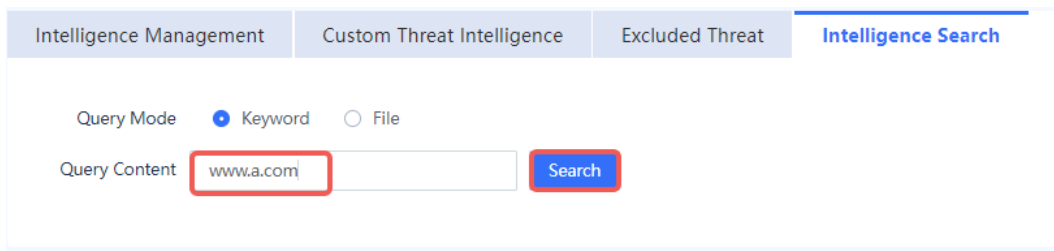
- Querying a Single Threat Intelligence Entry

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



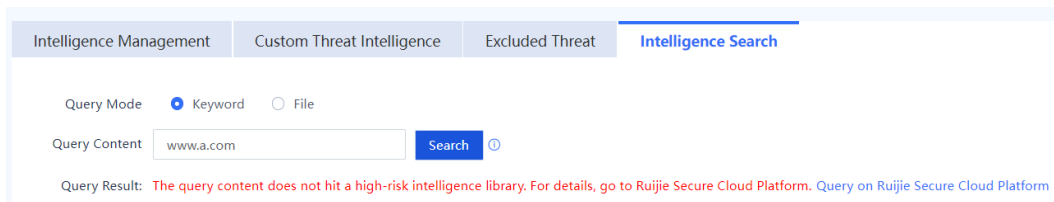
The screenshot shows the 'Intelligence Search' tab selected in the navigation bar. Below the navigation bar, there are two radio buttons for 'Query Mode': 'Keyword' (selected) and 'File'. Below that is a text input field labeled 'Query Content' containing the placeholder text 'IP or Domain Name' and a blue 'Search' button.

(2) On the **Intelligence Search** tab page, click **Keyword** and enter the IP address or domain name to be queried in the **Query Content** input box.



The screenshot shows the 'Intelligence Search' tab selected. The 'Query Mode' radio buttons are still visible. The 'Query Content' input field now contains the text 'www.a.com', which is highlighted with a red box. The 'Search' button is also highlighted with a red box.

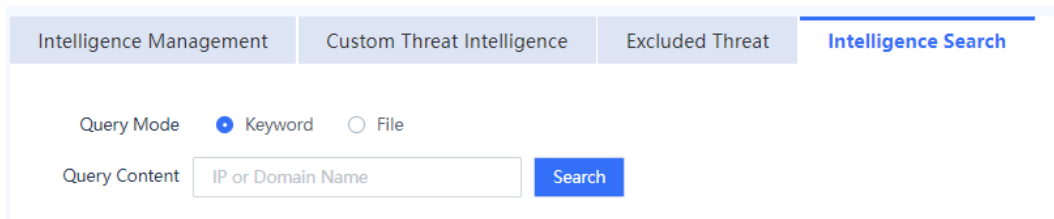
(3) Click **Search** and wait for the system to return the query result.



The screenshot shows the 'Intelligence Search' tab selected. The 'Query Content' input field contains 'www.a.com' and the 'Search' button is highlighted with a blue circle. Below the input field, a red message reads: 'Query Result: The query content does not hit a high-risk intelligence library. For details, go to Ruijie Secure Cloud Platform. Query on Ruijie Secure Cloud Platform'.

- Importing a File for Batch Query

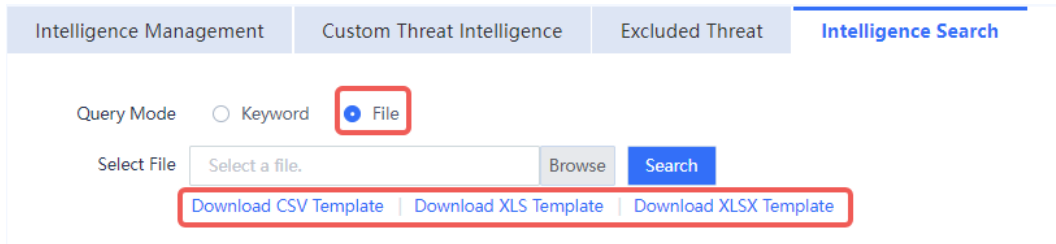
(1) Choose **Policy > Security Defense > Threat Intelligence > Intelligence Search**.



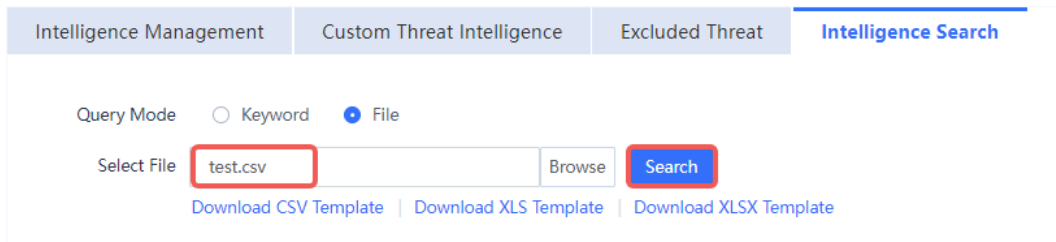
The screenshot shows the 'Intelligence Search' tab selected. Below the navigation bar, there are two radio buttons for 'Query Mode': 'Keyword' (selected) and 'File'. Below that is a text input field labeled 'Query Content' containing the placeholder text 'IP or Domain Name' and a blue 'Search' button.

(2) On the **Intelligence Search** tab page, set **Query Mode** to **File**.

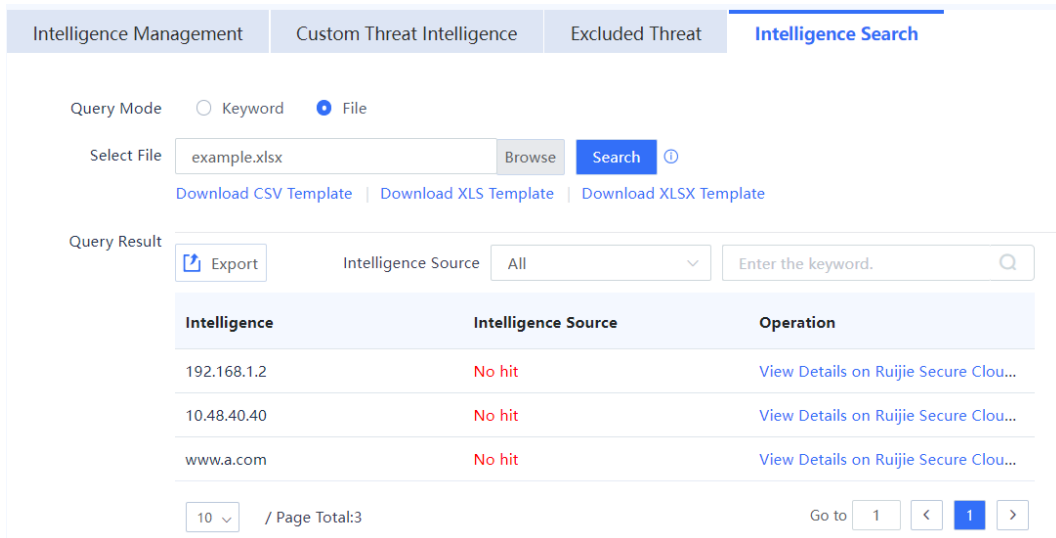
(3) Click a link to download a file template. CSV, XLS, and XLSX file formats are supported.



- (4) Enter the IP addresses or domain names to be queried in the file template and save the edited file.
- (5) Return to the web UI, click **Browse**, select the edited file, and click **Search**.



- (6) Wait for the system to return the query result. The result is displayed in a list at the bottom of the page.



Follow-up Procedure

- Click **Export** to export the query result.
- You can filter the query result based on the value of **Intelligence Source** and keyword in threat intelligence.

6. Viewing Threat Intelligence Logs

Application Scenario

When a malicious connection matches the threat intelligence, a security log is generated, and the log type is **Threat Intelligence**. By checking the logs, you can view the specific attack information and matched threat intelligence type, helping you take further actions.

Procedure

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

Security Log

Export Refresh Export All Search Criteria Enter an IP address or a port number.

Search Criteria: Time: 2023-12-13 00:00:00 -- 2023-12-13 23:59:59 Severity: High,Medium,Low x Clear

No.	Severity	Security Event	Log Type	Attack Type	Defense Rule	Time	Src. Address	Dest. Address	App	Action	Operation
1	High	EICAR-Test-File	Virus Protection	Malware	0	2023-12-13 15:51:02	172.168.1.2	172.168.2.2	HTTP-BROWSE	Permit	View Details
2	High	EICAR-Test-File	Virus Protection	Malware	0	2023-12-13 11:16:11	2001:db8:1:2	2001:db8:3:2	HTTP-BROWSE	Permit	View Details
3	High	EICAR-Test-File	Virus Protection	Malware	0	2023-12-13 11:16:03	2001:db8:1:2	2001:db8:3:2	HTTP-BROWSE	Permit	View Details
4	High	EICAR-Test-File	Virus Protection	Malware	0	2023-12-13 11:15:44	2001:db8:1:2	2001:db8:3:2	HTTP-BROWSE	Permit	View Details
5	High	EICAR-Test-File	Virus Protection	Malware	0	2023-12-13 11:15:25	2001:db8:1:2	2001:db8:3:2	HTTP-BROWSE	Permit	View Details
6	High	EICAR-Test-File	Virus Protection	Malware	0	2023-12-13 11:15:06	2001:db8:1:2	2001:db8:3:2	HTTP-BROWSE	Permit	View Details
7	High	EICAR-Test-File	Virus Protection	Malware	0	2023-12-13 11:10:10	2001:db8:1:2	2001:db8:3:2	HTTP-BROWSE	Permit	View Details
8	High	EICAR-Test-File	Virus Protection	Malware	0	2023-12-13 11:09:51	2001:db8:1:2	2001:db8:3:2	HTTP-BROWSE	Permit	View Details
9	High	EICAR-Test-File	Virus Protection	Malware	0	2023-12-13 11:09:32	2001:db8:1:2	2001:db8:3:2	HTTP-BROWSE	Permit	View Details
10	High	EICAR-Test-File	Virus Protection	Malware	0	2023-12-13 11:09:14	2001:db8:1:2	2001:db8:3:2	HTTP-BROWSE	Permit	View Details

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

Security Log Details ✕

Exclude

Src.

Src. Security Zone: trust

Src. IP: 203.0.114.2

Src. Port: 58281

MAC: 52:54:00:d8:1b:81

User:

Custom-Custom Intelligence

→

Dest.

Dest. Security Zone: zone4

Dest. IP: 203.0.113.2

Dest. Port: 80

App: ApplicationBeingIdentified

Basic Info

Time: 2023-11-16 19:23:18	Type: Custom-Custom Intelligence
Security Event: test2	Direction: WAN-to-LAN
Severity: High	Action: Deny
Blocking Duration: 0s	Defense Rule: 0
Security Policy Name: Threat Intelligence	Intelligence Source: Custom
Domain Name/IP: 203.0.114.2	

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

Note

For more information and configurations about the fields in security logs, see [9.3.2 Querying Security Logs](#).

8.4 Content Identification Library

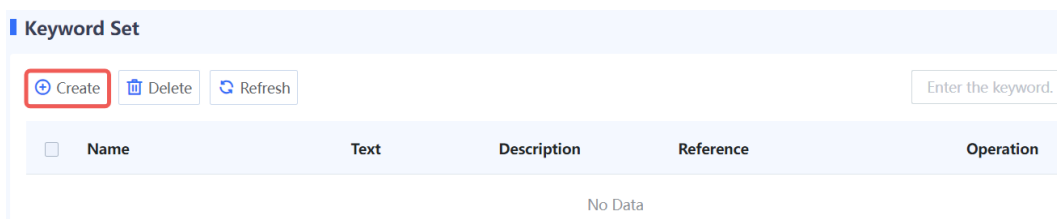
8.4.1 Configuring a Keyword Set

Application Scenario

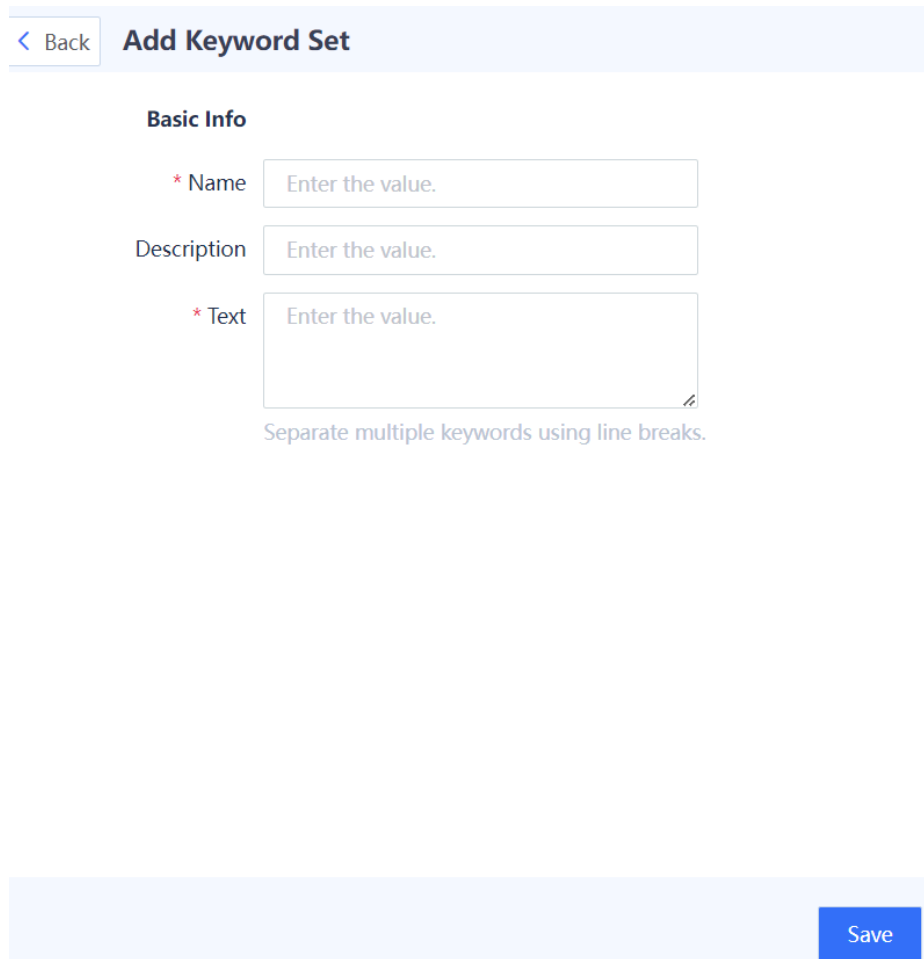
Configure a keyword set to specify the keyword text for filtering. The keyword set can be used together with a keyword filtering template to block or generate an alarm for traffic containing keywords. For details about the keyword filtering template, see [8.6 Keyword Filtering](#).

Procedure

- (1) Choose **Object > Content Identification Lib. > Keyword Set**.
- (2) Click **Create**.



- (3) Configure a keyword set.



Item	Description	Remarks
Basic Info		
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.

8.4.2 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 [8.5 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 [3 License Activation](#).

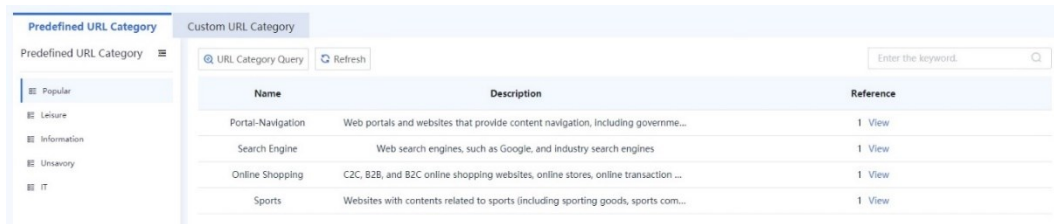
Note

- 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.



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

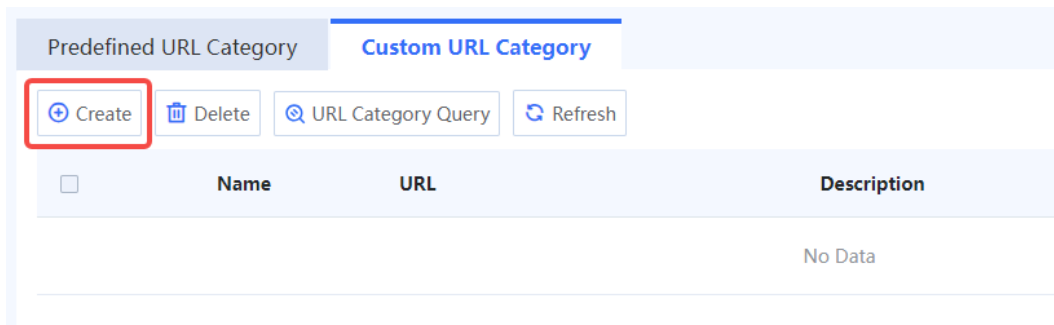
3. Configuring a Custom URL Category

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.**



Name	URL	Description
No Data		

- (3) Enter URL category information.

< Back

Create Custom URL Category

Basic Info

* Name

Description

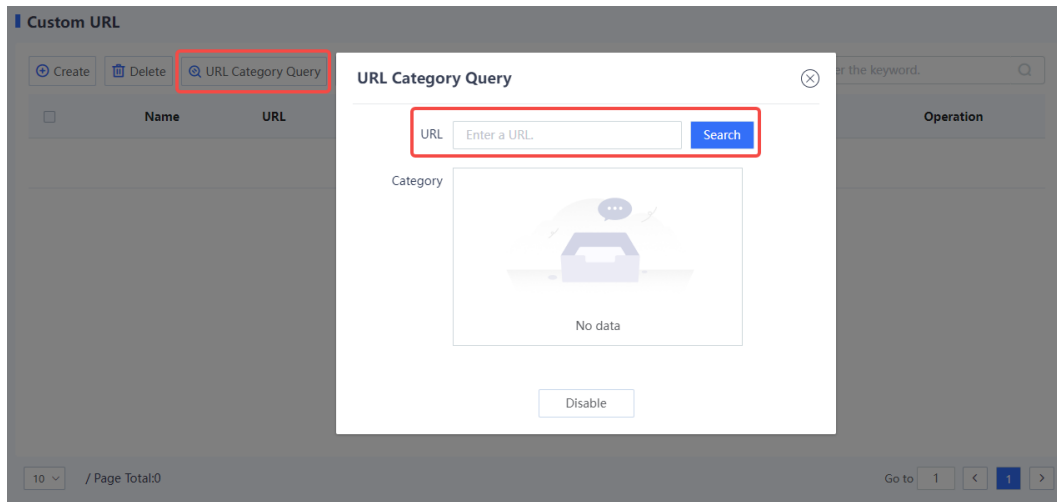
① URL

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

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

Follow-up Procedure

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



8.5 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 [8.12 Security Policy](#).

Precautions

- To detect HTTPS-based URLs, you need to configure an SSL proxy policy. For details about SSL proxy, see [8.9 Configuring SSL Proxy Policies](#).
- After you configure custom URL categories, URLs that are not in the custom categories are classified as uncategorized. When detecting traffic that accesses uncategorized URLs, the device processes the traffic according to the action set for uncategorized URLs.

8.5.1 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.

< Back

Create URL Filtering

Basic Info

* Template Name

Description

Blocklist and Allowlist

URL Allowlist

Allowlists take precedence over blocklists.

URL Blocklist

Allowlists take precedence over blocklists.

URL Filtering

Name	<input type="radio"/> Permit ⌵	<input type="radio"/> Alarm ⌵	<input type="radio"/> Block ⌵
> Popular	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> Business-Economy	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> IT	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> Information	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> Leisure	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> Life	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> Policy-Law	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> Science-Art	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> House	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> Transportation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
> Unsavory	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Uncategorized	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Save

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

Item	Description	Remarks
URL Allowlist	<p>After a URL is added to an allowlist, the device directly permits traffic that accesses the URL.</p> <p>URL allowlists take precedence over URL blocklists.</p> <p>Note:</p> <p>Multiple URLs can be entered. A URL can contain the wildcard character (*). Enter one URL per line. Press Enter to separate lines.</p> <p>If a URL contains the pound sign (#), the sign and the string after the sign do not take effect for matching. For example, if www.test.com/#123 is configured, all the domain names that start with www.test.com/ will be matched.</p> <p>If a URL contains the characters http:// or https://, these characters will be automatically removed during matching.</p> <p>If an IPv6 address is configured as a URL, the input format should be <i>[IPv6 address]</i>. For example, [2001::1].</p>	<p>[Example]</p> <p>www.abc1.com</p>
URL Blocklist	<p>After a URL is added to a blocklist, the device directly blocks traffic that accesses the URL. The input format is the same as that for the URL allowlist.</p>	<p>[Example]</p> <p>www.abc2.com</p>
URL Filtering		
URL Filtering	<p>Set processing actions for different URL categories:</p> <p>Permit: Permit traffic that accesses the URLs of the specific categories.</p> <p>Alarm: Permit traffic that accesses the URLs of the specific categories and generate an alarm log.</p> <p>Block: Block traffic that accesses the URLs of the specific categories and generate an alarm log.</p>	N/A

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

Follow-up Procedure

- Virus detection can be triggered only after a custom URL filtering template is referenced by a security policy. For details about security policies, see [8.12 Security Policy](#).

8.5.2 Predefined URL Filtering Template

Prerequisites

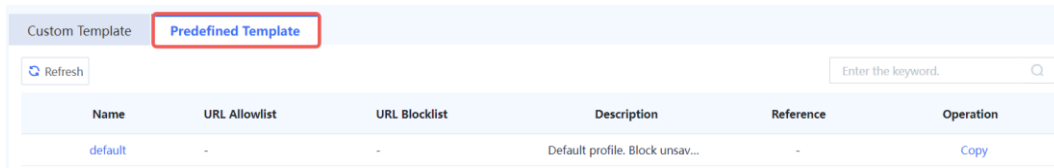
After a license is activated for the device, a default filtering template is displayed on the **Predefined Template** tab page. For details about license activation, see [3 License Activation](#).

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

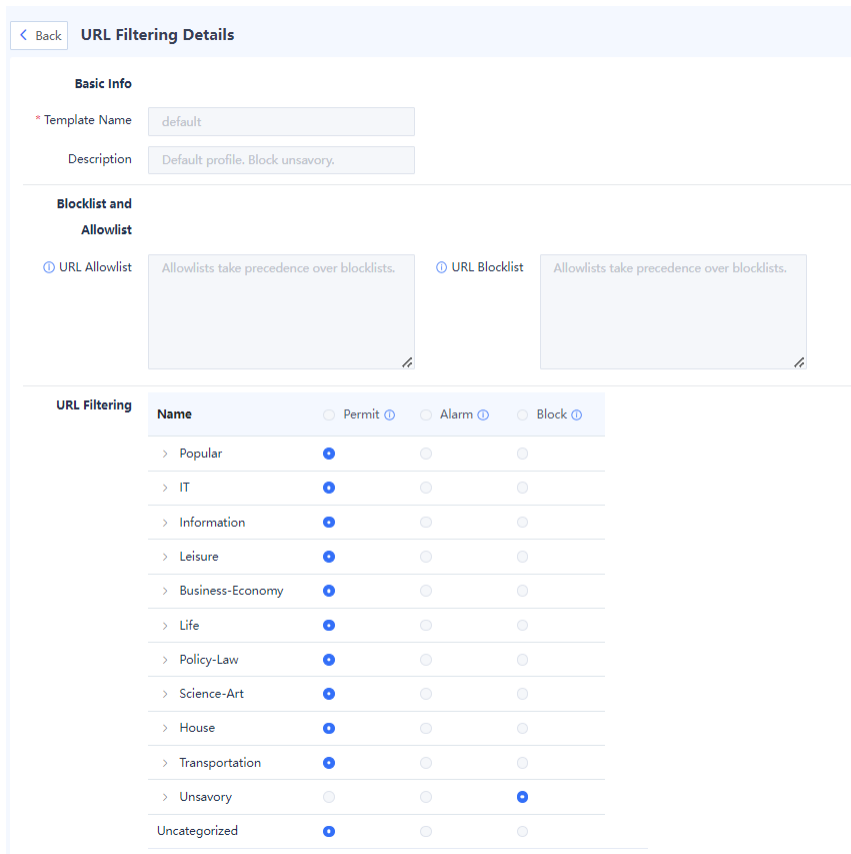
Procedure

(1) Check the predefined URL filtering template.

a Choose **Object > Content Template > URL Filtering > Predefined Template**.

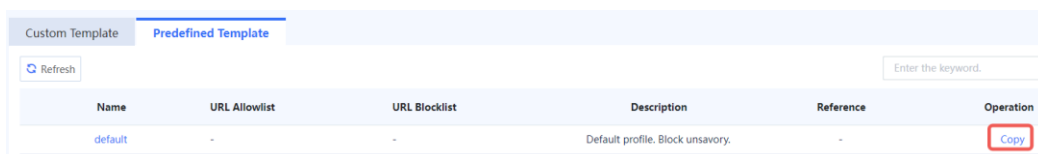


b Click a template name to view URL filtering details.



(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 [8.12 Security Policy](#).

8.5.3 Configuration Examples of Blocking Websites

1. Applicable Products and Versions

Table 8-15 Products and Versions

Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	All versions

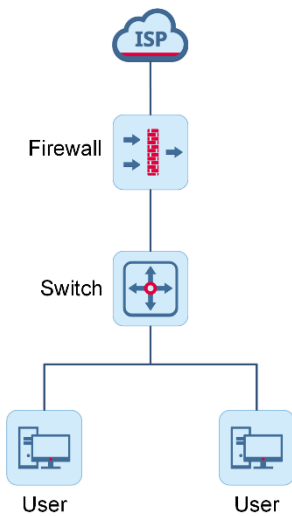
2. Service Demands

A firewall is deployed at the egress of an internal network in routing mode. The network administrator wants to configure URL filtering to block access traffic to specified web pages. The specific requirements are as follows:

- Block frequently visited websites, such as Google and YouTube.
- Block websites of a certain type, such as gaming and gambling websites.
- Block a custom website, which may be a niche website.

3. Topology

Figure 8-5 Topology



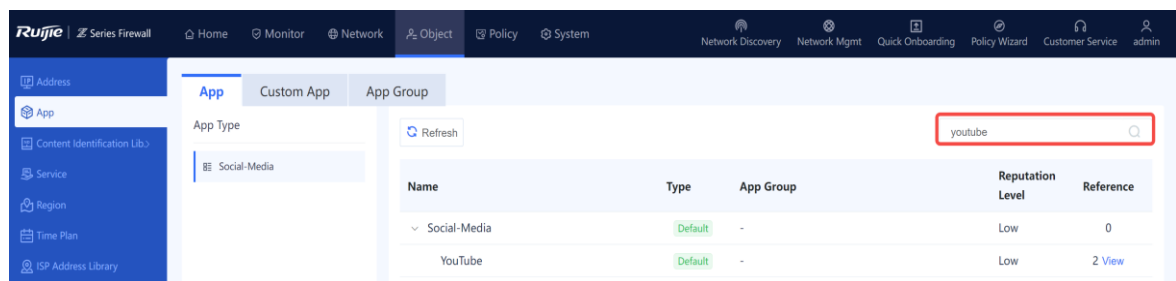
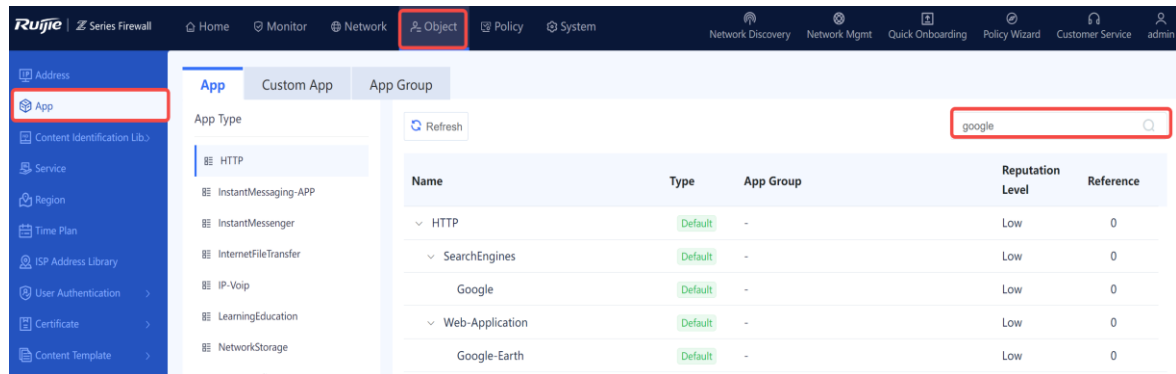
4. Restrictions and Guidelines

The basic network configurations, such as the interface IP addresses and default routes, have been completed on the firewall.

5. Configuration Roadmap

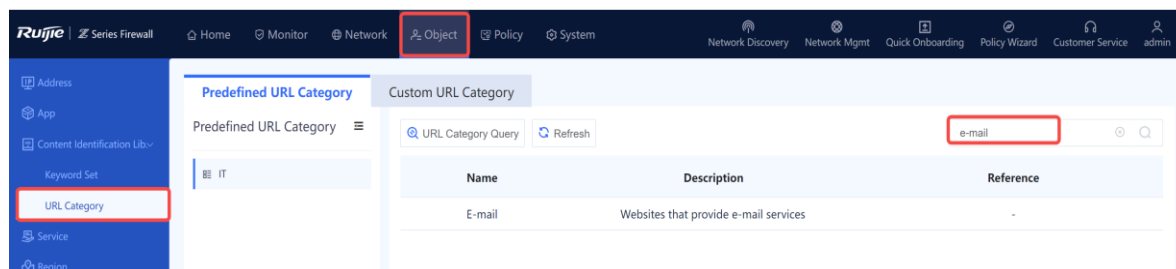
- **Blocking a Well-Known Website**

The built-in application identification library of the firewall already includes common applications and websites (well-known websites are also considered applications by the firewall). If you want to block a website, search for the website name in the application library and check whether the website name already exists. For example, you can directly call the names of well-known websites such as Google and YouTube in the application identification library.

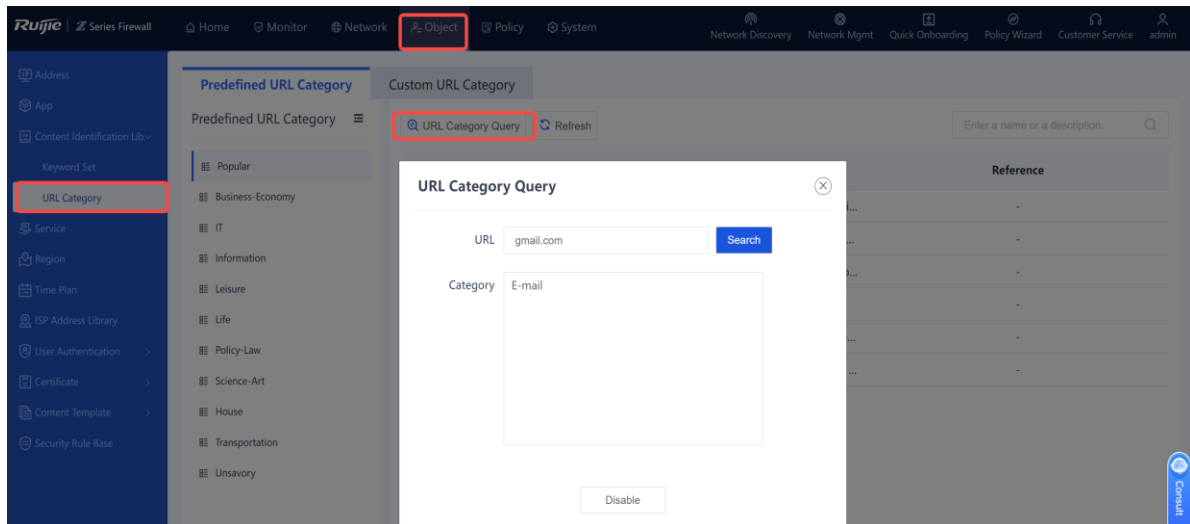


● **Blocking Websites of a Certain Type**

To block websites of a certain type, search for the website type in the built-in URL category. For example, to block email websites, search for **email** in **URL Category**.



To further confirm whether the website to be blocked is in this category, you can enter the website name.



- **Blocking a Customized Website**

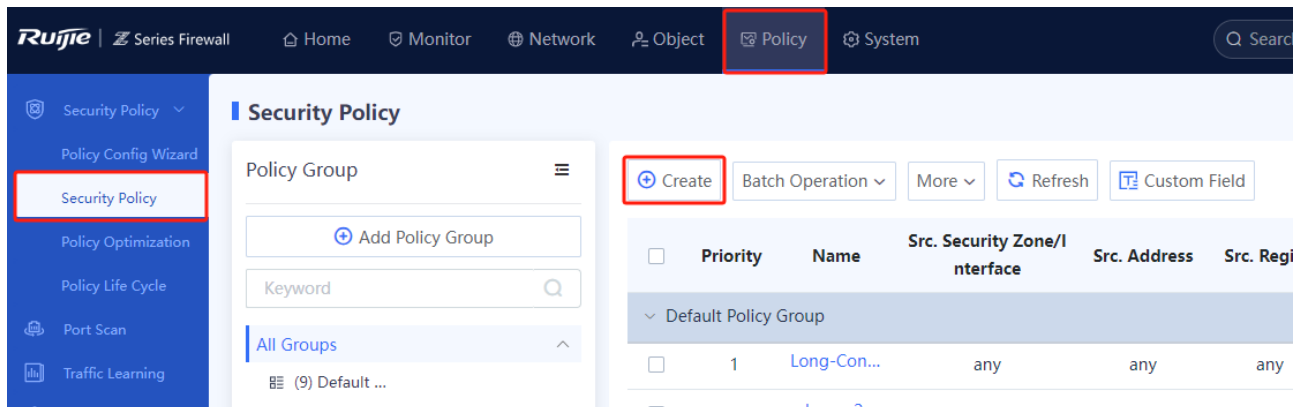
If you want to block a customized website but it does not exist in the application library or URL category, you can perform either of the following configurations:

- If the IP address of the website is not fixed but the website URL is definite, you can configure a customized URL.
- If the website IP address is fixed, you can configure a custom application to block the website.

6. Procedure

- **Blocking Websites Such as YouTube**

(1) Choose **Policy > Security Policy** and click **Create** to create a policy.



(2) Read the pop-up window and decide whether to create a policy in the simulation space as required. In this example, click **Create**.

Tip



Are you sure you want to add it in the simulation space?

The policy execution process can be simulated before actual execution. The simulation helps you identify vulnerabilities and issues in policies in advance and avoid risks to services in actual execution.

Do Not Show This Again



- (3) Configure the basic information of the security policy.
 - o Enter a policy name, for example, **BlockYoutube**.
 - o Retain the default **Enable** state for **Enabled State**.
 - o Set **Policy Group** to **Default Policy Group**. You can select a custom policy group as required.
 - o Set **Priority** as required. A policy at the top of the list indicates a higher matching priority.

* Name

Enabled State Enable

* Policy Group [+ Add Group](#)

* Priority

Description

- (4) Set **Src. and Dest.** parameters to any (more specific matching conditions can be configured in actual scenarios) and set **Action Option** to **Deny**.

Src. and Dest.

Src. Security

Zone/Interface

* Src. Address

Src. Region

Dest. Security

Zone/Interface

* Dest. Address

Dest. Region

Service

Action Option Permit Deny

App, User, Effective Time

- (5) Click **App, User, Effective Time** to display the application selection page.
- (6) Click the drop-down list box next to **App**, search for and select YouTube in the displayed dialog box.

App ⊗

To-be-selected (7207)

Select

- ▾ Social-Media
 - YouTube

[⊕ Add App Group](#) [⊕ Add Custom App](#)

Selected (1) [Clear](#)

Enter app or app group name.

YouTube 🗑

- (7) Click **Confirm** to make the configuration take effect.
- (8) Set **User, Service, Src, Effective Time**, and other parameters to **any**, as shown in the following figure, since the restriction needs to take effect for all users at any time in this example. In actual scenarios, you can set the parameters as required.

Src. and Dest.

Src. Security

Zone/Interface

* Src. Address

Src. Region

Dest. Security

Zone/Interface

* Dest. Address

Dest. Region

Service

App

User

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

Action Option Permit Deny

[Fold](#) ^

Save

(9) After configuration, click **Save**.

● **Blocking a Custom Website Through URL Filtering**

- (1) If the website can be searched in the predefined URL category, skip this step and go to step 2. Otherwise, you need to create this custom website category as follows:
 - a Choose **Object** > Content Identification Lib. > **URL Category** > **Custom URL Category**.
 - b Click **Create**, enter a name and website URLs in the **URL Category**.

Ruijie | Series Firewall | Home | Monitor | Network | **Object** | Policy | System | Network Discovery

URL Category

[Back](#) **Edit Custom URL Category**

Basic Info

* Name

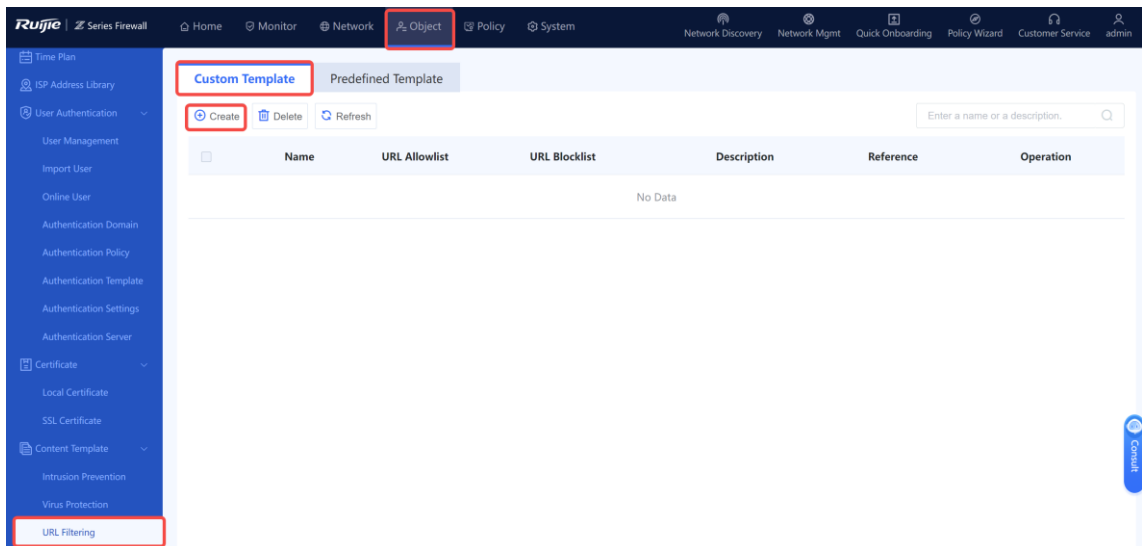
Description

URL

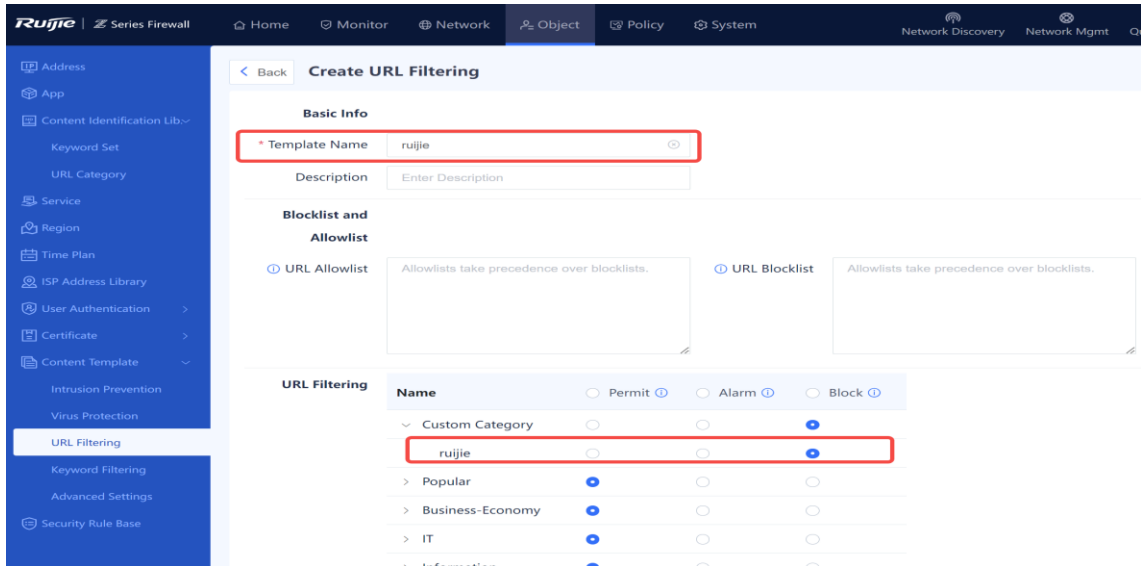
Note

- (1) 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]**.

- (2) In **URL Filtering**, create a user-defined template and associate it with the URL category created in the previous step.
 - a Choose **Object > Content Template > URL Filtering > Custom Template**.
 - b Click **Create**.



- c Enter the template name, select the created URL category in the **URL Filtering** area, and set the action to **Block**.

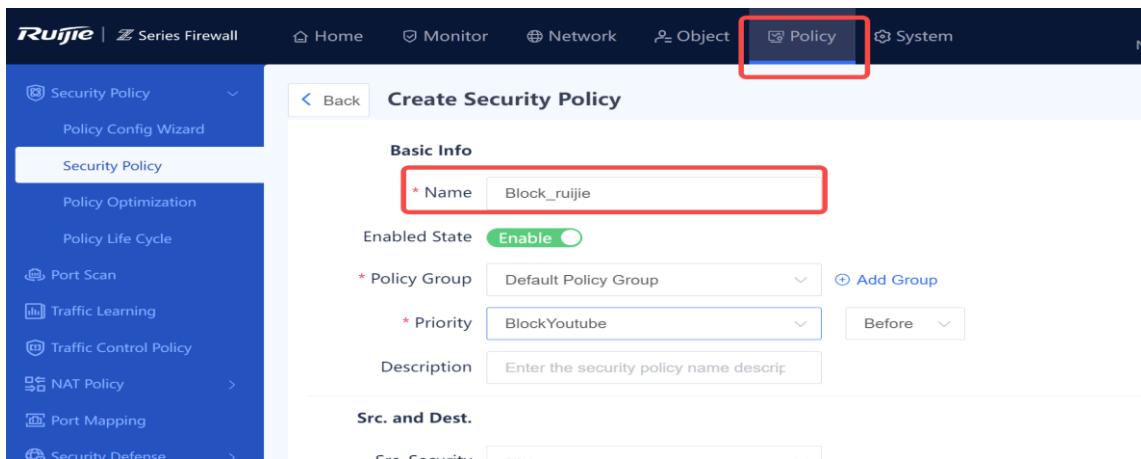


(3) Create a security policy and enable URL filtering.

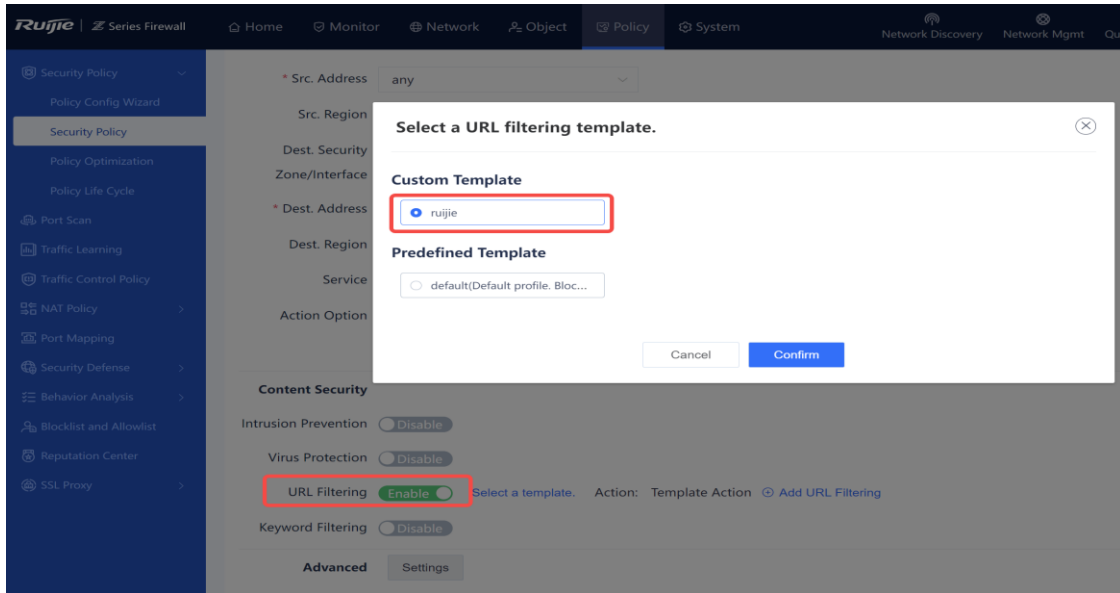
a Choose **Policy > Security Policy > Security Policy**, and click **Create**.

b Configure a security policy and set key parameters as follows:

- o Enter a policy name, for example, Block_ruijie.
- o Retain the default **Enable** state for **Enabled State**.
- o Set **Policy Group** to **Default Policy Group**. You can select a custom policy group as required.
- o The **Priority** can be set as required. A policy at the top of the list indicates a higher matching priority.
- o Set **Src. and Dest.** parameters to any (more specific matching conditions can be configured in actual scenarios) and set **Action Option** to **Permit**.



- o Toggle on **URL Filtering**, set **Custom Template** to the created URL filtering profile, and set **Action** to **Template Action**.

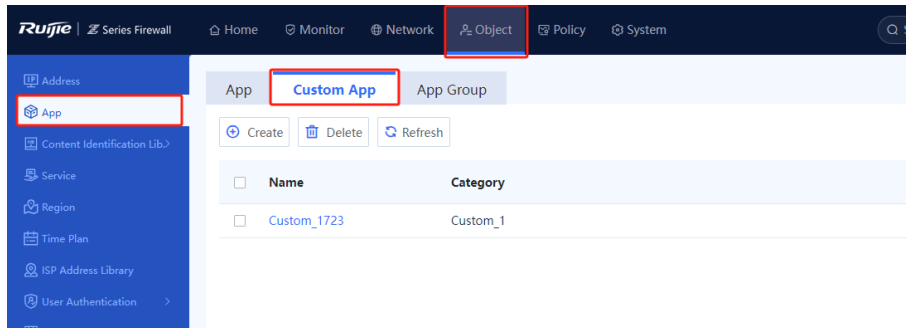


c After completing the configuration, click **Save**.

- **Blocking Certain Websites by Customizing Applications**

If the website IP address to be blocked is fixed, you can configure a custom application to block the website IP address. The configuration steps are as follows:

(1) Choose **Object > App > Custom App** and click **Create** to create a custom application.



(2) Enter the custom application name and category name, and click **Create** to create an **App Rule**.

Add Custom App



* Name

Category Custom Type Select from existing categories.

* Category Name

* App Rule

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

- (3) Set **Protocol Type** and other parameters based on actual requirements, and click **Confirm**.

Create Custom App Rule



Protocol Type TCP UDP

*

Number range: 0-65535

*

icates any

*

- (4) Click **Confirm**. The custom application is created.

Add Custom App



* Name

Category Custom Type Select from existing categories.

* Category Name

* App Rule

Protocol Type	Src. IP	Dest. IP	Dest. Port	Operation
TCP	0.0.0.0/0	128.34.21.0/24	65535	Edit Delete

(5) Set **App** to the created custom application by referring to the process of creating a security policy.

Src. and Dest.

Src. Security

Zone/Interface

* Src. Address

Src. Region

Dest. Security

Zone/Interface

* Dest. Address

Dest. Region

Service

App

User

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

Action Option Permit Deny

[Fold](#) ^

7. Verification

Check the security policy to verify that the packets match the predefined security policy.

<input type="checkbox"/>	Priority	Name	Src. Security Zone/Interface	Src. Address	Src. Region	Dest. Security Zone/Interface	Dest. Address	Dest. Region	Service	
▼ Default Policy Group										
<input type="checkbox"/>	1	BlockYou...	any	any	any	any	any	any	any	<input checked="" type="checkbox"/>

8.6 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 [8.12 Security Policy](#).

Procedure

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

Keyword Filtering

<input type="checkbox"/>	Name	Description	Reference	Operation
No Data				

- (3) Enter keyword filtering template information.

[Back](#) **Add Keyword Filter**

Basic Info

* Template Name

Description

* Filter Rule

<input type="checkbox"/>	Name	Application Protocol	Keyword Set	Direction	Action	Operation
No Data						

Total: 0

Item	Description	Remarks
Basic Info		

Item	Description	Remarks
Template Name	Name of the keyword filtering template.	Characters such as `~!#%^&*+ \{};:","/<>? and spaces are not allowed. [Example] Template_1
Description	Description of the keyword filtering template.	Characters such as `~!#%^&*+ \{};:","/<>? are not allowed. [Example] Template_1
Filter Rule		
Rule Name	Name of the filter rule.	Characters such as `~!#%^&*+ \{};:","/<>? and spaces are not allowed. [Example] RULE_1
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 8.4.1 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

- Detection can be triggered only after a keyword filtering template is referenced by a security policy. For details about security policies, see [8.12 Security Policy](#).
- To delete a filtering template, you need to delete the reference to the template in the security policy first.

8.7 Behavior Analysis

1. Configuring an Analysis Policy

Application Scenario

Configure an analysis policy to perform analysis and generate logs based on user online behaviors to facilitate subsequent tracing and analysis. Content types that support analysis include URL, instant messaging (IM), email, search engine, Weibo posting, forum posting, and files.

Precautions

- When analyzing the content of websites based on HTTPS, you must configure an SSL proxy policy first. For details about SSL proxy, see [8.9 Configuring SSL Proxy Policies](#).
- The device predefines two analysis policies: The **default_recommended** policy is used to perform analysis based on the predefined default template and analyze all types except files. The **default_all** policy is used to perform analysis on all types including files. File analysis consumes a lot of resources and affects device performance. Therefore, **default_recommended** has a higher priority than **default_all**. You can only view the two policies and cannot delete or modify them. A custom analysis policy has a higher priority than a predefined analysis policy.

Procedure

- (1) Choose Policy > Behavior Analysis > Analysis Policy.
- (2) Click Create.

The screenshot displays the 'Analysis Policy' management page. At the top, there is a notification: 'SSL proxy must be enabled to analyze HTTPS website content.' Below this is a toolbar with buttons for 'Create', 'Delete', 'Enable', 'Disable', 'Move', 'Clear Hit Record', 'Custom Field', and 'Refresh'. A search input field is also present with the placeholder text 'Enter a name or an analysis template.' The main area contains a table with the following data:

Policy Name	Analysis Template	Description	Src. Address	User/User Group	Hit Count	Operation
default_reco..	default_reco...	Analyze common services	any	any	0 Clear	<input checked="" type="checkbox"/> View Delete
default_all	Analyze All	Analyze all services	any	any	0 Clear	<input checked="" type="checkbox"/> View Delete

- (3) Configure an analysis policy.

< Back
Add Analysis Policy

Basic Info

* Name

Enabled State Enable Disable

Description

Src. Address

Src. Address

User

User/User Group

Analyze

Action Analyze All Analyze by Template Not Analyze

Analysis Template [Template:Select a template.](#) [Add Analysis Template](#)

Advanced Settings

Src. Security Zone

Dest. Security Zone

Dest. Address

Services and Apps

Service

App

Time Range

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

Item	Description	Remarks
Basic Info		
Name	Name of an analysis policy.	Characters such as `~!#%^&*+\\{ };:;"/<>? and spaces are not allowed. [Example] Test
Enabled State	Enable or disable the analysis policy.	[Example] Enable
Description	Description of an analysis policy.	Characters: `~!#%^&*+\\{ };:;"/<>? are not allowed. [Example] Analysis Template

Item	Description	Remarks
Src. Address	Source IP address for analysis.	Select a value from the drop-down list or add a new address.
User/User Group	User or user group for analysis.	Select a value from the drop-down list or add a new user or user group.
Analyze		
Action	<ul style="list-style-type: none"> ● Analyze All: analyzes all traffic that passes through the device and records logs. ● Analyze by Template: performs analysis based on the analysis type and analysis content defined in the template and records logs. ● Not Analyze: does not analyze the traffic that passes through the device. 	[Example] Not Analyze
Analysis Template	Analysis template referenced by the analysis policy.	This parameter is mandatory when Action is set to Analyze by Template .
(Optional) Advanced Settings		
Src. Security Zone	Source security zone of the analysis content.	Select a value from the drop-down list or add a new security zone.
Dest. Security Zone	Destination security zone of the analysis content.	Select a value from the drop-down list or add a new security zone.
Dest. Address	Destination address of the analysis content.	Select a value from the drop-down list or add a new address.
Service	Service to which the analysis content belongs.	Select a value from the drop-down list or add a new service.
App	Application to which the analysis content belongs.	Select a value from the drop-down list or add a new application.
Time Range	Time when the analysis policy takes effect.	Select a value from the drop-down list or add a new time plan.

(4) Click **Save**.

Follow-up Procedure

- Click **Create** to add more analysis policies.
- Select an analysis policy and click **Delete** to delete the policy.
- Select an analysis policy and click **Enable** to enable the policy or click **Disable** to disable the policy.
- Select an analysis policy and click **Move** to move a policy. The policy listed before has a higher 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.

2. Configuring an Analysis Template

Application Scenario

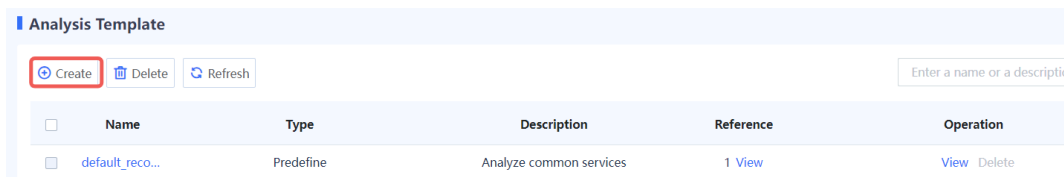
Configure the analysis content using an analysis template. The detection mechanism can be triggered only when the analysis template is referenced by an analysis policy. For details about analysis policies, see [1. Configuring an Analysis Policy](#).

Precautions


- The device predefines the default analysis template default_recommended, which can be viewed only but cannot be deleted or modified.
- To delete a custom analysis template, you need to delete the reference to the template in the analysis policy first.

Procedure

- (1) Choose Policy > Behavior Analysis > Analysis Template.
- (2) Click Create.



- (3) Configure an analysis template.

Toggle on or off  to enable or disable analysis for a specific type.

< Back
Add Analysis Template

Basic Info

* Template Name

Description

Analysis Types

URL

IM

Search Engine

Webmail

Analysis Content Recipient, Sender, Body, Attachment Name Attachment Content

Client Email

Analysis Content Recipient, Sender, Body, Attachment Name Attachment Content

Forum

Analysis Content Account, Title, Body, Attachment Name Attachment Content

Weibo

Analysis Content Account, Title, Body, Attachment Name Attachment Content

FTP

Analysis Content Uploaded/Downloaded File Name Uploaded File Content Downloaded File Content

HTTP File Transfer

Analysis Content Uploaded File Name Downloaded File Name Uploaded File Content

After HTTP file transfer is enabled, many log records will be generated. Enable it with caution.

Save

Item	Description	Remarks
Basic Info		
Template Name	Name of the analysis template.	[Example] Test
Description	Description of the analysis template.	[Example] Audit Template
Analysis Types		
URL	Users access web pages.	[Example] Enable
IM	Users log in to and log out from IM software.	[Example] Enable
Search Engine	Users use search engines to search for	[Example]

Item	Description	Remarks
	content.	Enable
Webmail	Users send emails through web mailboxes. Select analysis content as required.	[Example] Enable
Client Email	Users send emails using an email client. Select this item as required.	[Example] Enable
Forum	Users access a forum and post in the forum. Select this item as required.	[Example] Enable
Weibo	Users log in to Weibo and post content. Select this item as required.	[Example] Enable
FTP	Users transfer files through FTP. Select this item as required.	[Example] Enable
HTTP File Transfer	Users transfer files through HTTP. Select this item as required.	[Example] Enable

(4) Click **Save**.

3. Configuring an Analysis Allowlist

Application Scenario

To exempt specific users, applications, or URLs on the network from analysis, you can configure allowlists for the corresponding users, applications, or URLs.

Procedure

- (1) Choose Policy > Behavior Analysis > Analysis Allowlist.
- (2) Select an allowlist type as required and configure an allowlist.

(3) Click **OK**.

4. Viewing Analysis Logs

View analysis logs to check the analysis configuration. For details about analysis logs, see [9.3.4 Querying Behavior Analysis Log](#).

5. Upgrading the Behavior Analysis Signature Library

The behavior analysis signature library is updated continuously. You can upgrade the signature library to improve content analysis capabilities.

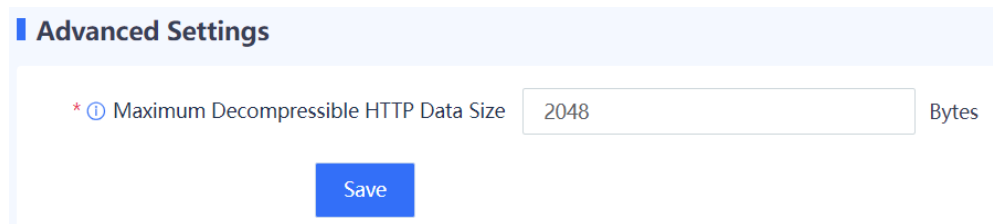
8.8 Configuring HTTP Packet Resolution

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.

8.9 Configuring SSL Proxy Policies

8.9.1 Overview

To protect data security and privacy, traffic of many applications is encrypted by Transport Layer Security (TLS) during transmission. To detect the content of TLS encrypted traffic, the firewall needs to decrypt traffic as proxy so that the function modules such as intrusion prevention and virus protection can detect the decrypted traffic and files. Currently, the firewall can only decrypt the HTTPS encrypted traffic.

The following table describes the application scenarios of SSL proxy.

Scenario	Similarity	Difference
Client protection	The firewall sets up an SSL connection with client and server respectively, to send and receive SSL encrypted data. The firewall decrypts the encrypted data from the client, performs security	The firewall uses the temporary server certificate re-issued by the imported CA certificate to set up SSL connection with the client.

Scenario	Similarity	Difference
Server protection	check, re-encrypts the data that passes the check, and sends it to the server.	The firewall uses the imported server certificate to set up SSL connection with the client.

8.9.2 Configuring an SSL Proxy Template

Application Scenario

Configure this function if you need to perform virus protection detection or IPS detection for HTTPS encrypted traffic. The system predefines the default template, which can be directly referenced or customized according to your needs.

Note

After configuring an SSL proxy template, you need to reference it in the SSL proxy policy to decrypt traffic. The SSL proxy policy is used to set the matching conditions of packets and whether to decrypt them after they are hit. The SSL proxy template specifies how the device decrypts packets that hit the policy.

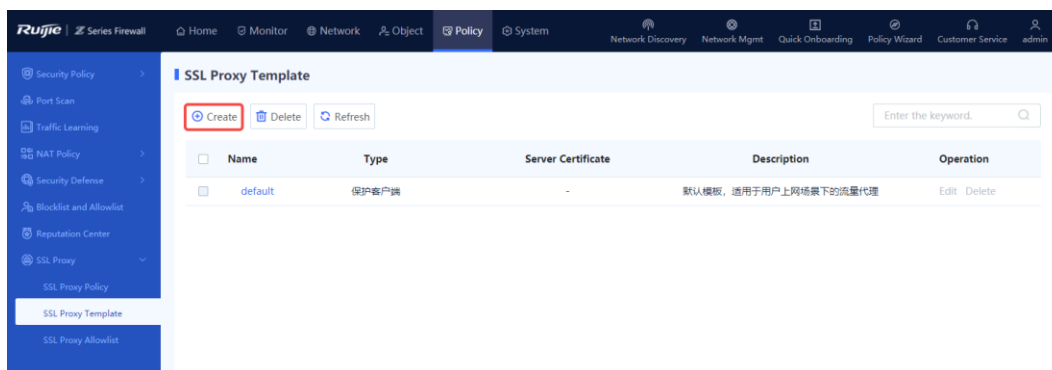
Prerequisites

If you select **Protect Client** as the SSL proxy template type, import the SSL proxy certificate (CA certificate) first. For details about SSL proxy certificate import, see [8.9.3 1. Importing SSL Proxy Certificate](#).

If you select **Protect Server** as the SSL proxy template type, import the server certificate first. For details about server certificate import, see [8.9.3 2. Importing Server Certificate](#).

Procedure

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



- (3) Enter the template name and description, select template type, and click **Save**.

Note

If the type is set as **Protect Server**, the server certificate needs to be selected.

< Back

Create SSL Proxy Template

*** Name**

Description

Type Protect Client Protect Server

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

Follow-up Procedure

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

8.9.3 Importing Certificate

1. Importing SSL Proxy Certificate

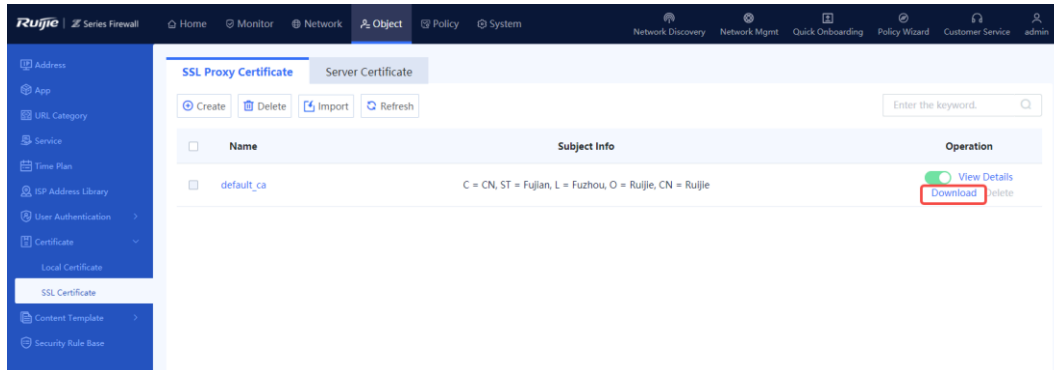
Application Scenario

If HTTPS encrypted traffic needs to be decrypted and the SSL proxy template type is set to **Protect Client**, you must import an SSL proxy certificate (that is, a CA certificate). The device provides a predefined certificate. You can also import a new certificate as needed.

Precautions

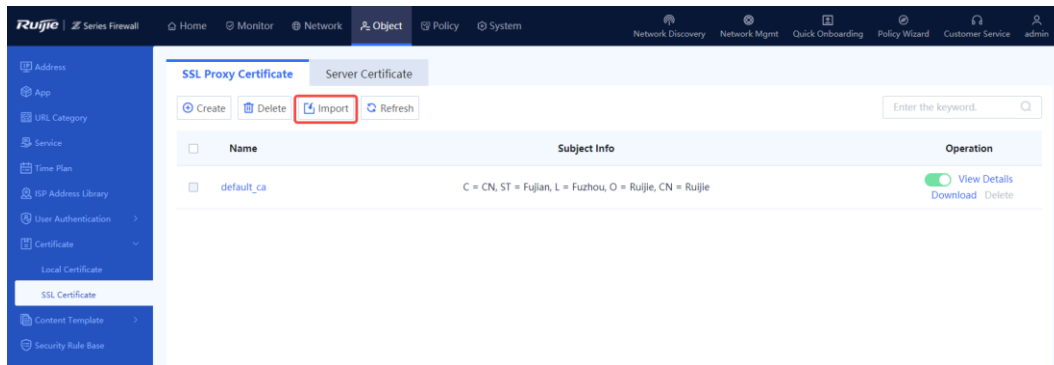
After configuring the SSL proxy certificate, click **Download** in the row where the trusted certificate resides, save the SSL proxy certificate to the local device, and then import it to the client to make the client trust it. If you do not install this certificate and the SSL proxy is enabled on the firewall, when the client accesses website by using

the browser through HTTPS, an alarm indicating that the server certificate is not issued by a trusted CA is displayed. In some cases, connection may even be directly interrupted, affecting the user's Internet access.



Procedure

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



i Note

It is recommended that you import a certificate. You can click **Create** to add a CA certificate.

- (3) Select a certificate format. Click **Browse** to upload the certificate file, enter the certificate password, and click **Confirm**.

Import SSL Proxy Certificate




* Certificate ▼
 Format

* Certificate
 File

* Password
 Password

Item	Description	Remarks
Certificate Format	Select the certificate format according to the suffix of the imported certificate file, and you can import certificates in PEM, P12, or CRT format.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Certificate with the p12 or pem suffix: You need to specify the password of the certificate when importing the certificate. Certificate with the crt suffix: When you import the certificate, specify the key file and password of the key file.

Follow-up Procedure

-  is used to configure whether to trust the SSL proxy certificate. When the icon is red, the certificate is not trusted; when the icon is green, the certificate is trusted. Click the icon to modify the credibility of the

certificate. Only one trusted SSL proxy certificate can exist on the device.

- Download the SSL proxy certificate, and import it into the client to make the client trust it.



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

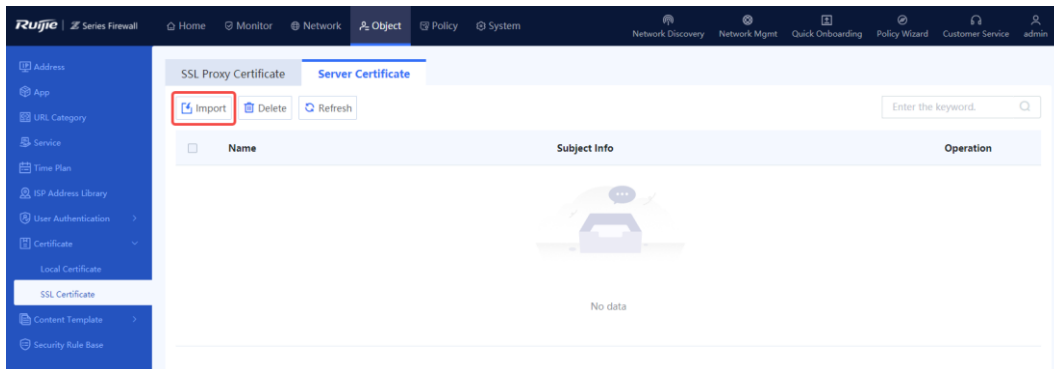
2. Importing Server Certificate

Application Scenario

If you need to decrypt the HTTPS encrypted traffic and the SSL proxy template type is set to **Protect Server**, you must import a server certificate.

Procedure

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



- (3) Select a certificate format. Click **Browse** to upload the certificate file, enter the certificate password, and click **Confirm**.

Import Server Certificate ⊗

* Certificate ▼
 Format

* Certificate
 File

* Password

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

8.9.4 Configuring an SSL Proxy Policy

Application Scenario

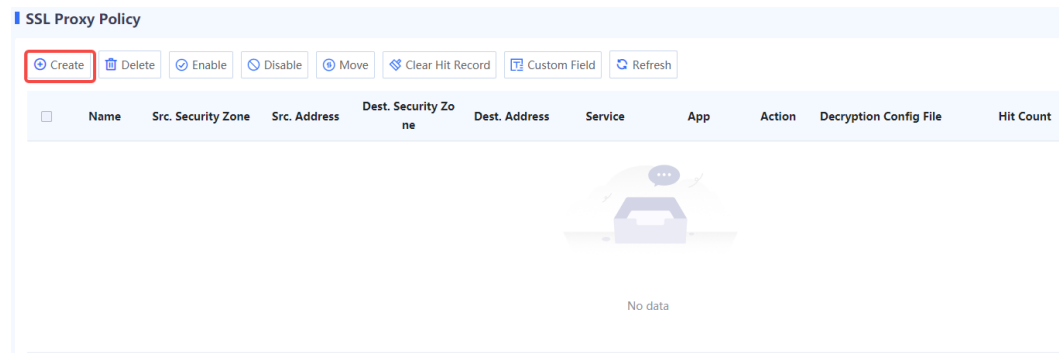
Configure this function if you need to perform virus protection detection or IPS detection for HTTPS encrypted traffic.

Prerequisites

The SSL proxy template has been created. For details about SSL proxy template creation, see [8.9.2 Configuring an SSL Proxy Template](#).

Procedure

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



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

< Back

Create SSL Proxy Policy

Basic Info

* Name

Enabled State Enable Disable

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Decryption Settings

Action Option Decrypt Not Decrypt

Item	Description	Remarks
Basic Info		
Name	Name of the SSL proxy policy.	Characters such as `~!#%^&*+V0::"/<>? and spaces are not allowed. [Example] SSLPolicy_1
Enabled State	Whether to enable the new SSL proxy policy.	[Example] Enabled

Item	Description	Remarks
Description	Description of SSL proxy policy.	Characters such as `~!#%^&*+ \ {};:'"/<>?` are not allowed. [Example] Decrypt the HTTPS encrypted traffic from security zone 1 to security zone 2.
Src. and Dest.		
Src. Security Zone	Source security zone that initiates the target data connection.	[Example] trust
Src. Address	Source address that initiates the target data connection.	Click the drop-down list, and select a source address in the To-be-selected area. The selected address is automatically added to the Selected area. [Example] Any
Dest. Security Zone	Destination security zone of the target data connection.	[Example] trust
Dest. Address	Destination address of the target data connection.	Click the drop-down list, and select a destination address in the To-be-selected area. The selected address is automatically added to the Selected area. [Example] Any
Service	Service type of the target data connection request.	[Example] Any
App	Application type of the target data connection request.	[Example] Any

Item	Description	Remarks
Action Option	Action taken by the SSL proxy policy, decrypting or not decrypting the content of target data connection. If Decrypt is selected, the SSL proxy template must be specified.	[Example] Decrypt

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

Follow-up Procedure

- View or clear the number of times a policy is hit on the **SSL Proxy Policy** page.
- To move a policy to a specified position, select the policy and click **Move**. The closer a policy is to the front, the higher its priority is in matching.

8.9.5 Allowlist

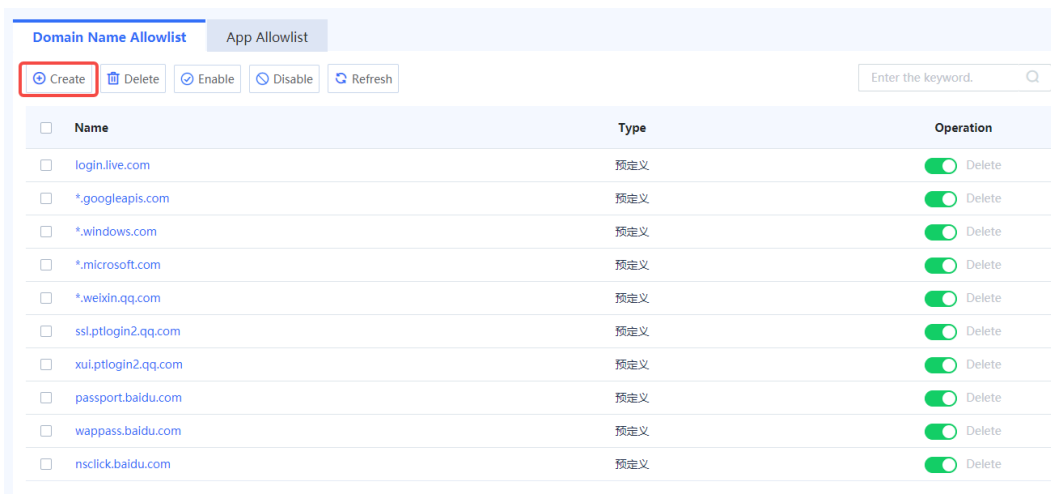
1. Domain Name Allowlist

Application Scenario

If the traffic of certain domain names does not need to be decrypted, you can add the domain names to the allowlist. The device does not decrypt the traffic of the domain names in the allowlist. The device has added the commonly used domain names and the domain names that do not need to be or cannot be accessed by SSL proxy to the allowlist. The predefined allowlist cannot be deleted, but can be forbidden according to actual situation.

Procedure

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



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

Create Domain Name Allowlist

* i Domain Name

2. Application Allowlist

Application Scenario

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

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

Procedure

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

Domain Name Allowlist **App Allowlist**

Enter the keyword.

<input type="checkbox"/> Name	Type	Operation
<input type="checkbox"/> HttpGames	预定义	Delete
<input type="checkbox"/> IPVoip	预定义	Delete
<input type="checkbox"/> OnlineGames	预定义	Delete
<input type="checkbox"/> VideoCategory	预定义	Delete
<input type="checkbox"/> SoftwareUpdates	预定义	Delete
<input type="checkbox"/> OnlineBankingPayment	预定义	Delete
<input type="checkbox"/> Videoconferencing	预定义	Delete

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

Edit App Allowlist

* App

To-be-selected (4328) Select All

- HTTP
- IPVoip
- OnlineGames
- OnlineShopping
- P2PSoftWare
- InternetFinance

Add App Group

Selected (0) Clear

app is required

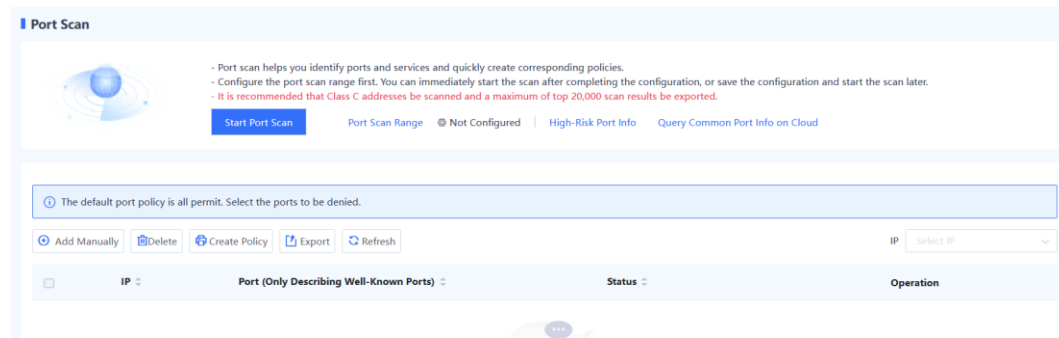
8.10 Port Scan

Application Scenario

The port scan function can help administrators quickly identify the IP address and open port information of the intranet server, and choose whether to generate security policies based on the scan results. This can help build a secure enterprise intranet.

Procedure

- (1) Choose Policy > Port Scan.



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

- a Click **Start Port Range**.

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

Tip



! Configure the port scan range first.

Configure

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

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

Note

To quickly add IP addresses, click **Quick Import from Traffic Learning** or **Quick Import from Address Object**.

Set Address Range and Port Range for Scan ⊗

ⓘ A larger number of objects will take longer scanning time. Select only necessary ports and addresses.

ⓘ Ensure that the firewall is connected to the device to be scanned and that scan traffic will not be blocked by other security devices such as an IPS.

ⓘ The scan process leads to high CPU consumption. Start the scan when the system is idle to obtain a better user experience.

Select or Add Addresses for Scan

* Add Custom IP Address/Range

IP Address/Range

No Data

Select or Add Ports for Scan

UDP Scan Yes No

Ports All Ports Custom Ports

Quick Scan

c Select or add the port to be scanned.

ⓘ **Note**

- If UDP scan is not enabled, you are advised to select **All Ports**.

Select or Add Ports for Scan

UDP Scan Yes No

Ports All Ports Custom Ports

Common Ports [Select Common Ports](#)

Custom Ports

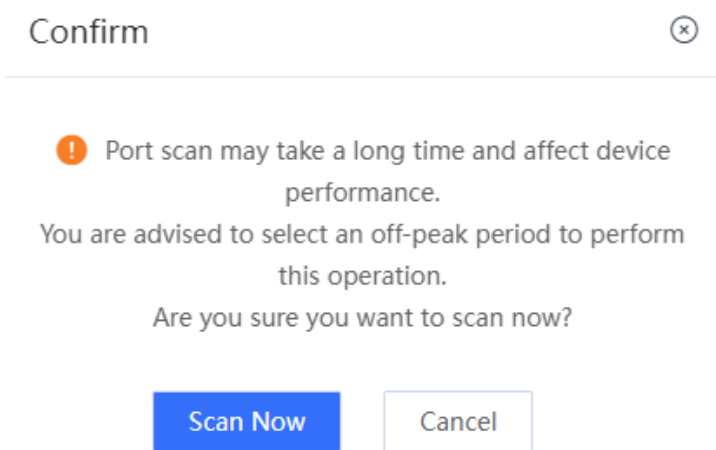
Add Custom Port Range

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

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

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

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



- (3) (Optional) If port scan policy has been configured:
 - a Click **Start Port Scan**.
 - b Click **Scan Now** to start port scan.

Tip ⊗

! Port scan range is set. Choose whether to scan now.

Port scan may take a long time and affect device performance.
You are advised to select an off-peak period to perform this operation.

[Scan Now](#) [Configure](#) [Cancel](#)

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

Port Scan

Port scan is complete. Create policies based on the result.
Port Scan Range | Configured | High-Risk Port Info | Query Common Port Info on Cloud | Rescan

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

Add Manually | Delete | **Create Policy** | Export | Refresh | IP: Select IP

IP	Port (Only Describing Well-Known Ports)	Status	Operation
<input checked="" type="checkbox"/>	10.52.25.2 445(Critical),80,5040 / 49 ports in total	and no policy has been created for 49 results.	Create Policy View Details Delete
<input type="checkbox"/>	10.52.25.3 139(Critical),445(Critical),135 / 11 ports in total	and no policy has been created for 11 results.	Create Policy View Details Delete
<input type="checkbox"/>	10.52.25.4 139(Critical),135,8848 / 16 ports in total	and no policy has been created for 16 results.	Create Policy View Details Delete
<input type="checkbox"/>	10.52.25.5 445(Critical),1024(Critical),3389(Critical) / 15 ports in total	and no policy has been created for 15 results.	Create Policy View Details Delete
<input type="checkbox"/>	10.52.25.8 139(Critical),445(Critical),2001(Critical) / 11 ports in total	and no policy has been created for 11 results.	Create Policy View Details Delete

Port Scan

Port scan is complete. Create policies based on the result.
Port Scan Range | Configured | High-Risk Port Info | Query Common Port Info on Cloud | Rescan

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

Add Manually | Delete | **Create Policy** | Export | Refresh | IP: Select IP

Tip ⊗

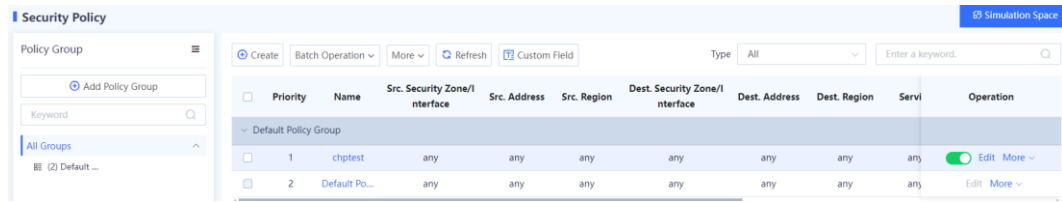
! Are you sure you want to add the policy in the simulation space?

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

[Create](#) [Add to Simulation Space](#)

IP	Port (Only Describing Well-Known Ports)	Status	Operation
<input checked="" type="checkbox"/>	10.52.25.2 445(Critical),80,5040 / 49 ports in total	and no policy has been created for 49 results.	Create Policy View Details Delete
<input type="checkbox"/>	10.52.25.3 139(Critical),445(Critical),135 / 11 ports in total	and no policy has been created for 11 results.	Create Policy View Details Delete
<input type="checkbox"/>	10.52.25.4 139(Critical),135,8848 / 16 ports in total	and no policy has been created for 16 results.	Create Policy View Details Delete
<input type="checkbox"/>	10.52.25.5 445(Critical),1024(Critical),3389(Critical) / 15 ports in total	and no policy has been created for 15 results.	Create Policy View Details Delete
<input type="checkbox"/>	10.52.25.8 139(Critical),445(Critical),2001(Critical) / 11 ports in total	and no policy has been created for 11 results.	Create Policy View Details Delete

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



- o Click **Add to Simulation Space** to add the generated policy to the simulation space. Run the policy in simulation mode and then add it to the security policy list.

Follow-up Procedure

- 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.

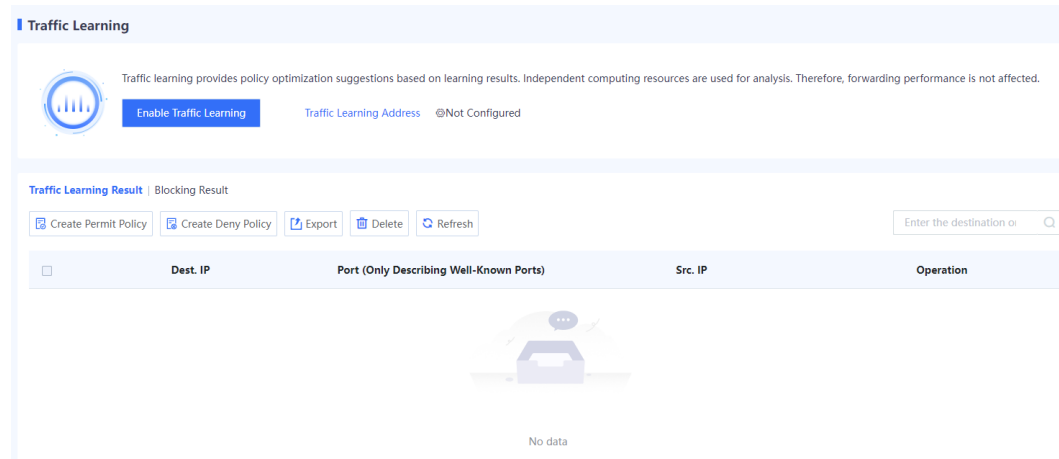
8.11 Traffic Learning

Application Scenario

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

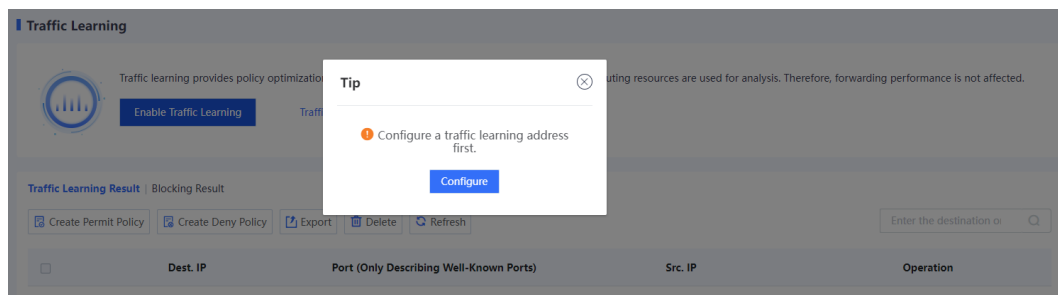
Procedure

- (1) Choose Policy > Traffic Learning.



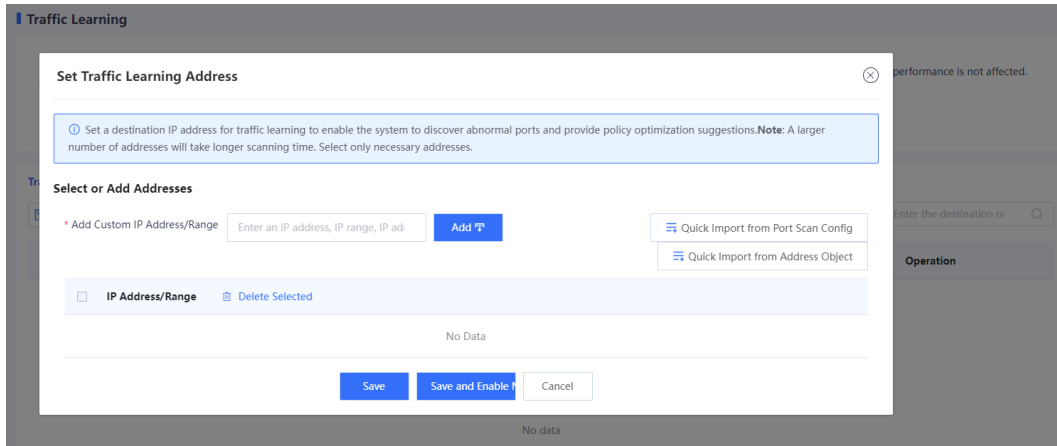
- (2) (Optional) If the traffic learning address is not configured, configure it first.

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



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

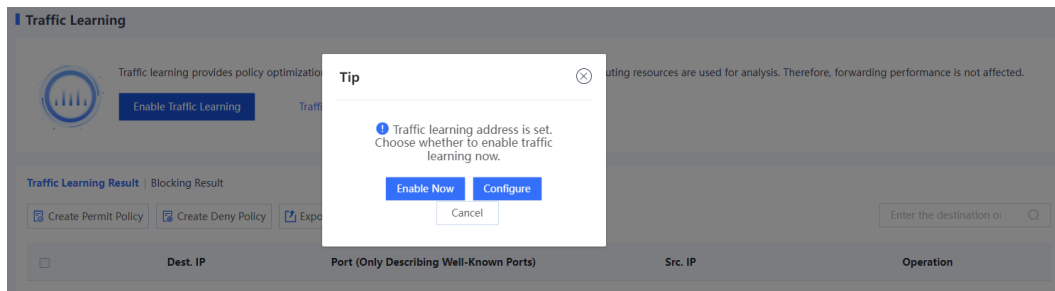
Enter the IP address or range to be learned in the **Add Custom IP Address/Range** input box, and click **Add** to add it to the **IP Address/Range** area.



Note

To quickly add IP addresses, click **Quick Import from Port Scan Config** or **Quick Import from Address Object**.

- c Choose whether to enable traffic learning immediately according to service situation.
 - o When services are busy, click **Save** to save the traffic learning address configuration. You can enable traffic learning when services are idle.
 - o When services are idle, click **Save and Enable Now** to save the traffic learning address configuration and enable traffic learning immediately.
- (3) (Optional) If the traffic learning address has been configured, click **Enable Traffic Learning** to modify the traffic learning address or enable traffic learning immediately.



Verification

- To view the information about learned IP addresses and ports, click the **Traffic Learning Result** tab. To view the detailed access relationship, click **View Details**.

Traffic Learning Result | Blocking Result

[Create Permit Policy](#)
[Create Deny Policy](#)
[Export](#)
[Delete](#)
[Refresh](#)

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

10 / Page Total:2

Go to 1 < 1 >

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



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

Tip ⊗

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

The policy execution process can be simulated before actual execution.

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

The policies are created only in the simulation space.

[Add to Simulation Space](#) [Create](#)

Insert it to the specified location. ✕

* Policy Name
Prefix

* Policy Group ▾

Policy ▾

Before/After ▾
the Adjacent
Policy

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

<input type="checkbox"/>	Priority	Name	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count	Hit Session	Operation
▼ Default Policy Group											
<input type="checkbox"/>	1	LnDeny_44:	TrafficLear...	any	any	any	Deny		0 Clear	View Details..	<input checked="" type="checkbox"/> Edit <input type="checkbox"/> Delete
<input type="checkbox"/>	2	port_scan...	PortScan_...	service_2...	any	any	Perm		0 Clear	View Details..	<input checked="" type="checkbox"/> Edit <input type="checkbox"/> Delete
<input type="checkbox"/>	3	test	any	any	any	any	Perm		0 Clear	View Details..	<input checked="" type="checkbox"/> Edit <input type="checkbox"/> Delete
<input type="checkbox"/>	4	allow_all	any	any	any	any	Perm		0 Clear	View Details..	<input checked="" type="checkbox"/> Edit <input type="checkbox"/> Delete

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

Traffic Learning

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

Traffic Learning Address @Configured

Traffic Learning Result | **Blocking Result**

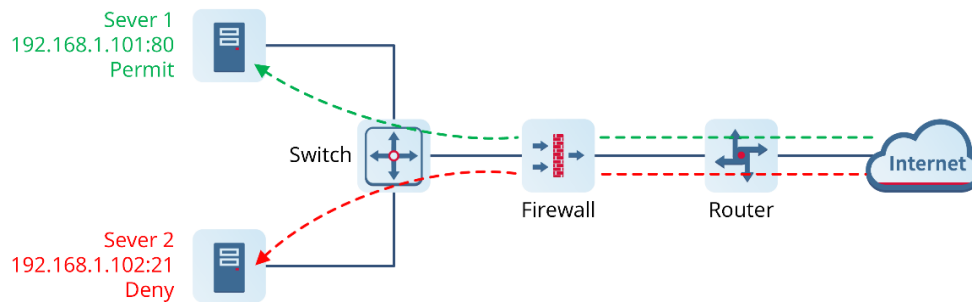
<input type="checkbox"/>	Dest. IP	Port (Only Describing Well-Known Ports)	Src. IP	Operation
<p>No data</p>				

8.12 Security Policy

8.12.1 Overview

The firewall verifies the passing traffic based on the security policy. Only the traffic matching the security policy with the permit action can be forwarded. For example, a firewall can be located at the boundary between an intranet and the Internet. A security policy is configured to establish a designated channel between the intranet and the Internet to filter sensitive data access.

With the stateful inspection packet filtering technology, firewalls can decide whether to allow packets to pass based on parameters such as IP address, service, port, and application type, and filter data at Layer 3 (network layer) and Layer 4 (transport layer).




As shown in the figure above, the firewall can filter the source and destination IP addresses and ports. For example, the firewall can be configured to allow or deny some IP addresses on the intranet to access the Internet, and allow or deny some IP addresses on the Internet to access the intranet.

Z-S series firewalls support multiple address objects:

- Single IP address (for example, 202.1.1.1)
- IP address network segment (for example, 192.168.1.0/255.255.255.0)
- IP address range (for example: 172.16.1.100-172.16.2.200)

For different IP addresses/segments with the same access permission, you can add them to an address group and reference them uniformly in the firewall policy.

Z-S series firewalls are preconfigured with port information for common network services, such as TCP port 80 used for HTTP and TCP port 21/20 for FTP. You can also customize TCP/UDP/ICMP/IP services and ports. Similarly, you can add different services and ports into a group for uniform reference by the policy.

Predefined Service		
Custom Service		
Service Group		
 Refresh		
Name	Protocol	
ping	ICMP: type 8, code 0	
ftp	TCP: 21	
ssh	TCP: 22	
telnet	TCP: 23	
smtp	TCP: 25	
dns-t	TCP: 53	
dns-u	UDP: 53	
sql_net	UDP: 66	
tftp	UDP: 69	
http	TCP: 80	

In addition to the IP address/port-based filtering function that traditional firewalls have, Z-S series firewalls can enforce different security policies for different time periods. For example, QQ is forbidden during working hours (such as 9:00-18:00 every day from Monday to Friday), but allowed in other time segments. This policy can be automatically implemented through the time-based policy of Z-S series firewalls.

< Back
Add Cyclic Time Plan



Basic Info

* Name

Description

* Effective Time Range Full Year Specific Time Range

*** Cycle List**

 Create
 Delete

<input type="checkbox"/>	Cycle	Time Range	Operation
<input type="checkbox"/>	Mon.,Tues.,Wen.,Thur.,Fri.	10:00:00-23:59:59	Edit Delete

Total: 1

Save

In addition, Z-S series firewalls can also enforce different security policies for the type of application of traffic. For example, to prevent intranet and extranet users from accessing game apps anywhere, anytime, configure a security policy and associate it with game apps.

Name	Type	App Group	Reputation Level	Reference
HTTP	Default	-	Low	0
WebApplication	Default	-	Low	0
HTTP-BROWSE	Default	-	Low	0
HTTP-PROXY	Default	-	Low	0
HTTP-GIF	Default	-	Low	0
MeituxixiuorMelyan	Default	-	Low	0
MSN	Default	-	Low	0
Firefox	Default	-	Low	0
Fast	Default	-	Low	0
Wikipedia	Default	-	Low	0
Google	Default	-	Low	0
QQ Application	Default	-	Low	0
QQ Space	Default	-	Low	0
QQ Yedian	Default	-	Low	0

Through the flexible combination of IP address, port, user, device, time and other parameters, a variety of firewall policies meeting actual network security needs can be configured, so that the user's security policy can be effectively implemented.

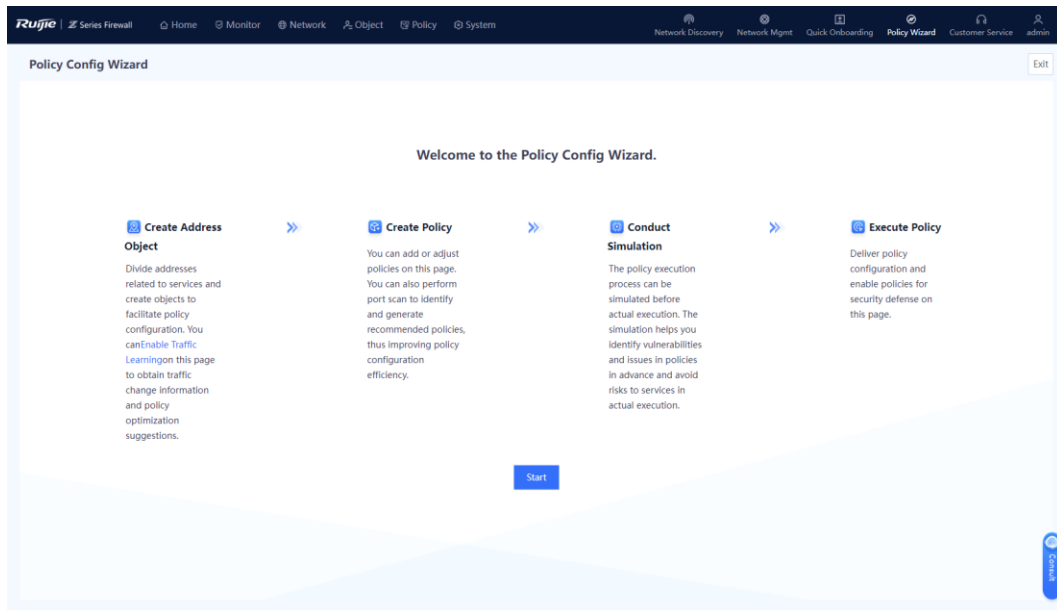
By default, the device is configured with a security policy that blocks all packets, and the default policy cannot be deleted or modified.

8.12.2 Configuring Security Policy (Using Wizard)

The web UI of Z-S series firewalls provides the policy configuration wizard for you to complete configuration and deployment efficiently.

Perform the following operations to enter the security policy configuration wizard:

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



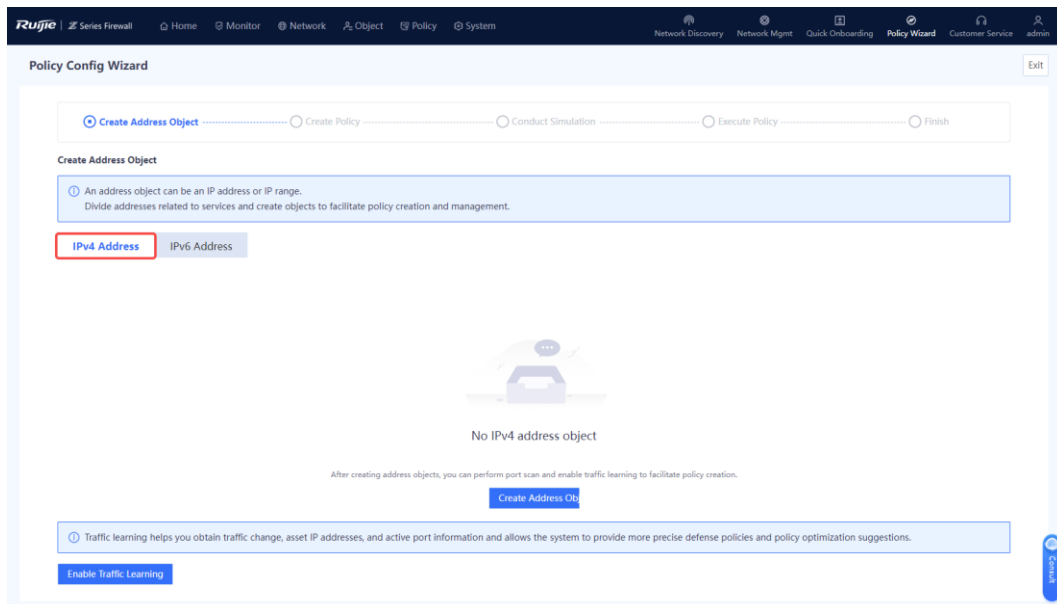
1. Creating an Address Object

Application Scenario

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

Procedure

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



- (2) Click Create Address Object.

Create Address Object

An address object can be an IP address or IP range.
Divide addresses related to services and create objects to facilitate policy creation and management.

IPv4 Address IPv6 Address



No IPv4 address object

After creating address objects, you can perform port scan and enable traffic learning to facilitate policy creation.

Create Address Ob

Traffic learning helps you obtain traffic change, asset IP addresses, and active port information and allows the system to provide more precise defense policies and policy optimization suggestions.

Enable Traffic Learning

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

Add IPv4 Address Object ⊗

* Address Object Name * IP Address/Range

Add IPv6 Address Object ⊗

* Address Object Name * IP Address/Range

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

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

 Note

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

(4) Click Confirm Creation.

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

Follow-up Procedure

- You can choose **Object > Address** to view, add, edit, and delete address objects.
- You can only delete the address with reference 0.

2. Configuring a Security Policy

Application Scenario

Configure the security policy according to the configuration wizard.

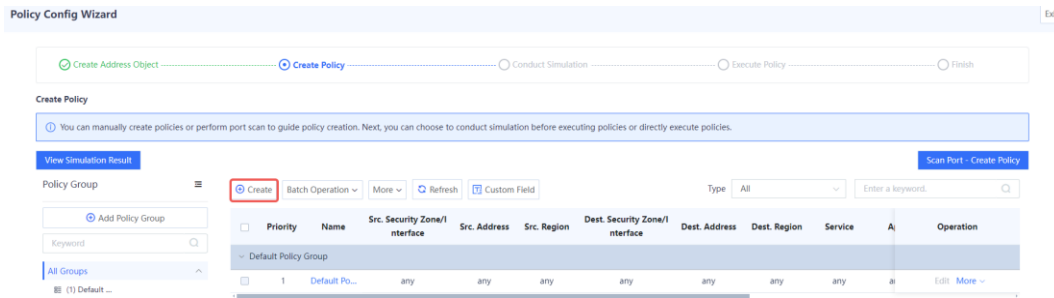
The security policy verifies the traffic passing the firewall. Only the traffic matching the security policy with the permit action can be forwarded. The security policy function provides security defense. For example, a firewall can be located at the boundary between an intranet and the Internet. A security policy is configured to establish a designated channel between the intranet and the Internet to filter sensitive data access.

Prerequisites

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

Procedure

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



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

Create Security Policy

Basic Info

* Name

Enabled State Enable

* Policy Group [+ Add Group](#)

* Priority

Description

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

Src. and Dest.

Src. Security Zone/Interface

* Src. Address

Src. Region

Dest. Security Zone/Interface

* Dest. Address

Dest. Region

Item	Description	Remarks
Src. Security Zone/Interface	Security zone or interface initiating the target data connection.	<ul style="list-style-type: none"> ● 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. <p>[Example] untrust</p>
Src. Address	Source address that initiates the target data connection.	<ul style="list-style-type: none"> ● 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. <p>[Example] Any</p>
Src. Region	Region initiating the target data connection.	<ul style="list-style-type: none"> ● 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. <p>[Example] any</p>
Dest. Security Zone/Interface	Destination security zone or interface of the target data connection.	<ul style="list-style-type: none"> ● 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. <p>[Example] trust</p>
Dest. Address	Destination address of the target data connection.	<ul style="list-style-type: none"> ● 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. <p>[Example] any</p>

Item	Description	Remarks
Dest. Region	Destination region of the target data connection.	<ul style="list-style-type: none"> 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 service, application, and user of the target data connection request.

Service

App

User

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

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

e Configure the action taken by the security policy. Permit or deny the target data connection.

Action Settings

Action Option Permit Deny

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

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

Content Security

Intrusion Prevention Disable

Virus Protection Disable

URL Filtering Disable

Keyword Filtering Disable

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

Advanced Option ⊗

Long-Lived Connection Disable

Cancel

Confirm

- h Click **Save**.

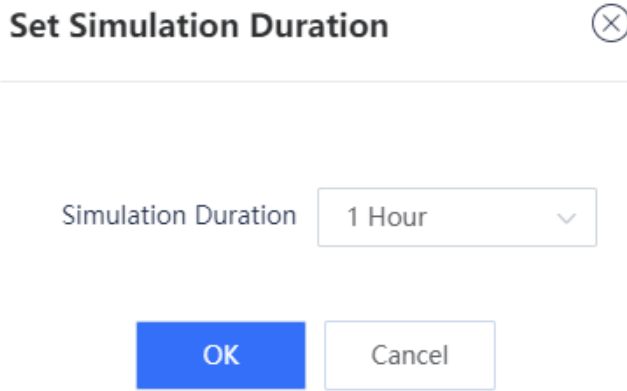
3. Simulation Run

Application Scenario

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

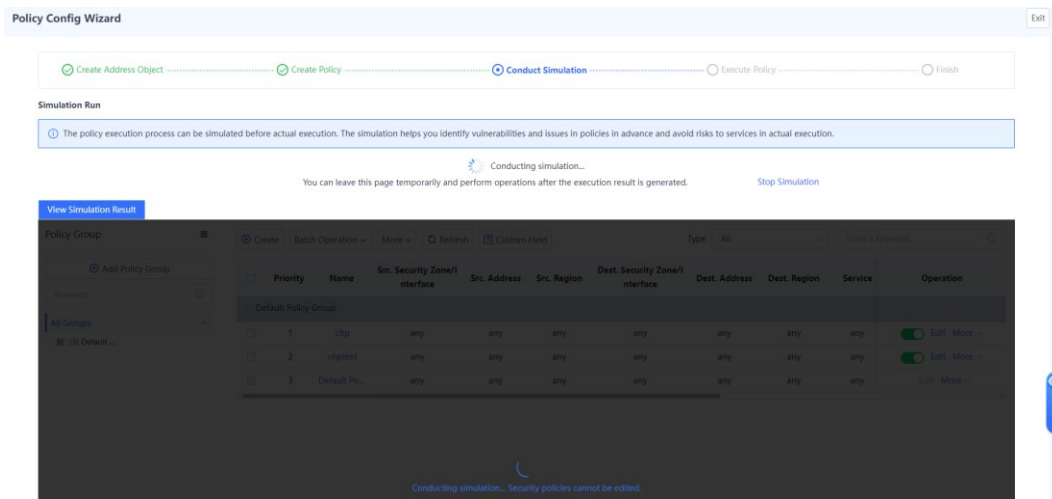
Procedure

- (1) On the **Create Policy** page, select the policy for which simulation run will be performed, and click **Start Simulation**.
- (2) In the **Set Simulation Duration** dialog box, set the duration of simulation run.



(3) Click **OK**.

The system automatically performs simulation run for the selected policies.



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

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


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

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

Simulation Results That Differ from Actual Execution Results ⊗

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

Refresh
Clear Result

Src. Address	Actual Execution Result	Simulation Result	Hit Count in Actual Execution	Hit Count in Simulation	Details
 <p style="color: red; font-weight: bold; margin-top: 10px;">The actual execution result is the same as the simulation result.</p>					

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

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

8.12.3 Configuring Security Policy (Manual)

Application Scenario

In addition to the wizard, RG-WALL 1600-Z-S series firewalls support manual configuration. You can manually configure security policies according to service needs.

Procedure

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

The system displays a tip.

Tip ⊗

Are you sure you want to add it in the simulation space?

The policy execution process can be simulated before actual execution. The simulation helps you identify vulnerabilities and issues in policies in advance and avoid risks to services in actual execution.

Do Not Show This Again

Simulation Space
Create

- (3) Click **Create**.

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

< Back
Create Security Policy

Basic Info

* Name

Enabled State Enable

* Policy Group [Add Group](#)

* Priority

Description

Src. and Dest.

Src. Security

Zone/Interface

* Src. Address

Src. Region

Dest. Security

Zone/Interface

* Dest. Address

Dest. Region

Service

App

User

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

Action Option Permit Deny

[Fold ^](#)

Content Security

Intrusion Prevention Disable

Virus Protection Disable

URL Filtering Disable

Keyword Filtering Disable

Advanced

(4) Set parameters of security policy.

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

Item	Description	Remarks
Enabled State	Whether to enable the new security policy.	[Example] Enable
Policy Group	Policy group to which the new security policy belongs.	<ul style="list-style-type: none"> ● Select from the drop-down list. ● Click Add Group to add a custom policy group. [Example] Default policy group.
Priority	Move the new security policy before or after the specified policy. The closer a policy is to the front, the higher its priority is in matching.	-
Description	Security policy description.	Characters such as `~!#%^&*+ \{};:~"/<>?` are not allowed. [Example] Perform virus detection for the HTTP traffic from security zone 1 to security zone 2.
Src. and Dest.		
Src. Security Zone/Interface	Source security zone or interface initiating the target data.	<ul style="list-style-type: none"> ● 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. [Example] trust
Src. Address	Source address that initiates the target data connection.	<ul style="list-style-type: none"> ● 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

Item	Description	Remarks
Src. Region	Region initiating the target data connection.	<ul style="list-style-type: none"> ● 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.	<ul style="list-style-type: none"> ● 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. [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
Dest. Region	Destination region of the target data connection.	<ul style="list-style-type: none"> ● 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.	<ul style="list-style-type: none"> ● Click the drop-down list, and select a service or service group in the To-be-selected area. The selected service or service group is automatically added to the Selected area. ● To add a custom service, click Add Service. [Example] any

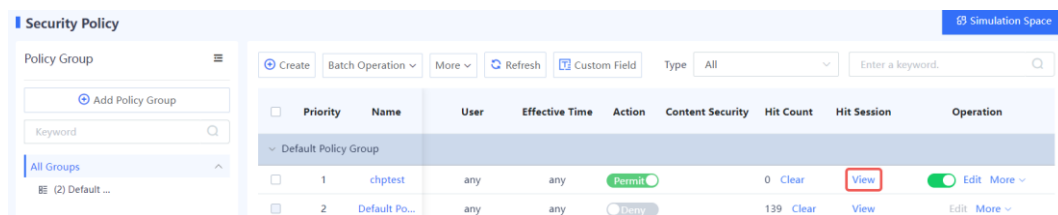
Item	Description	Remarks
App	Application type of the target data connection request.	<ul style="list-style-type: none"> ● Click the drop-down list, and select an application or application group in the To-be-selected area. The selected application or application group is automatically added to the Selected area. ● To add a custom application, click Add Custom App. [Example] any
User	The traffic of specified users or user groups matches the policy.	<ul style="list-style-type: none"> ● Click the drop-down list, and select a user or user group in the To-be-selected area. The selected user or user group is automatically added to the Selected area. ● Click Add User or Create User Group to create a user or user group. [Example] UserGroup_1
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.	<ul style="list-style-type: none"> ● To add a one-off time plan, click Add One-Off Time Plan. ● To add a cyclic time plan, click Add Cyclic Time Plan. [Example] any
Action Option	Action taken by the security policy to permit or deny the target data connection.	[Example] Permit
Content Security	Whether intrusion prevention, virus detection, URL filtering, and keyword filtering are enabled for the target data connection. If you want to enable content security check, you must specify the intrusion prevention and virus protection templates, and configure the actions. The 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] <ul style="list-style-type: none"> ● Intrusion Prevention: Enable ● Virus Protection: Enable ● URL Filtering: Not Enabled ● Keyword Filtering: Enable

Item	Description	Remarks
Advanced	<p>Advanced settings of the security policy, including:</p> <p>Long-Lived Connection: applies to the special servers that require long-lived connections. After this function is enabled, the server's connection request is not restricted by the connection timeout setting of the firewall. The connection duration needs to be set.</p>	<ul style="list-style-type: none"> ● 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. <p>[Example]</p> <p>Disable</p>

(5) Click **Save**.

Follow-up Procedure

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



8.12.4 Adjusting Policy Order

Application Scenario

When you configure multiple security policies, the list of security policies is arranged in the order of configuration by default. The security policies that are configured earlier have higher priorities. Security policy matching is performed in the order of the policy list, that is, starting from the top of the policy list. If the traffic matches a security policy, the next policy will not be matched.

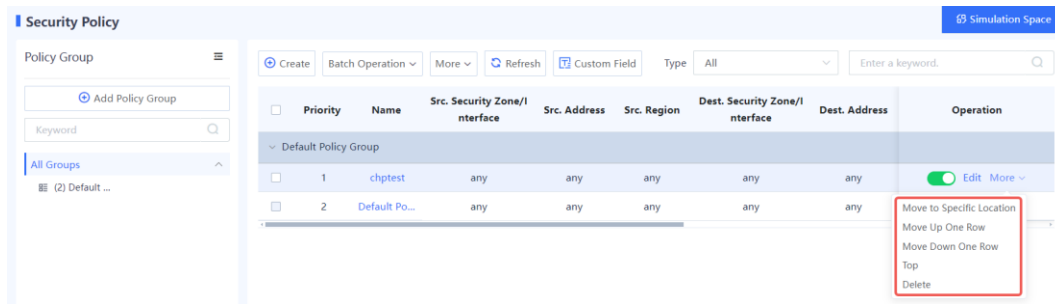
You can adjust the order of security policies to meet service requirements.

Note

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

Procedure

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



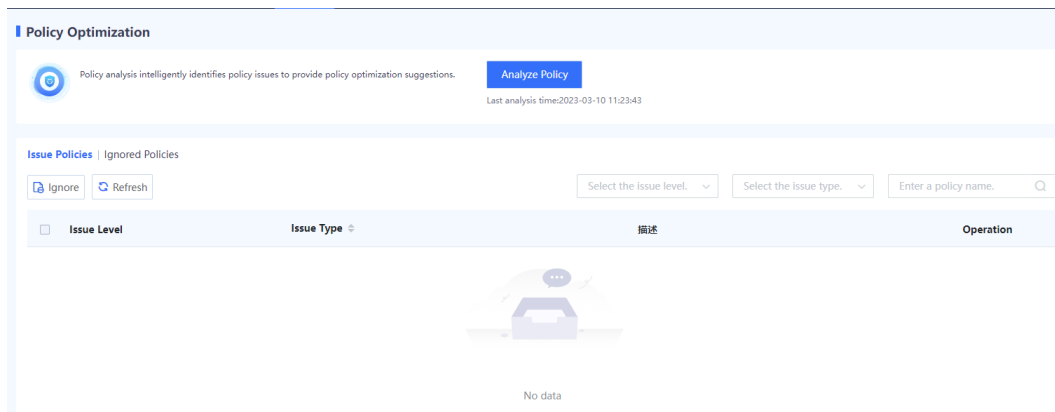
8.12.5 Optimizing Policy

Application Scenario

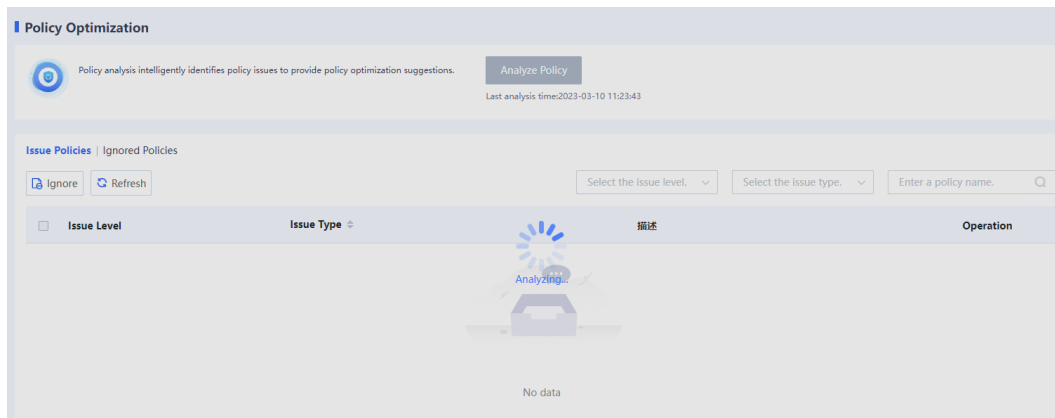
Affected by factors such as service accumulation and change of O&M personnel, the configuration complexity of security policies becomes increasingly high during the routine security policy O&M process. The policy optimization function of Z-S series firewalls can intelligently compare and analyze the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

Procedure

- (1) Choose Policy > Security Policy > Policy Optimization.



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



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

Issue Level	Issue Type	Description	Operation
4_To_2_out	Never Matched	The policy never matches a packet.	Ignore Handle
default组	Never Matched	The policy never matches a packet.	Ignore Handle
allow_all	Any Permission	The policy allows data packets to be forwarded from any source to any destination and is improper.	Ignore Handle

Note

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

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

Handle Issue Policy

Policy Name: 4_To_2_out

Policy Issues: Never Matched

Question Description

- Description:** The policy never matches a packet.
- Impact:** Redundant policies occupy the memory of the device and affect device forwarding performance.
- Solution:** You are advised to delete the policy or modify matching conditions of the policy.

Issue No./Total: 1/1 Previous Next

Optimize Policy

Color description: To-be-optimized Optimization suggestion: You are advised to delete the policy or modify matching conditions of the policy

Priority	Name	Source	First Creation Time	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Operation
2	4_To_2_out	manual	2024-02-08 09:41:05	any	any	4_To_2	any	any	any	Edit Delete

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

8.12.6 Policy Lifecycle Management

Application Scenario

Affected by factors such as service accumulation and change of O&M personnel, the security policies need to be repeatedly modified to meet new service requirements or solve existing problems. When encountering problems, O&M personnel often need to trace and analyze the changed policies and detailed change items. The policy lifecycle management function provided by Z-S series firewalls records the entire process of creating, modifying, and deleting each security policy, and records the operators and IP addresses of the operations in detail.

Procedure

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

Policy Life Cycle

Export Refresh Search Criteria Enter the policy name. Q

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

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

Change Details

Back

Operation Info

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

Change Details

Check Changed Items Only

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

On the **Details** page, you can view the details of a single change, solving the pain point of tracing security policy changes during O&M and reducing O&M costs.

8.12.7 Simulation Run

Application Scenario

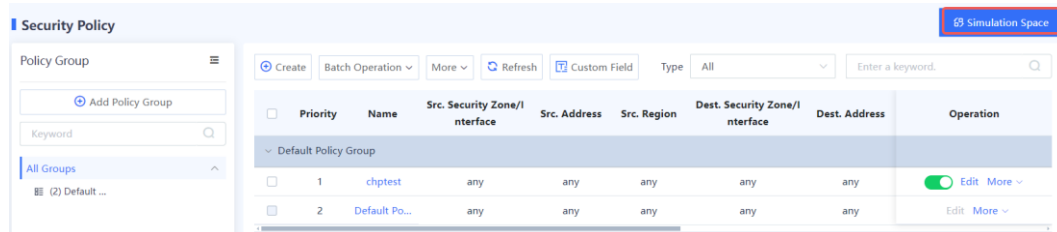
Affected by factors such as service accumulation and change of O&M personnel, the configuration complexity of security policies becomes increasingly high during the routine security policy O&M process. In the middle and late stages of O&M, if the security policy is modified improperly, the risk of service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

Z-S series firewalls provide a virtual space of policy simulation run for O&M personnel to verify and test policy modifications. This space does not affect the services in the real network environment. That is, the security policies in the simulation space will not permit or block real service traffic.

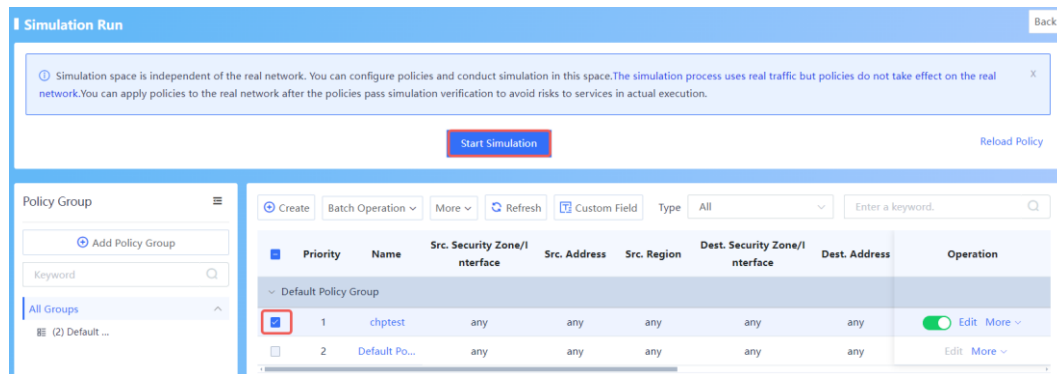
This function solves the problems such as service interruption caused by improper configuration in O&M, and provides O&M personnel with a test and verification environment, thus reducing O&M difficulty and risk, and lowering O&M costs.

Procedure

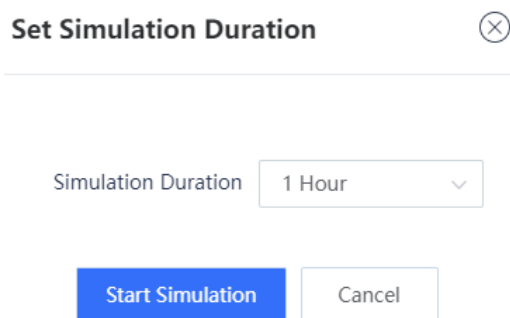
- (1) Choose **Policy > Security Policy > Security Policy**.
- (2) Click **Simulation Space** in the upper right corner of the operation area.



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

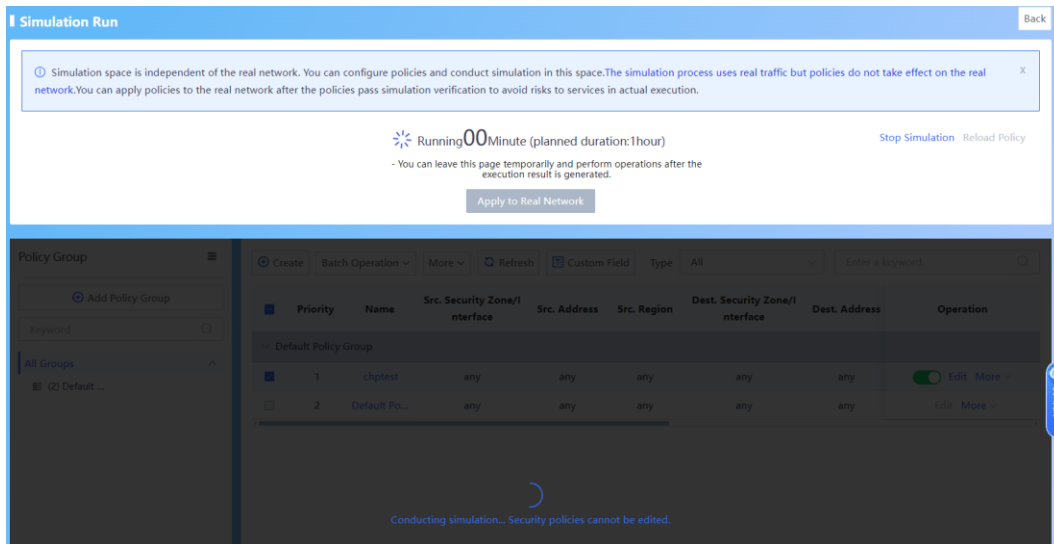


- (4) In the **Set Simulation Duration** dialog box, set the duration of simulation run.



- (5) Click Start Simulation.

The system automatically performs simulation run for the selected policies.

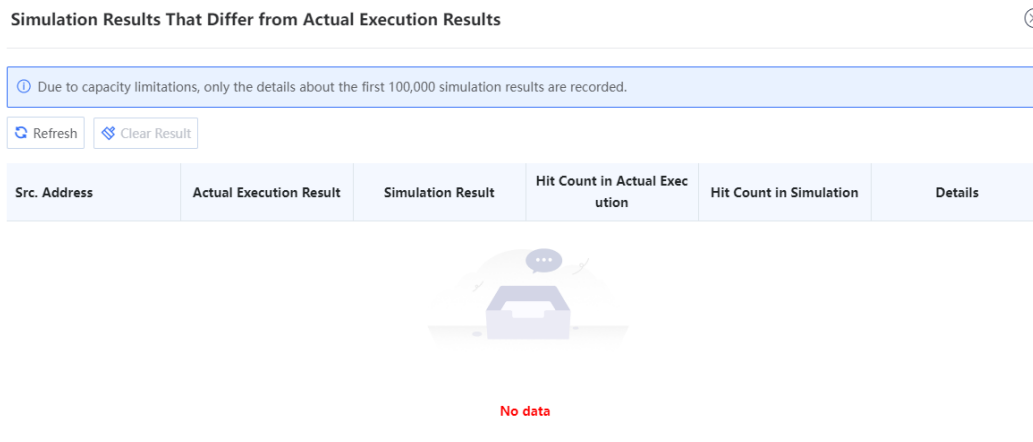


(6) When simulation run is finished, click **View Simulation Result**.

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

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

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



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

Follow-up Procedure

- O&M personnel can copy a currently effective security policy to the simulation space and modify the policy as required. For example, the O&M personnel can add, modify, and delete the policies according to service requirements.
- When the O&M personnel verify that there are no problems with the security policies in the simulation space, they can export the security policies to make them effective and replace the current security policies.

8.12.8 Importing Security Policies in a Batch

Application Scenario

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

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

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

Caution

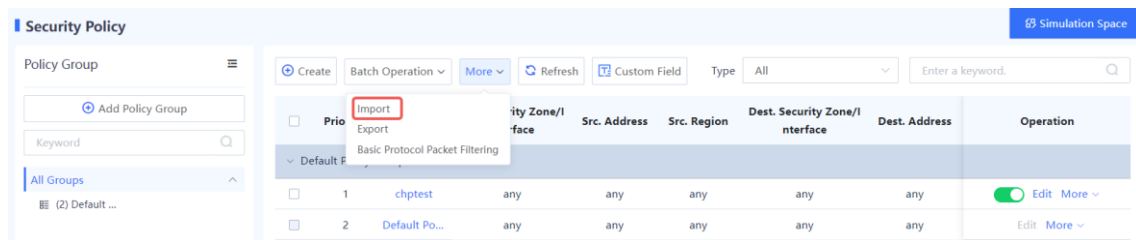
The security policies containing IPv6 addresses cannot be imported in a batch.

Note

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

Procedure

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

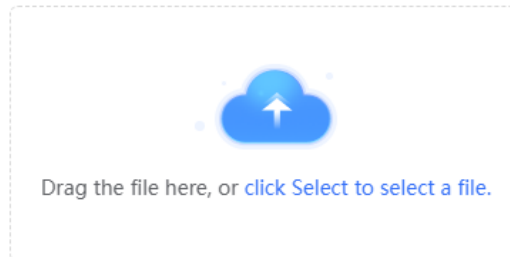


- (3) The system displays a tip.

Tip

i The format of the configuration file to be imported must be config-conversion-yyyyMMddHHmmssSSS.csv.
 For example, config-conversion-20220228145158060.csv.
 The total number of configuration entries must be less than 1000, and the maximum import duration is about 2 min. For details about the content format, see the sample file.

[Download CSV Sample File](#)



If imported configurations conflict with existing configurations,

Display Conflicting Data Skip

OK

Cancel

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

i Note

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

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

- (6) Configure the method used when data conflicts.

When the imported data conflicts with the existing data, the following processing methods can be used:

- o **Display Conflicting Data**: The system displays the conflicting configuration items and the conflict reason for you to modify the configuration file.
- o **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.

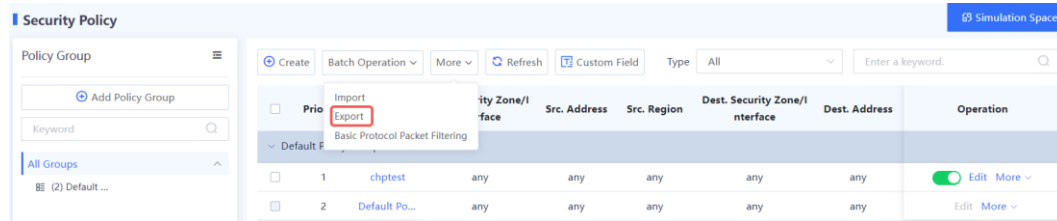
8.12.9 Exporting Security Policies

Application Scenario

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

Procedure

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



8.12.10 Enabling Basic Protocol Packet Control

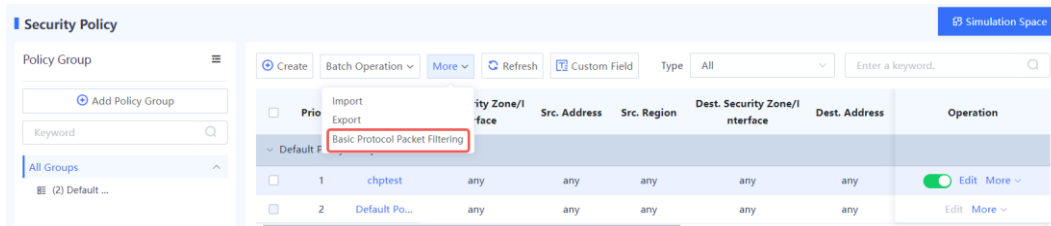
Application Scenario

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

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

Procedure

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



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



(4) Click **OK**.

8.12.11 Configuration Examples of DHCP + Security Policies

1. Applicable Products and Versions

Table 8-16 Applicable Products and Versions

Device Type	Device Name	Version
NGFW	RG-WALL 1600-Z-S series firewalls	All versions

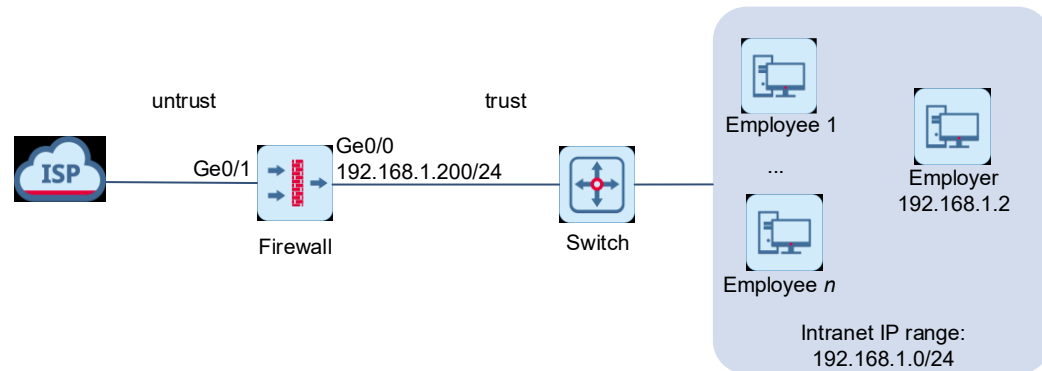
2. Service Demands

In the office scenario shown in [Figure 8-6](#), a firewall is deployed at the egress of the intranet in routing mode and serves as a DHCP server to assign IP addresses to intranet users. The employer and employees use IP addresses from the same DHCP address pool. Security policies need to be configured to meet the following requirements:

- Employees' IP addresses are controlled by a policy. They can only access specified applications, such as office OA.
- The employer's IP address is not subject to any restrictions.

3. Topology

Figure 8-6 Office Networking



4. Restrictions and Guidelines

The basic network configurations, such as the IP address of the Ge0/1 interface and default routes, have been completed on the firewall.

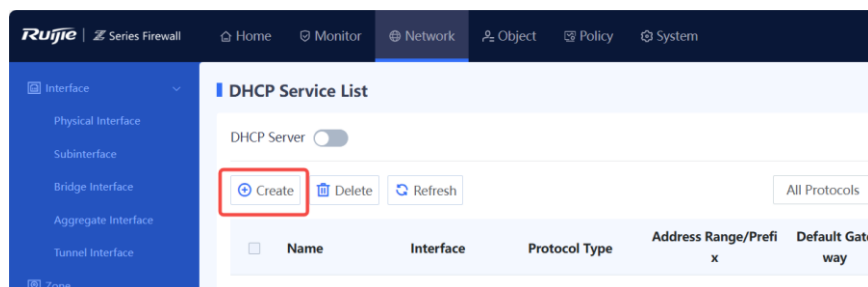
5. Configuration Roadmap

- (1) To prevent the employer's IP address from being mistakenly limited by a policy, configure DHCP static IP address assignment for the employer.
- (2) Create two security policies to permit traffic from the employer's IP address and limit traffic from employees' IP addresses.
- (3) Configure a higher priority for the policy that permits traffic from the employer's IP address.

6. Procedure

(1) Configuring DHCP

- a Choose **Network > DHCP > DHCP Server** and click **Create** to create a DHCP address pool.



- b Configure basic information of the DHCP address pool as shown in the following figure.
 - o The address pool name is configured according to the actual needs, and **test** is used in this example.
 - o Configure the firewall interface Ge0/0 to connect to the intranet.
 - o Allocate IP addresses based on the actual needs. In this example, the 192.168.1.0/24 addresses are allocated.

< Back

Create DHCP Service

Protocol Type IPv4 IPv6

Basic Info

* Name

* i Interface

* i IP Assignment Range

* Subnet

* Default Gateway

* Primary DNS Server Use System DNS Settings

Secondary DNS Server

☰ Advanced

- c Click **Advanced** to go to the advanced settings. In the **Binding Host MAC** box, enter the employer's IP address and MAC address for IP-MAC address binding, and click **Save**.

In this example, to statically assign an IP address to the employer, bind the IP address 192.168.1.2 to the MAC address d8:9e:f3:3f:d5:64 of the employer's endpoint.

☰ Advanced

* Lease Time Day Hour Minute

Primary WINS Server

i Option 43

i Option 138

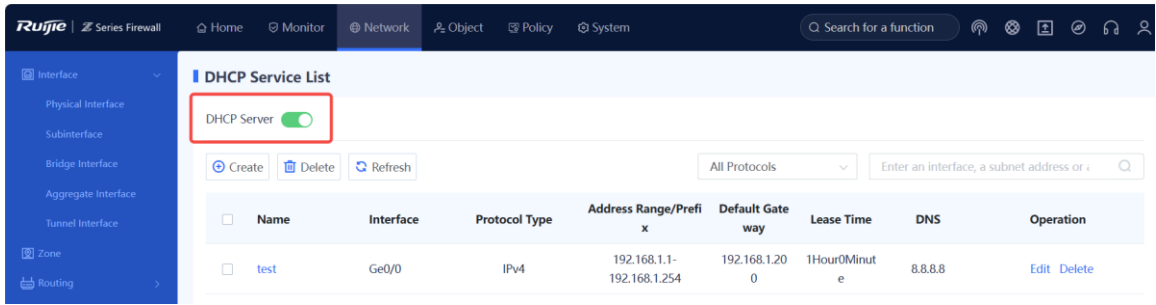
Secondary WINS Server

i Reserved IP Address/Range

i Binding Host MAC

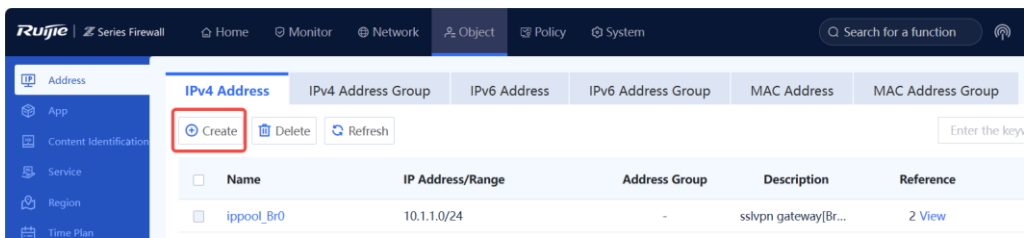
Save

- d Check whether the DHCP server function is automatically enabled. If it is disabled, manually enable it.



(2) Configuring the IP Address Objects

- a Choose **Object > Address > IPv4 Address** and click **Create** to create an IP address object for employees.



- b Configure an IP address object named **allstaff** for employees, and set **IP Address/Range** to **192.168.1.1-192.168.1.254**. Then, click **Save**.

< Back

Add IPv4 Address Object

Basic Info

* Name

Description

IP Address/Range

*

- c Configure an IP address object named **boss** for the employer as shown in the following figure, and set **IP Address/Range** to **192.168.1.2**. Then, click **Save** after configuration.

Add IPv4 Address Object

Basic Info

* Name: boss

Description: [Empty text area]

IP Address/Range

* IP Address/Range: 192.168.1.2

[Save]

After all address objects are created, the following figure is displayed.

Name	IP Address/Range	Address Group	Description	Reference	Operation
boss	192.168.1.2	-	-	-	Edit Delete
allstaff	192.168.1.1-192.168.1.254	-	-	-	Edit Delete

(3) Configuring Security Policies

- a Choose **Policy > Security Policy > Security Policy** and click **Create** to create a security policy for employees' IP addresses.

Security Policy

[Create] [Batch Operation] [More] [Refresh] [Custom Field]

Priority	Name	Src. Security Zone/Interface	Src. Address	Src. Region	Dest. Security Zone/Interface
Default Policy Group					

- b Read the pop-up window and select whether to create a policy in the simulation space as required. In this example, click **Create**.

Tip

Are you sure you want to add it in the simulation space?

The policy execution process can be simulated before actual execution. The simulation helps you identify vulnerabilities and issues in policies in advance and avoid risks to services in actual execution.

Do Not Show This Again



- c On the **Create Security Policy** page, configure a security policy for employees' addresses.
 - o Set the policy name based on the actual needs. In this example, the policy name is set to **forallstaff**.
 - o Set **Policy Group** to **Default Policy Group**. You can select a custom policy group as required.
 - o Configure the priority to be before the default policy. During the actual configuration, you can set the policy location based on requirements. A policy earlier in the list has a higher priority.
 - o Set Src. Address to allstaff and Dest. Address to any.
 - o Set **Src. Security Zone/Interface** and **Dest. Security Zone/Interface** according to the actual needs. In this example, **trust** and **untrust** are selected.
 - o Expand **App, User, Effective Time**. Set **App** to an application that is allowed to be accessed. In this example, select **Work-OA**.
 - o Set **Action Option** to **Permit** and then click **Save**.

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

Basic Info

* Name

Enabled State Enable

* Policy Group [⊕ Add Group](#)

* Priority

Description

Src. and Dest.

Src. Security

Zone/Interface

* Src. Address

Src. Region

Dest. Security

Zone/Interface

* Dest. Address

Dest. Security

Zone/Interface

* Dest. Address

Dest. Region

Service

Action Option Permit Deny

Content Security

Intrusion Prevention Disable

Dest. Security

Zone/Interface

* Dest. Address

Dest. Region

Service

App

User

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

Action Option Permit Deny

[Fold ^](#)

Content Security

Intrusion Prevention Disable

Virus Protection Disable

URL Filtering Disable

Keyword Filtering Disable

Advanced

- d Repeat the preceding steps to create a security policy for the employer's IP address.
 - o Set a policy name based on the actual needs. **forboss** is used in this example.
 - o Set **Policy Group** to **Default Policy Group**. You can select a custom policy group as required.
 - o Set the priority to be before **forallstaff** to ensure that the security policy for the employer's IP addresses has a higher priority.
 - o Set **Src. Address** to the address object **boss**.
 - o Set **Src. Security Zone/Interface** and **Dest. Security Zone/Interface** according to the actual needs. In this example, **trust** and **untrust** are selected.
 - o Set other parameters to **any** and **Action Option** to **Permit** to permit traffic from the employer's IP address.

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

Basic Info

* Name

Enabled State Enable

* Policy Group [⊕ Add Group](#)

* Priority

Description

Src. and Dest.

Src. Security

Zone/Interface

* Src. Address

Src. Region

Dest. Security

Zone/Interface

* Dest. Address

* Priority

Description

Src. and Dest.

Src. Security

Zone/Interface

* Src. Address

Src. Region

Dest. Security

Zone/Interface

* Dest. Address

Dest. Region

Service

Action Option Permit Deny

[App, User, Effective Time](#)

Content Security

7. Verification

After the configuration is completed, the following two security policies are displayed on the page: One policy permits traffic from the employer’s IP address and the other policy restricts employees’ access to applications. The **forboss** policy has a higher priority.

Type

<input type="checkbox"/>	Priority	Name	Src. Security Zone/Interface	Src. Address	Src. Region	Dest. Security Zone/Interface	Operation
▼ Default Policy Group							
<input type="checkbox"/>	1	forboss	trust	boss	any	untrust	<input checked="" type="checkbox"/> Edit More
<input type="checkbox"/>	2	forallstaff	trust	allstaff	any	untrust	<input checked="" type="checkbox"/> Edit More
<input type="checkbox"/>	3	Default Po...	any	any	any	any	<input type="checkbox"/> Edit More

8.13 Traffic Control Policy

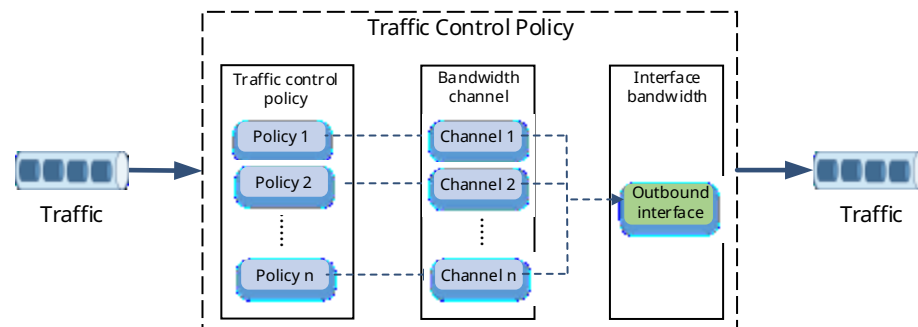
8.13.1 Overview

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

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

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

The processing procedure of traffic control policies is as follows:

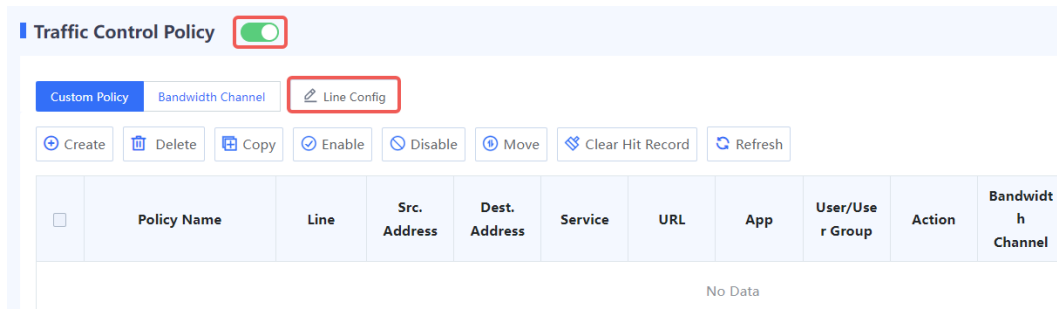


- (1) After a device receives traffic, the device matches the traffic against traffic control policies in the configured order until one policy is matched. If the traffic matches no policy, no traffic control action is performed.
- (2) The closer a policy is to the front, the higher its priority in matching.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

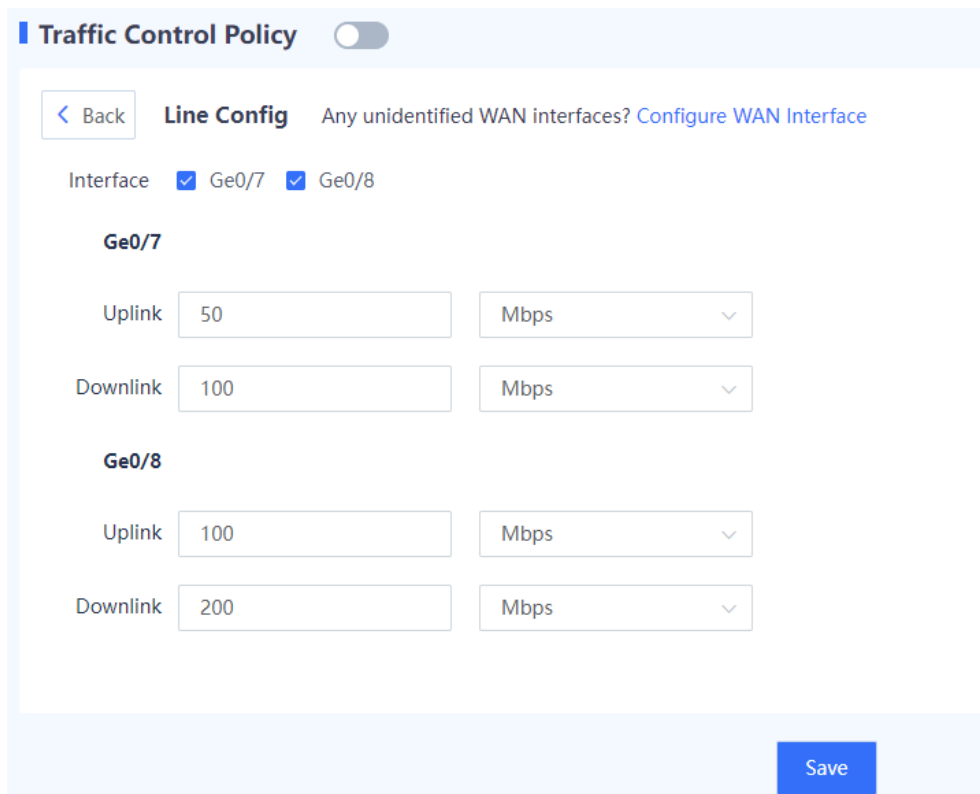
8.13.2 Configuring Traffic Control Policies

1. Configuring Egress Bandwidth

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



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



Note

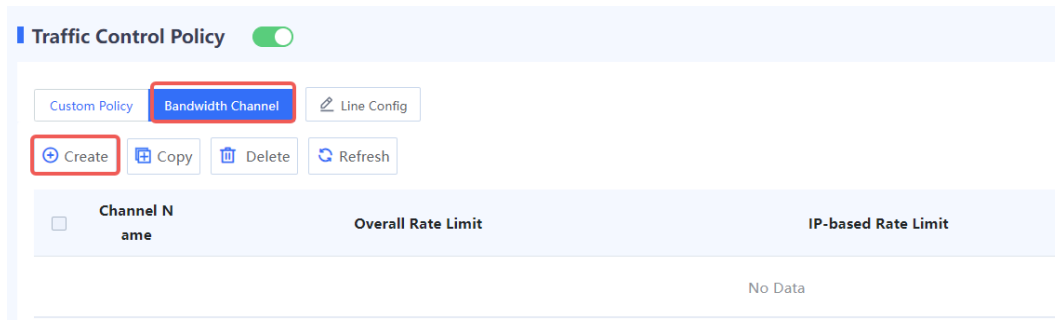
The outbound interface must be a WAN interface.

(4) Click **Save**.

2. Configuring Bandwidth Channels

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

(2) Click the Bandwidth Channel. Click Create.



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

< Back

Add Bandwidth Channel

Basic Info

* Name

Overall Rate Limit ⓘ

Max. Uplink Rate Mbps ▾

Guaranteed Uplink Rate Mbps ▾

Max. Downlink Rate Mbps ▾

Guaranteed Downlink Rate Mbps ▾

IP-based Traffic Limit ⓘ

Max. Uplink Rate Mbps ▾

Max. Downlink Rate Mbps ▾

Priority

ⓘ Priority 4 (Medium) ▾

ⓘ Enable Refined Traffic Limiting

Save

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

Item	Description	Remarks
Max. Uplink Rate	The maximum bandwidth resource available to the traffic transmitted over the channel. The excessive traffic is discarded. If the parameter is not specified, the traffic is not limited.	[Example] 10 Mbps
Guaranteed Uplink Rate	The minimum bandwidth resource available to the traffic transmitted over the channel. If the parameter is not specified, no bandwidth resource is guaranteed.	[Example] 10 Mbps
Max. Downlink Rate	The maximum bandwidth resource available to the traffic transmitted over the channel. The excessive traffic is discarded. If the parameter is not specified, the traffic is not limited.	[Example] 10 Mbps
Guaranteed Downlink Rate	The minimum bandwidth resource available to the traffic transmitted over the channel. If the parameter is not specified, no bandwidth resource is guaranteed.	[Example] 10 Mbps
Priority	Bandwidth channel priority. When traffic from multiple bandwidth channels is simultaneously forwarded by an interface and traffic congestion occurs on the interface, the device forwards traffic from channels with higher priority first.	[Example] 1
Enable Refined Traffic Limiting	<p>If this function is enabled, the device performs weight-based scheduling on the traffic entering the channel based on the service priority and guarantees the bandwidth of key services first when the bandwidth is insufficient.</p> <p>If this function is not enabled, services transmitted over the tunnel compete for bandwidth resources without priority differentiation.</p> <p>Refined traffic limiting can be enabled only when the priority value is 1. It does not take effect when it is enabled for parent or child policies.</p>	This function can be enabled only when the priority of a bandwidth channel is 1 (highest priority).

(4) Click **Save**.

3. Configuring Traffic Control Policies

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

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

Traffic Control Policy

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

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

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

Basic Info

* Name

Parent Policy

Location

Enabled State Enable Disable

Line

* Line

Src. and Dest.

Src. Address

Dest. Address

Services and Apps

Service

App

URL

URL

User/User Group

User/User Group

Action Execution

Action Limit No Rate Limit Block

* Bandwidth

Channel

Time Range

Time Range

Item	Description	Remarks
Basic Info		
Name	Name of the traffic control policy	[Example] Policy_1
Parent Policy	<p>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.</p> <p>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.</p> <p>The bandwidth channels of the parent policy and its child policy cannot be the same.</p>	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 packets with specified source IP addresses match the policy.	[Example] any
Dest. Address	The packets with specified destination IP addresses match the policy.	[Example] any
Services and Apps		

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

(4) Click **Save**.

8.14 DHCP Management

8.14.1 Overview

Dynamic Host Configuration Protocol (DHCP) is a network management protocol applied on the LAN. It works using UDP and is widely used to dynamically allocate network resources that can be reused, such as IP addresses. For small networks, DHCP makes subsequent network device adding easy and fast.

DHCP provides the following benefits:

- Reduced client configuration and maintenance costs

DHCP is easy to configure and deploy. For non-technical users, DHCP can minimize configuration-related operations on the client and reduce remote deployment and maintenance costs.

- Centralized management

The DHCP server can be used to manage the configuration information about multiple network segments. When the configurations of a network segment change, the administrator only needs to update related configurations on the DHCP server.

The Z-S series firewall can be configured as a DHCP server to allocate IP addresses to intranet users.

8.14.2 Configuring a DHCP Server

1. Application Scenario

The system enables the DHCP server function by default. The firewall can be configured as a DHCP server to allocate IP addresses to intranet users.

2. Configuring a DHCPv4 Server

(1) Choose Network > DHCP > DHCP Server.

(2) Configure the DHCP server information.

a Click **Create**.

The **Create DHCP Service** page is displayed. Set **IPv4**.

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

Protocol Type IPv4 IPv6

Basic Info

* Name

* Interface

* IP Assignment Range

* Subnet

* Default Gateway

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

Secondary DNS Server

Advanced

* Lease Time Day Hour Minute

Primary WINS Server

Option 43

Option 138

Secondary WINS Server

Reserved IP Address/Range

Binding Host MAC

[Save](#)

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.	[Example] Ge0/1
IP Assignment Range	Range of IP addresses allocated by the DHCP server.	<ul style="list-style-type: none"> ● Enter an IP address range per line. ● Connect the start IP address and end IP address with a hyphen (-). [Example] 192.168.1.1-192.168.1.10
Subnet	Subnet where the IP addresses are located.	Enter the subnet address/ mask bits. [Example] 192.168.1.0/24
Default Gateway	Default gateway that provides network access service to the terminals, which obtain IP addresses.	[Example] 255.255.255.0
Primary DNS Server	Preferred DNS server used by the DHCP service.	Click Use System DNS Settings . Then the system automatically fills in the system DNS server. You can also configure a public DNS server. [Example] 192.168.10.1
Secondary DNS Server	Alternative DNS server used by the DHCP service.	[Example] 192.168.30.1
Advanced		

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.	<ul style="list-style-type: none"> ● The lease period ranges from 3 minutes to 365 days. ● The default lease period is 1 hour. [Example] 1 hour
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 43	<p>Option 43 carried in DHCP packets.</p> <p>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.</p>	<ul style="list-style-type: none"> ● 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: <ul style="list-style-type: none"> ○ IP address: Enter the IP address of the AC. Typically, the loopback address of the AC is configured. ○ ASCII code: Set Option 43 to a hexadecimal number in ASCII format.

Item	Description	Remarks
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.
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
Binding Host MAC	Static bindings between the pre-assigned IP addresses specified by IP Assignment Range and the MAC addresses of the clients. When receiving a request for an IP address from a client with a matching MAC address, the DHCP server allocates the pre-assigned IP address that is bound to the MAC address only to this client.	The value is in the format of IP address/MAC address, where the IP address should be a pre-assigned address in the IP Assignment Range . Enter one binding entry per line. [Example] 192.168.10.1/d8:9e:f3:3f:d5:64

c Click **Save**.

3. Configuring a DHCPv6 Server

(3) Choose Network > DHCP > DHCP Server.

(4) Configure the DHCP server information.

a Click **Create**.

The **Create DHCP Service** page is displayed. Set **IPv6**.

The screenshot shows the 'Create DHCP Service' configuration page. At the top left, there is a '< Back' button and the title 'Create DHCP Service'. Below this, the 'Protocol Type' is set to 'Ipv6' (indicated by a blue dot). Under the 'Basic Info' section, the 'Interface' dropdown menu is set to 'Select an interface.', the 'Primary DNS Server' field is empty, and the 'Lease Time' is configured as 0 Day, 8 Hour, and 0 Minute. The 'Address Pool' section contains a table with columns for 'Type', 'Prefix', 'Available Prefix Length', and 'Operation', which is currently empty and shows 'No Data'. At the bottom right, there is a blue 'Save' button.

b Set parameters of the DHCP server.

Item	Description	Remarks
Interface	Interface where the DHCPv6 server is configured. After the DHCPv6 function is enabled, the interface can allocate IPv6 addresses.	[Example] Ge0/4
Primary DNS Server	Preferred DNS server used by the DHCP service.	[Example] 2001::1
Secondary DNS Server	Alternative DNS server used by the DHCP service.	[Example] 2001::2
Lease Time	Address lease period. In general, terminal devices automatically renews the lease in connected state to keep the IP address unchanged. If the lease is not renewed due to disconnection or network instability, the IP addresses are reclaimed after the lease expires. When the terminal devices recover connectivity, they will request the addresses again.	[Example] 1 hour

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

Address Pool

<input type="checkbox"/>	Type	Prefix	Available Prefix Length	Operation
No Data				

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

Create Address Pool

* Type Network Address Prefix

* Prefix

Available Prefix Length

- e Click **Save**.

4. Follow-up Procedure

If only one row is left in the DHCP service list, and you want to delete the address pool, you need to disable the DHCP server first.

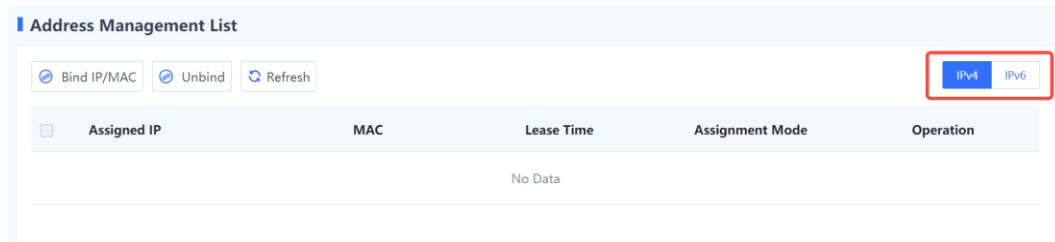
8.14.3 Address Management List

Application Scenario

You can view the IP addresses allocated by the DHCP server on the **Address Management List** page.

Procedure

- (5) Choose Network > DHCP > Address Management List.
- (6) Click **IPv4** or **IPv6** in the upper-right corner to view assigned IPv4 or IPv6 addresses.



(7) Process the IP addresses.

- Select addresses and click **Bind IP/MAC** or **Bind** in the **Operation** column to fixedly allocate IP addresses to the hosts with the corresponding MAC addresses.
- Select addresses and click **Unbind** to cancel the binding relationship between IP addresses and MAC addresses.

8.15 Blocklist and Allowlist

8.15.1 Overview

Z-S series firewalls support blocklist and allowlist to block or forward packets based on IP addresses.

- Allowlist

After the specified IP address is added to the allowlist, the firewall directly forwards the packets sent to or from the address, without performing security check, thus implementing high-speed packet forwarding.

For example, if you do not want to enforce security policies or anti-DoS/DDoS policies on some IP addresses (such as the administrator's address) on the network, you can add the IP addresses to the allowlist.

- Blocklist

After an IP address is added to the blocklist, the packets sent to or from the address will be discarded by the device.

For example, if you want to prevent traffic of some IP addresses (such as attackers' addresses) on the network from passing the device, add the IP addresses to the blocklist.

Caution

The IP addresses in blocklist cannot be used to log in to the firewall.

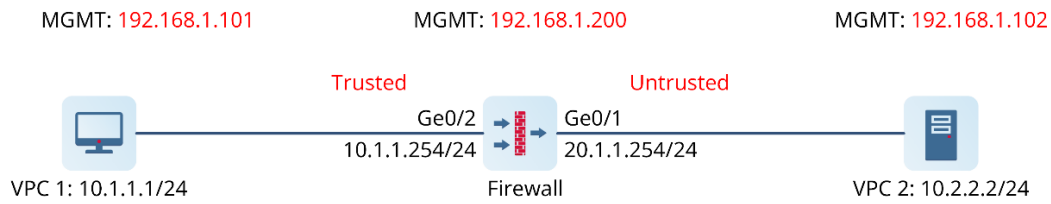
- Temporary blocklist

The temporary blocklist has the same function as the blocklist, but the temporary blocklist is valid for only a period of time. When the validity period expires, the blocklist becomes invalid and is automatically deleted.

When traffic hits a brute-force IPS policy, a temporary blocklist is automatically generated. The block period is the block period of the rules of brute-force IPS policy. You can also manually configure a temporary blocklist.

8.15.2 Precautions

RG-WALL 1600-Z-S series firewalls configure the blocklist and allowlist for source and destination separately. If a blocklist or allowlist needs to take effect on both the incoming and outgoing packets of an IP address, you need to add the IP address to the blocklist or allowlist of both the source and destination.



As shown in the above figure, the source address range in the security policy includes an allowlist and the security policy action is deny. If the source IP address 10.1.1.1 is in the allowlist and needs to access 10.2.2.2, consider the following two situations:

- When NAT is not configured, add destination IP address 10.2.2.2 to the blocklist and allowlist of both source and destination.
- When NAT is configured, the IP addresses will be translated. If you only add the original IP address to blocklist or allowlist, the bidirectional traffic of the IP address cannot be blocked or allowed after address translation. You also need to add the translated public address to the blocklist or allowlist. For example, when source NAT is configured, to allow all traffic of IP address 10.2.2.2 (20.1.1.254 after NAT), you need to add 10.2.2.2 to the source allowlist to allow incoming packets and add 20.1.1.254 to the destination allowlist to allow outgoing packets. (Note: This restriction will be eliminated in later versions.)

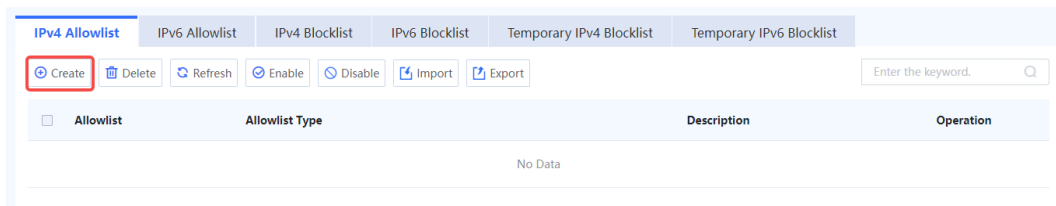
8.15.3 Creating an IPv4 Allowlist

Application Scenario

Configure an IPv4 allowlist on the web UI.

Procedure

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



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

< Back

Add Allowlist

IP Type IPv4

Allowlist Type Src. Address Dest. Address

* 🔔 IP Address/Range

Description

Item	Description	Remarks
Allowlist Type	Type of the allowlist: <ul style="list-style-type: none"> ● Src. Address: Permit packets sent from this address. ● Dest. Address: Permit packets sent to this address. 	[Example] Src. Address
IP Address/Range	Allowlist IP address/range.	The following three formats are supported: <ul style="list-style-type: none"> ● Single IP address: 192.168.1.1 ● Subnet: 192.168.1.0/24 ● IP address range: 192.168.1.1-192.168.1.10

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

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

📄 Create
🗑️ Delete
🔄 Refresh
🟢 Enable
🔴 Disable
📄 Import
📄 Export

Enter the keyword. 🔍

☐	Allowlist	Allowlist Type	Description	Operation
☐	172.26.1.19	Src. Address	-	🟢 Edit 🗑️ Delete

Follow-up Procedure

- To delete multiple allowlist policies in a batch, select the policies that you want to delete and click **Delete**.
- To enable multiple allowlist policies in a batch, select the policies that you want to enable and click **Enable**.
- To disable multiple allowlist policies in a batch, select the policies that you want to disable and click **Disable**.
- To export all allowlist configurations, click **Export**.
- Click **Import** to download the import template and upload the configured file, or directly select the CSV file to be uploaded. Then, click **Confirm** to start the import task.
- Enter the allowlist IP address, full or part of the allowlist description in the search box to search for the policies. Fuzzy search is supported.

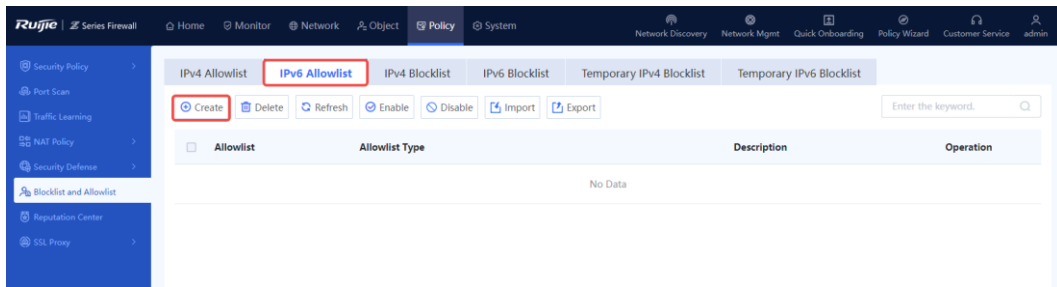
8.15.4 Creating an IPv6 Allowlist

Application Scenario

Configure an IPv6 allowlist on the web UI.

Procedure

- (1) Access the **Add Allowlist** page.
 - a Choose **Policy > Blocklist and Allowlist > IPv6 Allowlist**.
 - b Above the operation area, click **Create**.



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

< Back
Add Allowlist

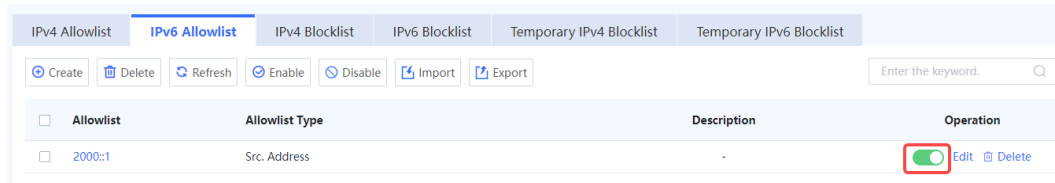
IP Type IPv6

Allowlist Type Src. Address Dest. Address

*

Item	Description	Remarks
Allowlist Type	Type of the allowlist: <ul style="list-style-type: none"> ● Src. Address: Permit packets sent from this address. ● Dest. Address: Permit packets sent to this address. 	[Example] Src. Address
IP Address/Range	Allowlist IP address/range.	The following three formats are supported: <ul style="list-style-type: none"> ● Single IP address: 1234::100 ● Subnet: 1234:100::/64 ● IP address 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.

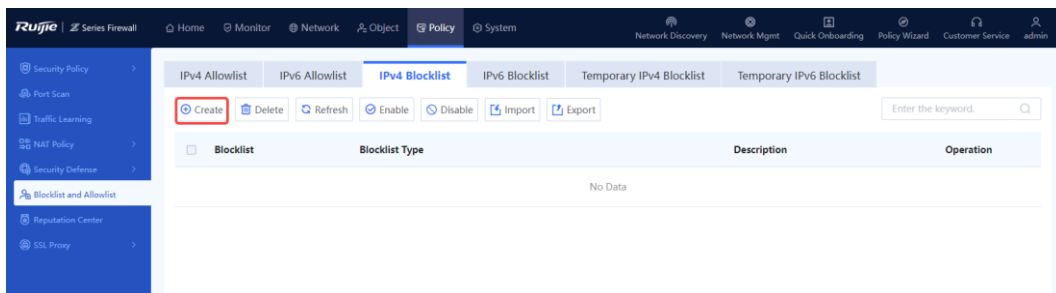
8.15.5 Creating an IPv4 Blocklist

Application Scenario

Configure an IPv4 blocklist on the web UI.

Procedure

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



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

< Back

Add Blocklist

IP Type IPv4

Blocklist Type Src. Address Dest. Address

*

Description

Item	Description	Remarks
Blocklist Type	Type of the blocklist: <ul style="list-style-type: none"> ● Src. Address: Block packets sent from this address. ● Dest. Address: Block packets sent to this address. 	[Example] Src. Address
IP Address/Range	Blocklist IP address/range.	The following three formats are supported: <ul style="list-style-type: none"> ● Single IP address: 192.168.1.1 ● Subnet: 192.168.1.0/24 ● IP address range: 192.168.1.1-192.168.1.10

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

IPv4 Allowlist

IPv4 Blocklist

IPv6 Allowlist

IPv6 Blocklist

Temporary IPv4 Blocklist

Temporary IPv6 Blocklist

	Blocklist	Blocklist Type	Description	Operation
<input type="checkbox"/>	1.1.1.1	Src. Address	-	<input checked="" type="checkbox"/> Edit Delete

Follow-up Procedure

- To delete multiple blocklist policies in a batch, select the policies that you want to delete and click **Delete**.
- To enable multiple blocklist policies in a batch, select the policies that you want to enable and click **Enable**.
- To disable multiple blocklist policies in a batch, select the policies that you want to disable and click **Disable**.
- To export all blocklist configurations, click **Export**.
- Click **Import** to download the import template and upload the configured file, or directly select the CSV file to be uploaded. Then, click **Confirm** to start the import task.
- Enter the blocklist IP address, full or part of the blocklist description in the search box to search for the policies. Fuzzy search is supported.

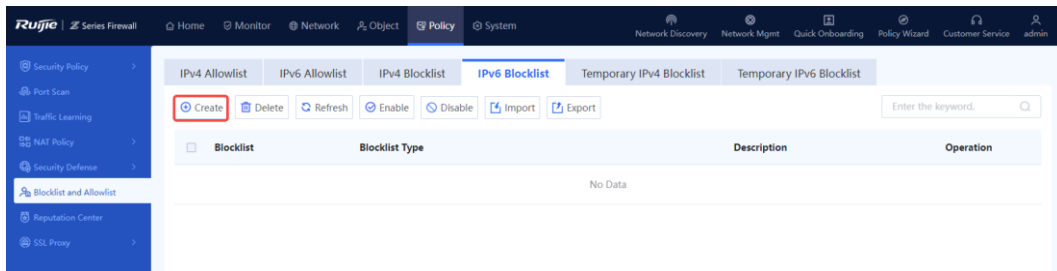
8.15.6 Creating an IPv6 Blocklist

Application Scenario

Configure an IPv6 blocklist on the web UI.

Procedure

- (1) Access the **Add Blocklist** page.
 - a Choose **Policy > Blocklist and Allowlist > IPv6 Blocklist**.
 - b Above the operation area, click **Create**.



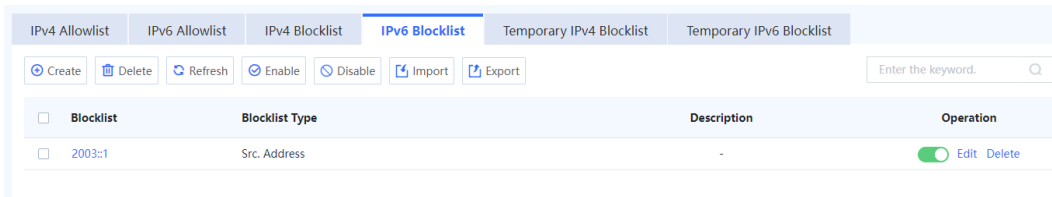
- (2) Set parameters for the blocklist policy and click **Save**.

The screenshot shows the 'Add Blocklist' configuration form. It includes a 'Back' button, a title 'Add Blocklist', and several configuration options:

- IP Type:** IPv6
- Blocklist Type:** Radio buttons for 'Src. Address' (selected) and 'Dest. Address'.
- IP Address/Range:** A text input field with a red asterisk and an information icon.
- Description:** A larger text input area.

Item	Description	Remarks
Blocklist Type	Type of the blocklist: <ul style="list-style-type: none"> ● Src. Address: Block packets sent from this address. ● Dest. Address: Block packets sent to this address. 	[Example] Src. Address
IP Address/Range	Blocklist IP address/range.	The following three formats are supported: <ul style="list-style-type: none"> ● Single IP address: 1234::100 ● Subnet: 1234:100::/64 ● IP address 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.

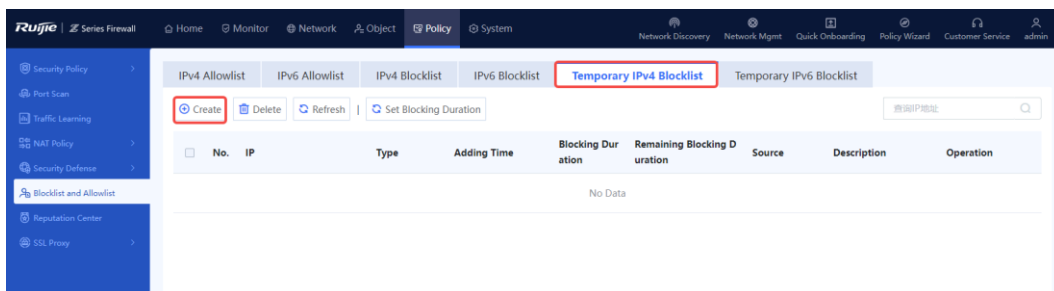
8.15.7 Creating a Temporary IPv4 Blocklist

Application Scenario

Configure a temporary IPv4 blocklist on the web UI.

Procedure

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



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

< Back

Add Temporary Blocklist

IP Type IPv4

Blocklist Type Src. Address Dest. Address

* i IP Address/Range

Blocking Duration Minute (Range: 3 min to 15 days)

Description

Item	Description	Remarks
Blocklist Type	Type of the temporary blocklist: <ul style="list-style-type: none"> ● Src. Address: Block packets sent from this address. ● Dest. Address: Block packets sent to this address. 	[Example] Src. Address
IP Address/Range	Temporary blocklist IP address/range.	The following three formats are supported: <ul style="list-style-type: none"> ● Single IP address: 192.168.1.1 ● Subnet: 192.168.1.0/24 ● IP address range: 192.168.1.1-192.168.1.10
Blocking Duration	Validity period of the temporary blocklist. When the validity period expires, the blocklist becomes invalid and is automatically deleted.	[Example] 5 minutes
Description	Description of the temporary blocklist.	Characters such as `~!#%^&*+ {};:"/<>?` are not allowed.

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

Follow-up Procedure

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

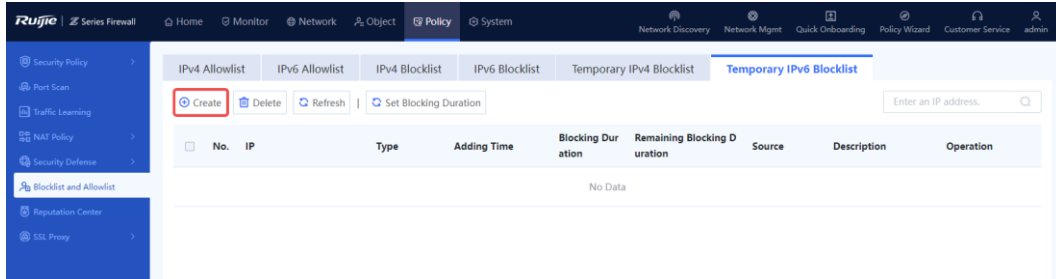
8.15.8 Creating a Temporary IPv6 Blocklist

Application Scenario

Configure a temporary IPv6 blocklist on the web UI.

Procedure

- (1) Access the Add Temporary Blocklist page.
 - a Choose **Policy > Blocklist and Allowlist > Temporary IPv6 Blocklist**.
 - b Above the operation area, click **Create**.



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

< Back

Add Temporary Blocklist

IP Type IPv6

Blocklist Type Src. Address Dest. Address

*

Blocking Duration (Range: 3 min to 15 days)

Description

Item	Description	Remarks
Blocklist Type	Type of the temporary blocklist: <ul style="list-style-type: none"> ● Src. Address: Block packets sent from this address. ● Dest. Address: Block packets sent to this address. 	[Example] Src. Address
IP Address/Range	Temporary blocklist IP address/range.	The following three formats are supported: <ul style="list-style-type: none"> ● Single IP address: 1234::100 ● Subnet: 1234:100::/64 ● IP address range: 1234::100-2345::100

Item	Description	Remarks
Blocking Duration	Validity period of the temporary blocklist. When the validity period expires, the blocklist becomes invalid and is automatically deleted.	[Example] 5 minutes
Description	Description of the temporary blocklist.	Characters such as `~!#%^&*+ \ {};:'"/<>? are not allowed.

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

Follow-up Procedure

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

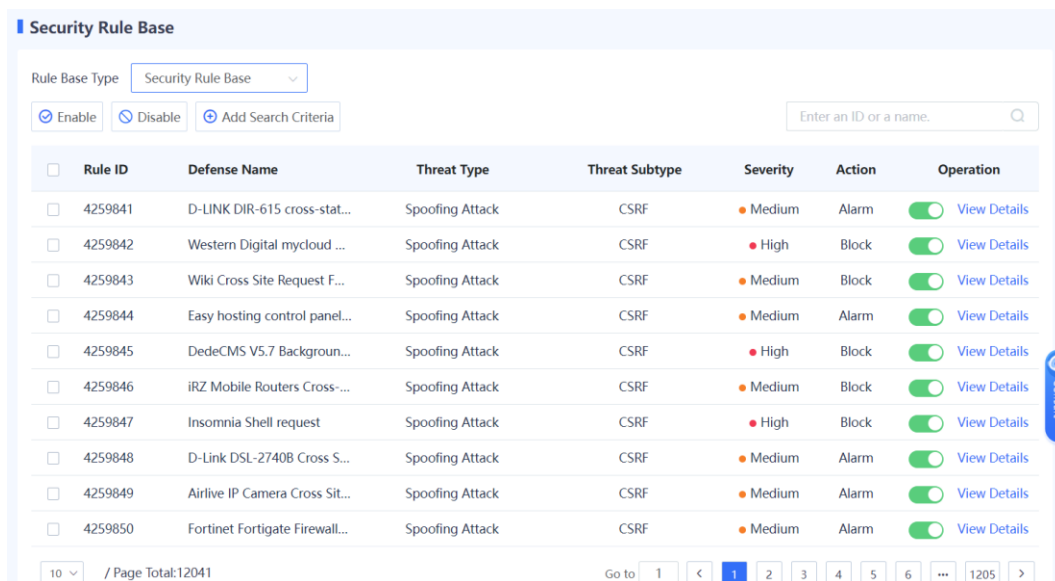
8.16 Security Rule Base Management

Application Scenario

The security rule base stores information about the features of the threats that can be detected from traffic. When traffic passes through the device, intrusion prevention matches the traffic against features in the security rule base. If matched, the device processes it according to user configuration.

Procedure

(1) Choose Object > Security Rule Base.



(2) Enable or disable a security rule.

- After a rule is enabled, the device detects the threats defined by the rule for the traffic passing the device.
- After a rule is disabled, the device does not detect the threats defined by the rule for the traffic passing the device.

8.17 Connecting to Ruijie Cloud

8.17.1 Overview

Ruijie Cloud is a remote management platform that manages all links and devices (such as gateway, switch, AP, and firewall) in SMB scenarios. The administrator can add devices to the Ruijie Cloud, and then manage the devices anytime, anywhere.

Note

You can bind a device to the Ruijie Cloud platform when the device is quickly online. If it is not bound, follow the steps described in this section to bind it.

8.17.2 Connecting to Ruijie Cloud

1. Enabling Ruijie Cloud

Application Scenario

Based on the Ruijie Cloud platform, you can view the basic information of devices (including software version, hardware version, MAC address, and product model), upgrade the devices, view the interface information of the devices, open reverse tunnels, and remotely control the devices through the devices' EWEB function.

Procedure

- (1) Choose System > Cloud Management Platform > Ruijie Cloud.
- (2) Enable **Ruijie Cloud-based Management** (enabled by default). Then you can manage the firewall on Ruijie Cloud.



2. Binding Devices

Application Scenario

Before managing the firewall using Ruijie Cloud, you need to bind the firewall. After the firewall is bound, you can view device information and maintain the firewall on Ruijie Cloud.

You can register a Ruijie Cloud account at <https://cloud.ruijienetworks.com> and bind devices on the platform.

8.17.3 Operations on Ruijie Cloud

1. Viewing Device Information

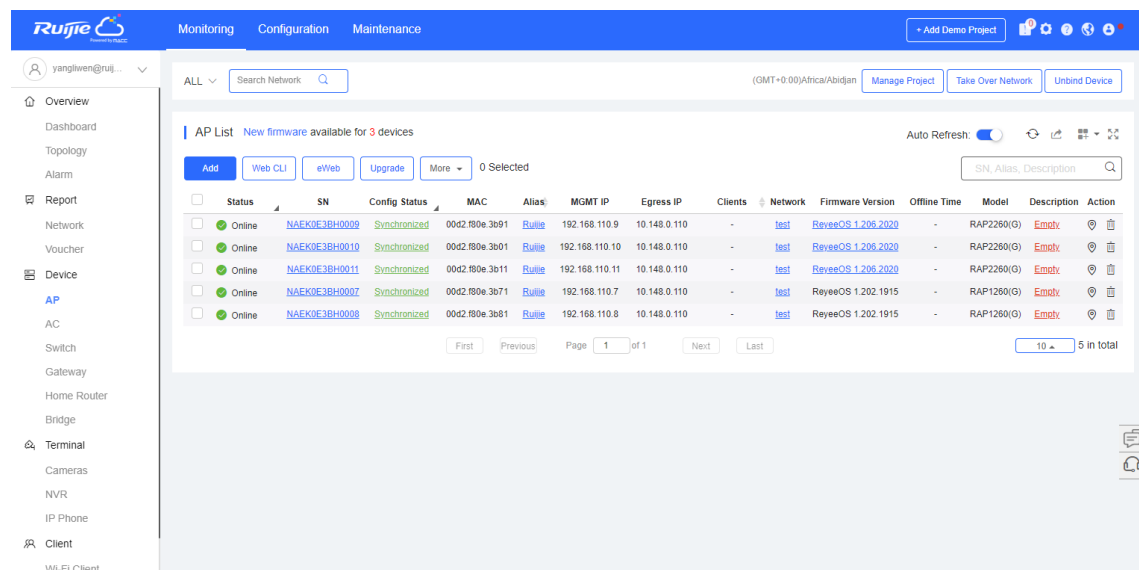
Application Scenario

After enabling Ruijie Cloud, enter the address of Ruijie Cloud platform in the browser, log in, and then you can view device information, online status, and interface information.

Procedure

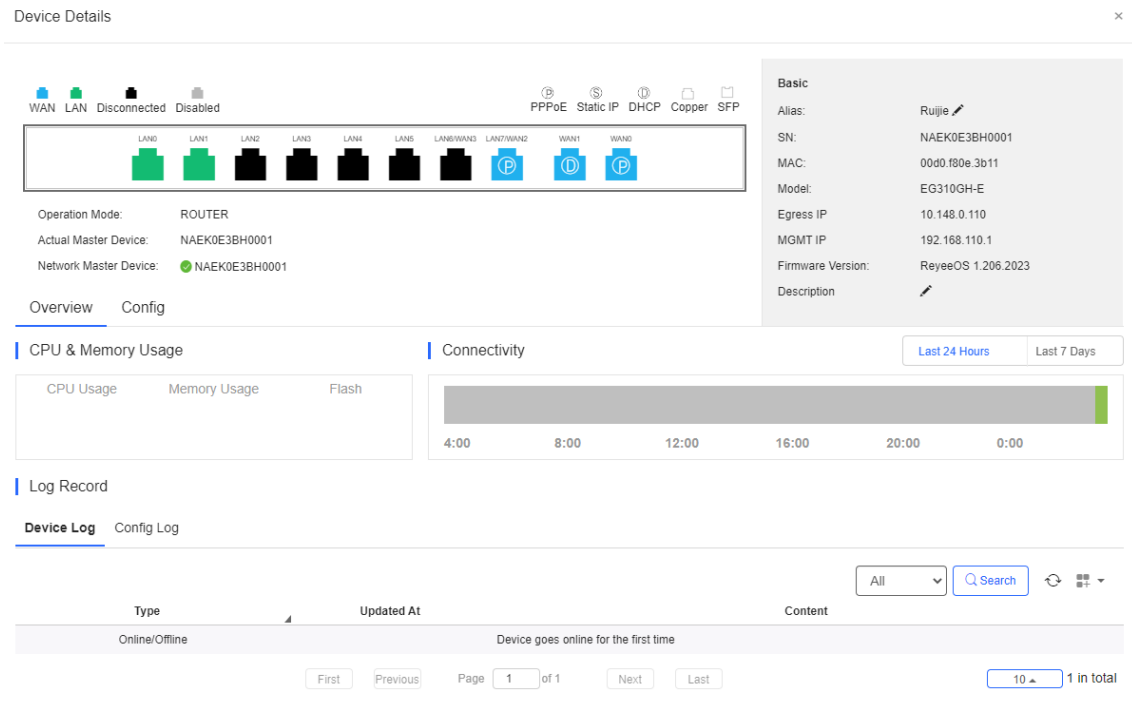
- (1) Choose **Monitoring > Device > Firewall** to open the device list.
- (2) View device details.

Figure 8-7 Firewall Details



The system displays the basic device information such as status, SN, device, management address, software version, and device model.

- (3) Click **SN** to enter the device management page. View device basic information, panel information, interface information, and status.



You can click the titles one by one to manage devices.

- Device panel: includes information such as interface distribution on panel.
- Basic information: includes device name, device model, SN, MAC address, and software version.
- Status: includes CPU and memory usage, offline status, and connectivity status.
- Interface information: By clicking the titles in status information, you can view detailed interface information, such as WAN/LAN port information (such as port number, mode, and subnet mask).

Figure 8-8 Device Panel Information

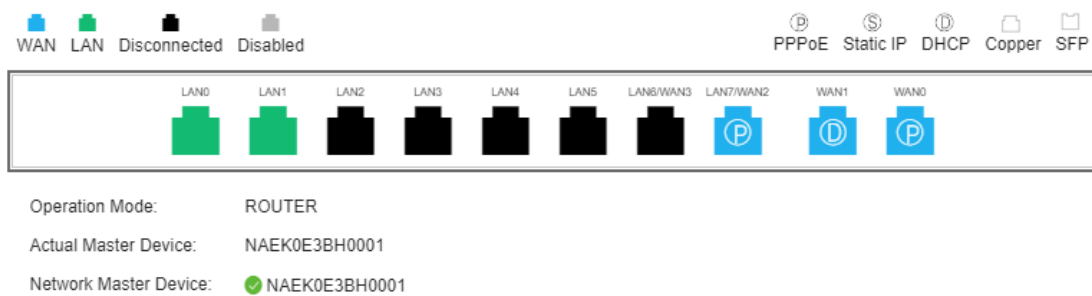


Figure 8-9 Basic Information

Basic

Alias: Ruijie 

SN: NAEK0E3BH0001

MAC: 00d0.f80e.3b11

Model: EG310GH-E

Egress IP: 10.148.0.110

MGMT IP: 192.168.110.1

Firmware Version: ReyeeOS 1.206.2023

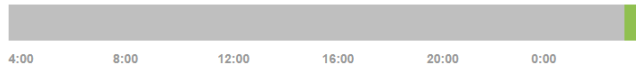
Description 

Figure 8-10 Status Information

Overview **Config**

CPU & Memory Usage **Connectivity** Last 24 Hours Last 7 Days

CPU Usage Memory Usage Flash



4:00 8:00 12:00 16:00 20:00 0:00

Figure 8-11 Interface Information

概览 **WAN** LAN 隧道管理

端口信息 Ge0/2

基本信息

模式: 路由模式

IP: --

子网掩码: --

IP地址类型: 其他类型

上行带宽: 100000kbps

下行带宽: 100000kbps

运营商: --

省份: --

城市: --

子接口信息

子接口名称	VLAN	IP地址
Ge0/2.101	101	--
Ge0/2.102	102	--

2. Managing Tunnels

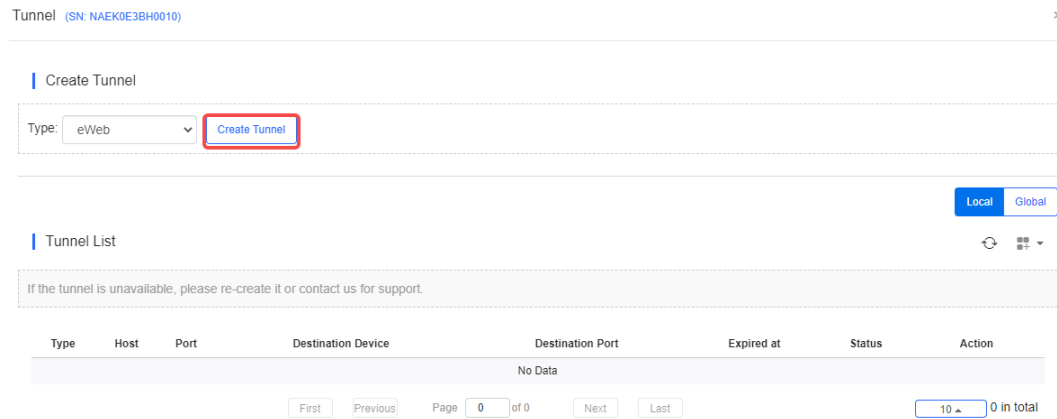
- (1) Click **Tunnel** or **eWeb** to access the EWEB page of the device.

Figure 8-12 Tunnel Management



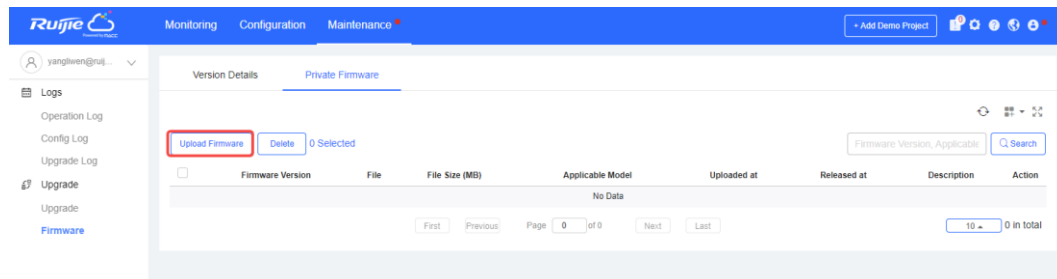
(2) To add a tunnel, click **Create Tunnel**.

Figure 8-13 Creating a Tunnel

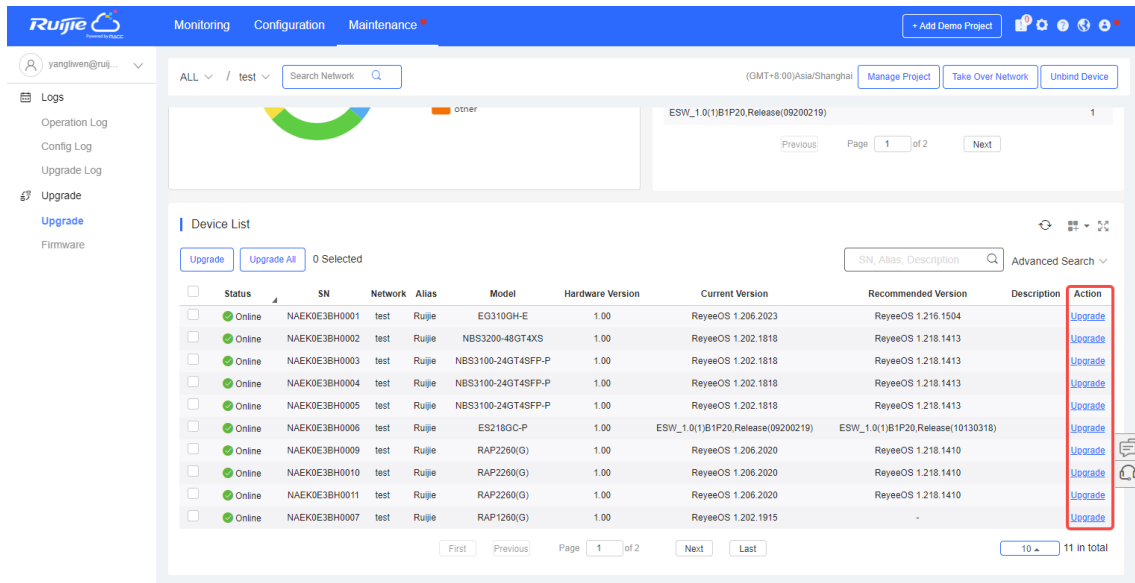


3. Upgrading Device Software/Firmware

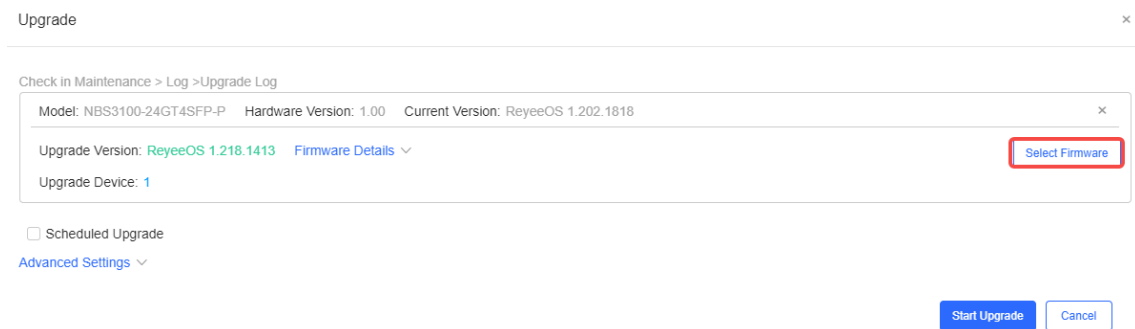
- (1) Choose Maintenance > Upgrade > Firmware > Private Firmware.
- (2) Click **Upload Firmware** to upload the software version/firmware version.



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



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

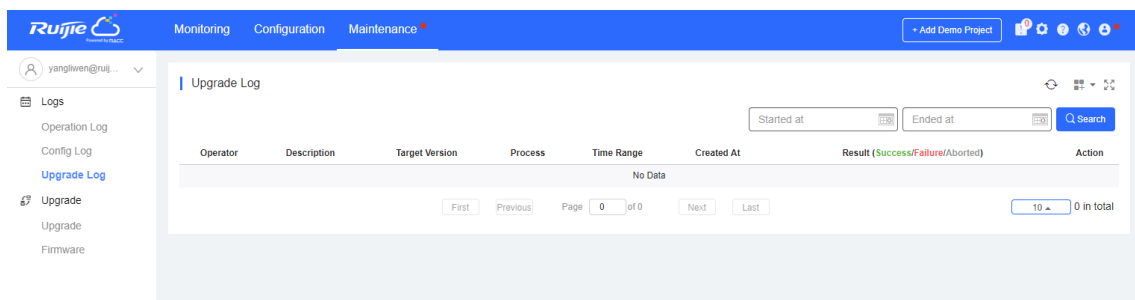


(5) Click **Start Upgrade** to start the upgrade.

Then the device performs upgrade. During the upgrade, the device will automatically restart. Wait until the upgrade is completed.

(6) When the upgrade is finished, choose **Maintenance > Logs > Upgrade Log** to view the upgrade result.

Figure 8-14 Upgrade Result



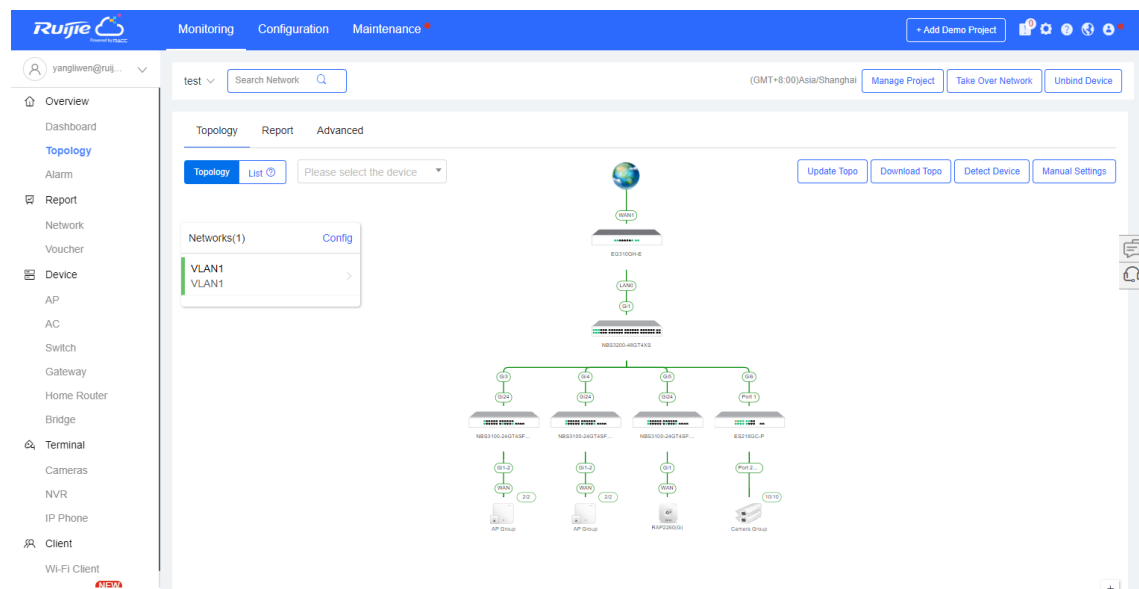
4. Viewing Network Topology

The relationships between the firewall and other network devices can be discovered on Ruijie Cloud and the topology is generated.

⚠ Caution

- When there are multiple default routes on the firewall, or when both bridge interfaces and routing interfaces are used, you will find that the topology on Ruijie Cloud is abnormal.
- When the firewall is in transparent mode, port 0/MGMT does not need to be connected separately.

Choose **Monitoring > Overview > Topology** to view the topology of firewall and other network devices.



Follow-up Procedure

- To obtain the latest topology, click **Update Topo**.
- To download the network topology, click **Download Topo**.
- To edit the topology and add the devices that are not discovered automatically, click **Manual Settings**.

8.18 DNS Server

8.18.1 Configuring DNS

Application Scenario

The Domain Name System (DNS), a distributed database on the Internet that provides mutual mapping between domain names and IP addresses, makes it easier for users to access the Internet without having to memorize IP strings that can be directly read by machines. Domain name resolution (or host name resolution) is a process where the IP address corresponding to a given host name is finally obtained.

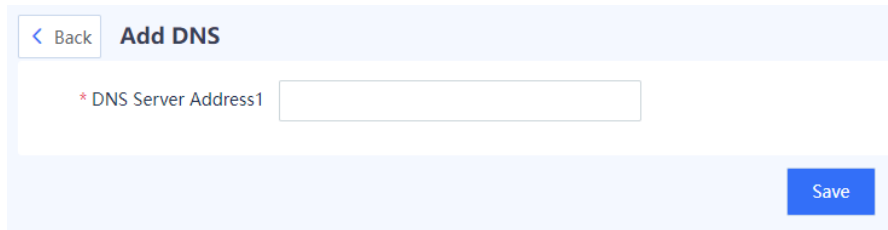
Prerequisites

The system supports at most three DNS servers. DNS server 1 has the highest priority and DNS server 3 has the lowest priority. The system uses the server with the highest priority first.

Procedure

- (1) Choose **Network > DNS**.
- (2) Set the IP address of DNS server 1.
 - a Click **Create**.

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



The screenshot shows a web interface for adding a DNS server. At the top left is a '< Back' button. The main title is 'Add DNS'. Below the title is a text input field with a red asterisk and the label '* DNS Server Address1'. At the bottom right is a blue 'Save' button.

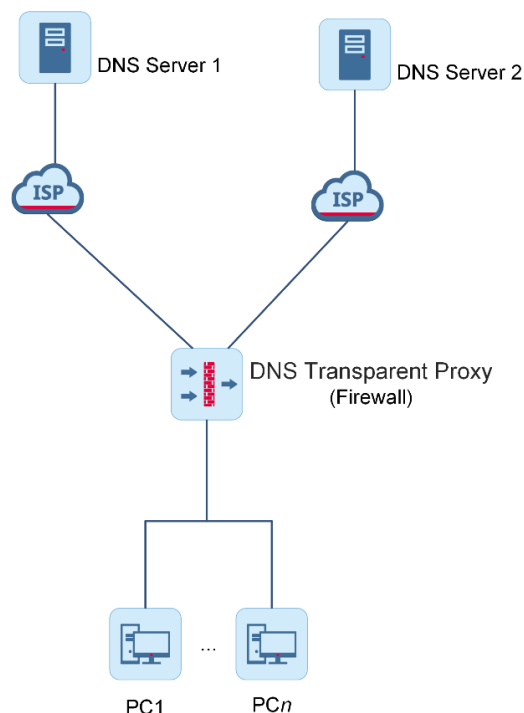
- b Enter the IP address of the DNS server 1 in the **DNS Server Address1** input box.
 - c Click **Save**.
- (3) (Optional) If multiple DNS servers are configured in the network environment, you can set the IP address for the second or third DNS server.

8.18.2 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 proxy is typically applied in multi-egress scenarios. For details about multi-egress load balancing, see [8.23 Outbound Interface Load Balancing](#).



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 hits the DNS transparent proxy policy. If the policy is hit and DNS transparent proxy needs to be performed, the device first determines whether the domain name to be resolved is an excluded domain name. If so, the device does not perform DNS transparent proxy. (For excluded domain names that require a specific DNS server for resolution, the device changes the destination address in the DNS request packet to the address of the specific DNS server.) If it is not an excluded domain name, the device adds a proxy flag to the packet for judgment in the subsequent process.
- (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: DNS transparent proxy, intelligent routing, egress load balancing, and static/dynamic routing.

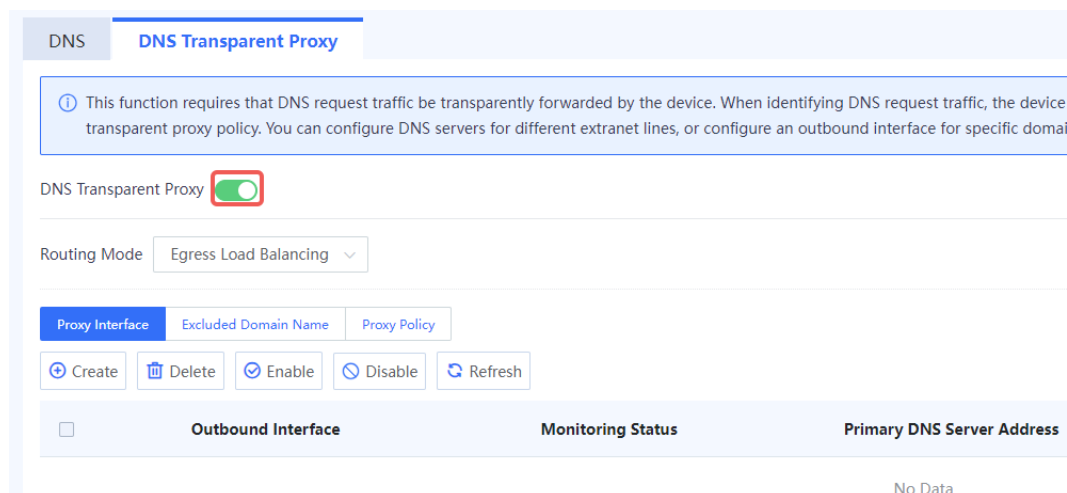
The DNS transparent proxy has the highest priority. Therefore, if the DNS transparent proxy policy is hit, the destination address is directly modified, and the packet will not be forwarded to the dynamic NAT processing module.

- (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

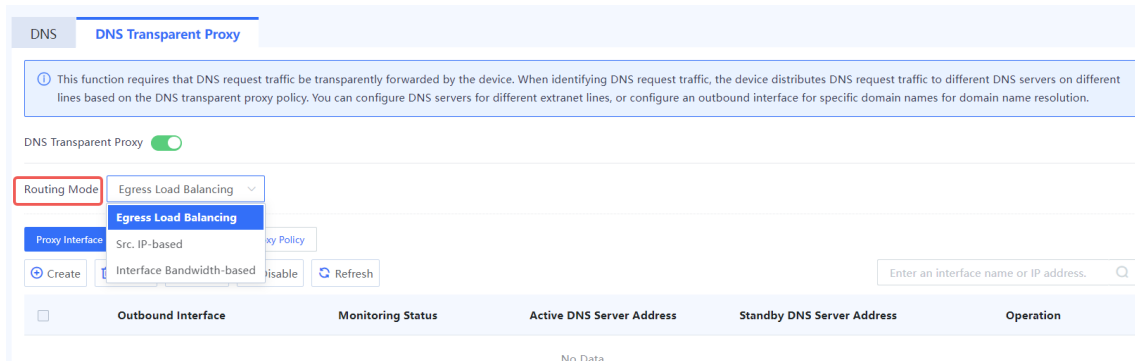
Procedure

- (1) Choose Network > DNS > DNS and click the DNS Transparent Proxy tab.
- (2) Toggle on the switch to enable DNS transparent proxy.



- (3) Set the routing mode.

When the device implements DNS transparent proxy and a DNS request packet hits the proxy policy, if the matched domain name is not excluded and is associated with multiple available interfaces or if the matched interface list contains multiple available interfaces, you need to configure the routing mode for the device to select an outbound interface for the DNS request packet.



Item	Description
Interface Bandwidth-based	A proxy outbound interface is selected for DNS request packets based on the interface bandwidth (downlink load). Other traffic is forwarded based on the forwarding mode described in 8.23 Outbound Interface Load Balancing .
Egress Load Balancing	DNS request packets and other traffic are forwarded based on the forwarding mode described in 8.23 Outbound Interface Load Balancing .
Src. IP-based	A proxy outbound interface is selected for DNS request packets based on the source IP address. DNS request packets with the same source address are forwarded by the same outbound interface. Other traffic is forwarded based on the forwarding mode described in 8.23 Outbound Interface Load Balancing .

(4) Configure DNS proxy parameters.

- Configure a proxy interface.
 - a Click **Create**.



- b Create a DNS proxy interface.

< Back
Add Proxy Interface

* Outbound Interface

* Primary DNS Server Address

Secondary DNS Server Address

DNS Probe [Add Link Detection](#)

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.

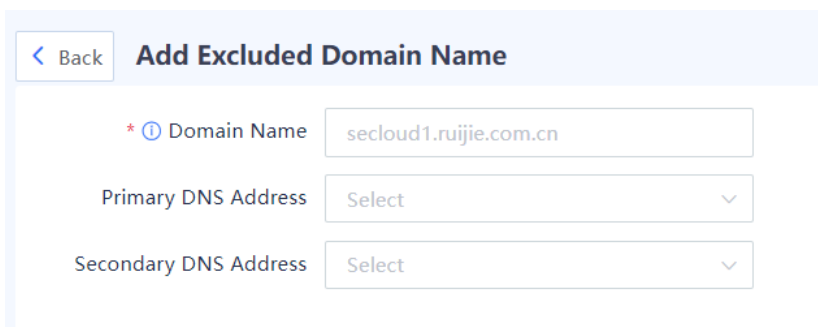
Item	Description	Remarks
DNS Probe	Select or create DNS link detection. The detection result is displayed in the lower part of the page. For link detection, the minimum number of survivability nodes needs to be configured. In primary/secondary DNS link detection, if the minimum number of survivability 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 8.22 Link Detection .

- c Click **Save**.
- Configure excluded domain names.
 - a Click **Create**.



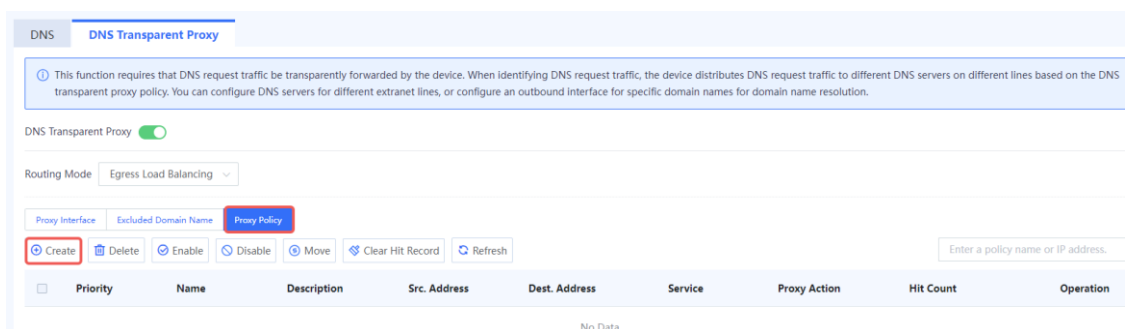
- b Add an excluded domain name.

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	<p>DNS domain name exclusion provides three matching modes:</p> <p>Exact match: Enter the complete domain name, such as www.ruijie.com.</p> <p>Prefix match: Enter an incomplete domain name ended with an asterisk (*), for example, www.ruijie.*.</p> <p>Suffix match: Enter an incomplete domain name started with an asterisk (*), for example, *.ruijie.com.</p> <p>The matching priorities in descending order are as follows: exact match, suffix match, and prefix match. Fuzzy match in other formats is not supported.</p>	<p>[Example]</p> <p>www.test.com</p>
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**.
- Configure a proxy policy.
 - a Click **Create**.



b Configure a proxy policy.

< Back

Add Proxy Policy

Basic Info

* Name

Enabled State Enable Disable

Adjacent Policy

Description

Src. and Dest.

* Src. Address

* Dest. Address

* Service

Action Settings

Proxy Action Proxy No Proxy

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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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**.

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.

8.18.3 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 extranet 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 extranet 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

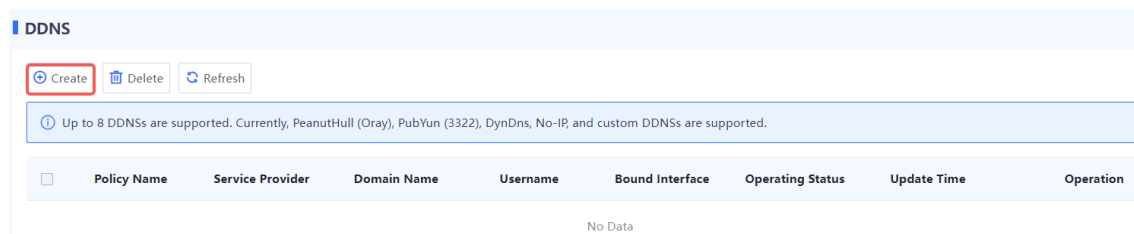
Configure a DDNS policy on the outbound interface of the firewall so that the firewall can act as a DDNS client. If the IP address of the device interface is updated, the firewall sends a request to the DDNS server to update the mapping between the domain name and IP address.

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.
- 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.

Create DDNS Policy ⊗

* Policy Name

* Service Provider ▾

* Username

* Password

* ⓘ Bound Interface ▾

* Domain Name

Item	Description	Remarks
Policy 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.	<ul style="list-style-type: none"> ● A physical interface, subinterface, 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
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.

8.19 Intelligent Routing

Application Scenario

Intelligent Routing, also called policy-based routing (PBR) or application-based routing, is a mechanism for routing and forwarding based on user-specified policies. By using intelligent routing, you can redirect the packets that meet the matching conditions to the specified outbound interface and next hop.

After PBR is configured, the device first filters the packets according to the configured rules, and then forwards the matched packets according to the specified forwarding policy. PBR creates rules according to specific fields (source or destination IP address and protocol type) in the data packets, and forwards the data packets through a specific interface.

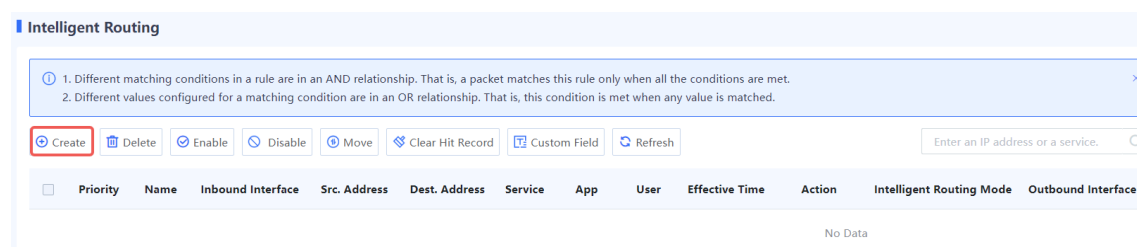
In a multi-path scenario where no routing rules are configured, if the device is connected to different service networks through different paths, the traffic will be evenly routed over the paths. In this situation, the access data to service networks may be incorrectly sent to other networks, causing a network abnormality. You can configure PBR to control data isolation and forwarding among networks.

Note

- PBR is supported from NTOS1.0R3. If your version is lower than NTOS1.0R3, upgrade it to NTOS1.0R3 or higher.
- Application routing is supported from NTOS1.0R4. If your version is lower than NTOS1.0R4, upgrade it to NTOS1.0R4 or higher.

Procedure

- (1) Choose **Network > Routing > Intelligent Routing**.
- (2) Click **Create** to enter the Create Intelligent Routing page.



- (3) Set parameters of intelligent routing.

Back
Create Intelligent Routing

Basic Info

* Name

Enabled State Enable Disable

Adjacent Policy Select a policy. Before

Description

Matching Conditions

Inbound Interface Select an inbound interface or sourc...

Src. Address Select the source address.

Dest. Address Select the destination address.

Service Select a service.

User Select a user.

App Select an application.

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

Action Settings

Action Option Forwarding No Intelligent Routing

Outbound Interface Type Single Interface Multiple Interfaces

* Intelligent Routing Mode Based on Src. IP Hash

Outbound Interface List

Create
Delete
Refresh

	Interface	Next-Hop Address	Uplink Load Threshold	Downlink
No Data				
Total: 0				

Link Detection Link Detection [Add Link Detection](#)

Save

Item	Description	Remarks
Basic Info		
Name	Name of intelligent routing.	Characters such as `~!#%^&*+√0::"/<>? and spaces are not allowed. [Example] Policy_1
Enabled State	Whether to enable the new intelligent routing.	[Example] Enabled

Item	Description	Remarks
Adjacent Policy	Move the new policy before or after the specified policy. The closer a policy is to the front, the higher its priority is in matching.	-
Description	Route description.	Characters such as `~!#%^&*+ {};:'''/<>?` are not allowed.
Matching Conditions		
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
Src. Address	Forwards the packets from this source address or address group based on the policy.	Click the drop-down list, and select a source address in the To-be-selected area. The selected address is automatically added to the Selected area. [Example] any
Dest. Address	Forwards the packets to this destination address or address group based on the policy.	Click the drop-down list, and select a destination address in the To-be-selected area. The selected address is automatically added to the Selected area. [Example] any
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. [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. [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. [Example] any
Effective Time	Time range in which the intelligent routing is effective.	[Example] any
Action Settings		
Action Option	Whether to forward the matched packets based on the policy. If forwarded, you need to configure Outbound Interface and Next-Hop Address .	[Example] Forwarding
Outbound Interface Type	<ul style="list-style-type: none"> ● Single Interface: A single outbound interface needs to be configured. ● Multiple Interfaces: Multiple outbound interfaces need to be configured. 	[Example] Single Interface
Intelligent Routing Mode	If the outbound interface 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 Link Weight
Outbound Interface List		
If the outbound interface type is Multiple Interfaces , you also need to configure an outbound interface list.		
Interface Name	Name of an outbound interface.	[Example] Ge0/0

Item	Description	Remarks
Next-Hop Address	Next-hop address for data forwarding. Typically, the address of the next-hop routing device is configured.	[Example] 192.168.1.1 or 1234::100
Uplink Load Threshold	When the uplink bandwidth usage exceeds the load threshold, the interface does not participate in load balancing.	-
Downlink Load Threshold	When the downlink bandwidth usage exceeds the load threshold, the interface does not participate in load balancing.	-
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. Connections	Maximum number of connections on the outbound interface. If the number of connections established on the interface exceeds the maximum number, traffic is forwarded based on the routing priority in the routing table.	[Example] 1
Link Detection	Link detection policy associated with outbound interface. This configuration can detect the network connectivity between the outbound interface and the next hop in real time. If the network connection between the outbound interface and the next hop is abnormal, this route becomes invalid.	For details about link detection, see 8.22 Link Detection .

(4) Click **Save**.

8.20 Address Library Routing (ISP-based Routing)

8.20.1 Overview

The ISP address library stores all the IP addresses on ISP's network. After the ISP address library is configured and bound to the device's WAN interface, the route to the corresponding ISP's IP address is generated, so that the packets destined for the ISP's network are forwarded through the corresponding outbound interface, meeting the ISP-based routing requirements in multi-egress scenarios and optimizing the forwarding path of traffic.

To customize an ISP address library, you can add routes or import routes in file format to the library.

8.20.2 Configuring an ISP Address Library

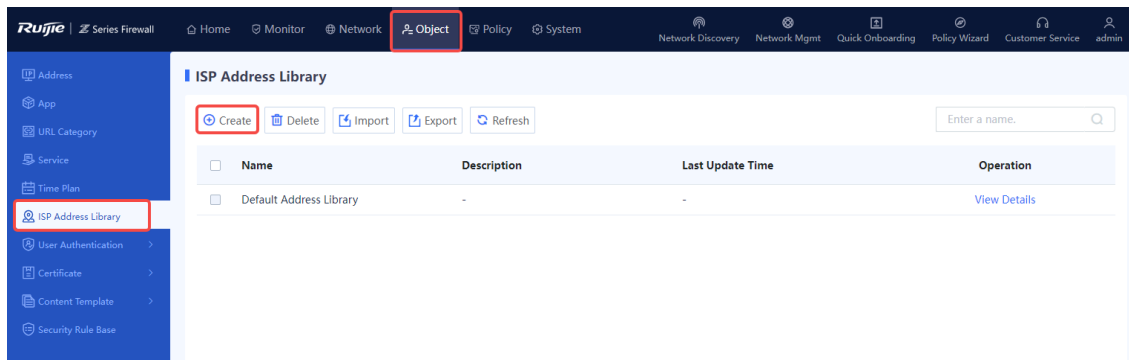
1. Creating an ISP Address Library Manually

Application Scenario

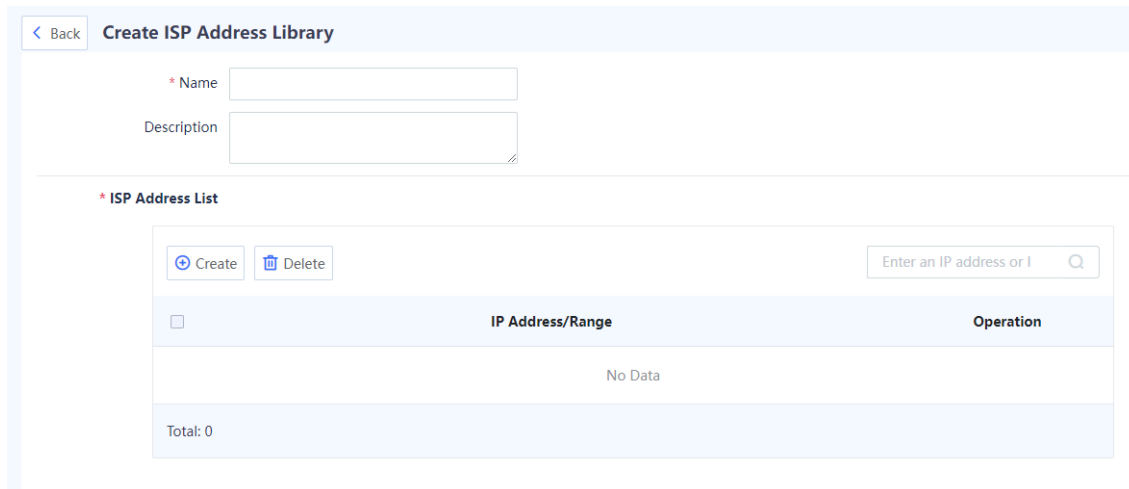
You can add addresses to the ISP address library one by one. This method is applicable to the address library containing a few addresses.

Procedure

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



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



Item	Description	Remarks
Name	Name of the ISP address library.	Characters such as `~!#%^&*+ {};:'"/<>?` and spaces are not allowed. [Example] Address library 1
Description	Description of the ISP address library.	Characters such as `~!#%^&*+ {};:'"/<>?` are not allowed. [Example] Address library 1
ISP Address List	IP addresses contained in the address library.	Click Create to enter a single IP address or an IP address range. Three configuration methods are supported: <ul style="list-style-type: none"> ● IP address: One or multiple IP addresses. Input an IP address per line. Press Enter to separate lines. Example: 192.168.20.3 ● IP address range: A contiguous range of addresses. Connect the start IP address and end IP address with a hyphen (-). Example: 192.168.20.1-192.168.20.3. ● Network segment: IP address network segment. Example: 192.168.1.0/24 or 192.168.1.0/255.255.255.0

(3) Click **Save**.

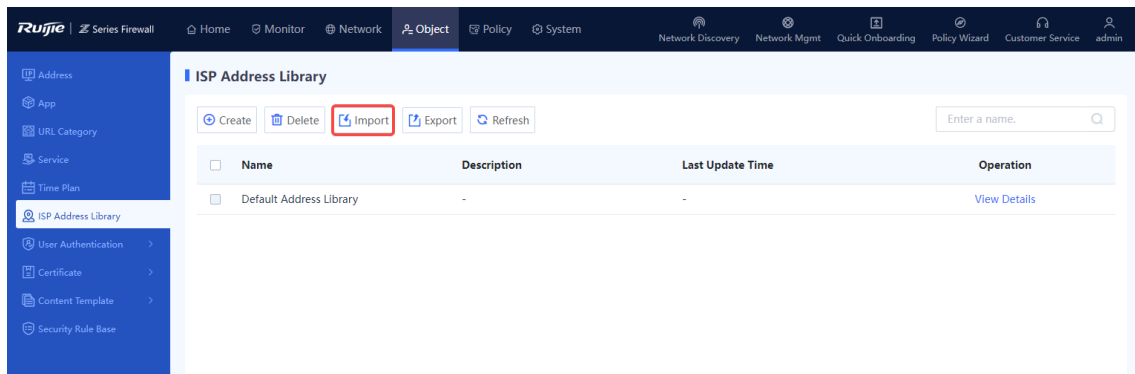
2. Importing an Address File to an ISP Address Library

Application Scenario

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

Procedure

(1) Choose **Object > ISP Address Library** and click **Import** in the operation area.



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

Import ⊗

[Download CSV Template](#)

* Name

* File

- (3) In the **Import** dialog box, enter the name of the ISP address library and click **Browse** to select the address library file. The file to be imported must be a CSV file.

- (4) Click **Confirm**.

Follow-up Procedure

- To delete the imported ISP address library, click **Delete**.

Caution

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

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

3. Upgrading ISP Address Library

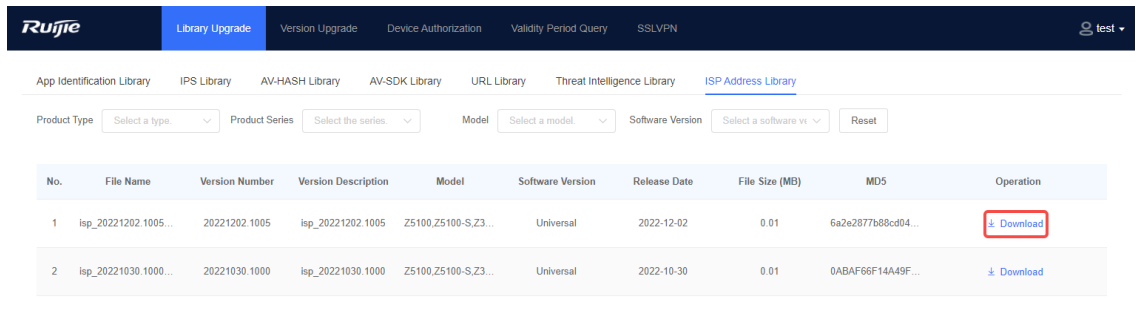
Application Scenario

The ISP address library is continuously updated. By upgrading the ISP address library, the device can obtain and generate the latest address library routes.

Procedure

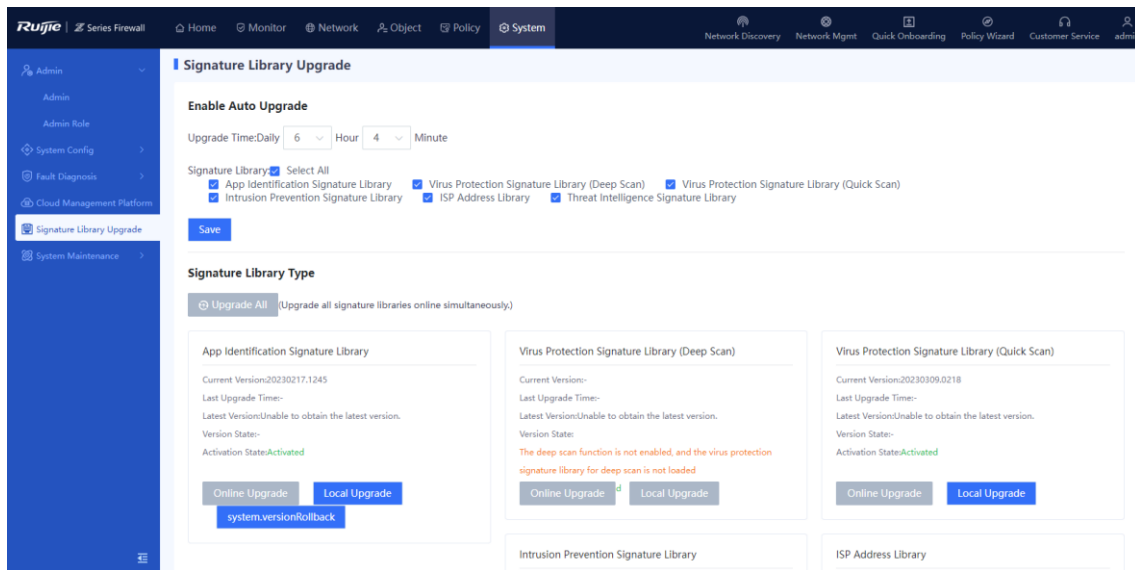
- (1) Log in to the Secure Cloud Platform and download the upgrade file of ISP address library.

Log in to <https://secloud1.ruijie.com.cn>, choose **Signature Library Upgrade > ISP Address Library**, and select a suitable version to download.



(2) Open the Signature Library Upgrade page.

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

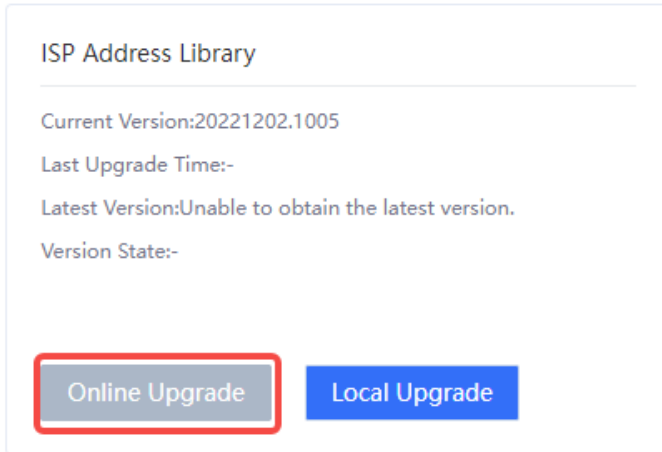


(3) Find out **ISP Address Library**, and select **Online Upgrade** or **Local Upgrade** according to actual situation.

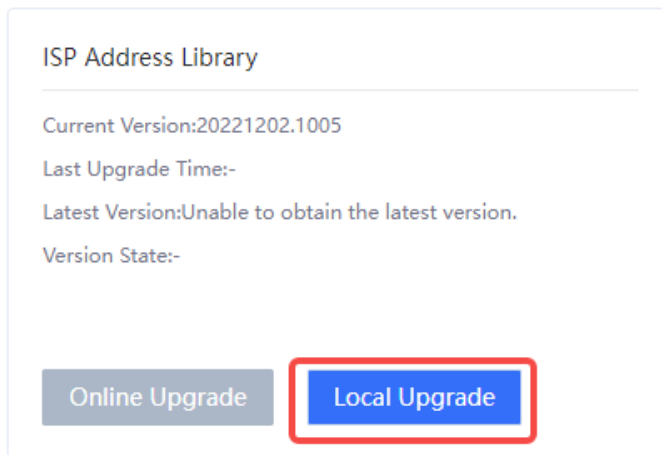
- o Online Upgrade: When the current version information about the firewall exists on the cloud platform and a new version is available, online upgrade of the device system can be performed on the firewall.

⚠ Caution

The firewall must be connected to the Internet.



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



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

Local Upgrade ⊗

① You can visit Ruijie Secure Cloud Platform at <https://SeCloud1.ruijie.com.cn>. On the platform, access the Signature Library Upgrade page and download the latest upgrade file. Then, perform the upgrade locally. Do not close or refresh this page during the upgrade process. Otherwise, the upgrade may fail. Note: The file name cannot contain any Chinese or full-width character. Before the upgrade, verify that the target version matches the device model.

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

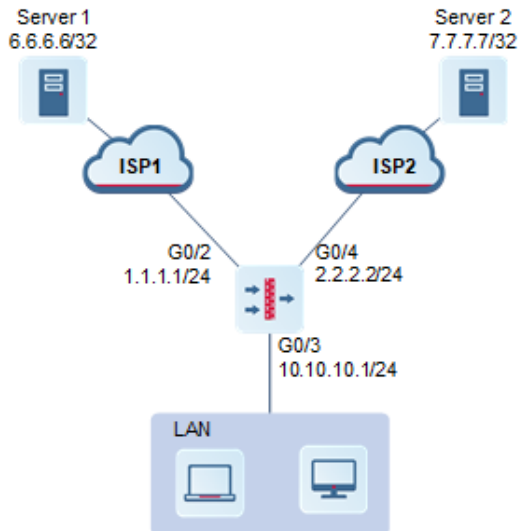
Import

8.20.3 Configuring ISP Routing

Network Requirements

The firewall is deployed at the network egress as a security gateway. The enterprise leases a line from each of ISP 1 and ISP 2. The enterprise requires that packets accessing Server 1 be forwarded through ISP 1 link and packets accessing Server 2 be forwarded through ISP 2.

Network Topology



Configuration Points

- (1) Complete basic network access settings.
- (2) Configure ISP address library.
- (3) Configure ISP routing (associating address library with interface).
- (4) Configure the security policy.

Procedure

- (1) Complete basic network access settings.

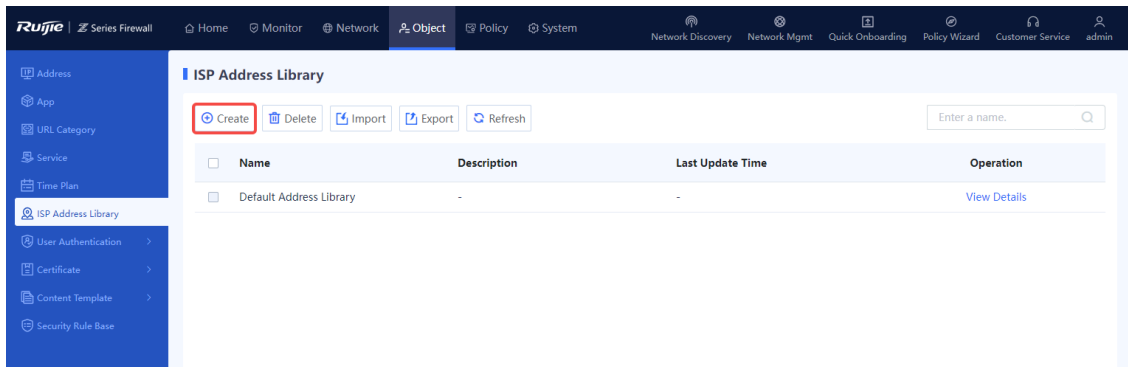
Configure the interface IP address, security zones, and gateway. For details, see [0](#)

[Routing](#) Mode.

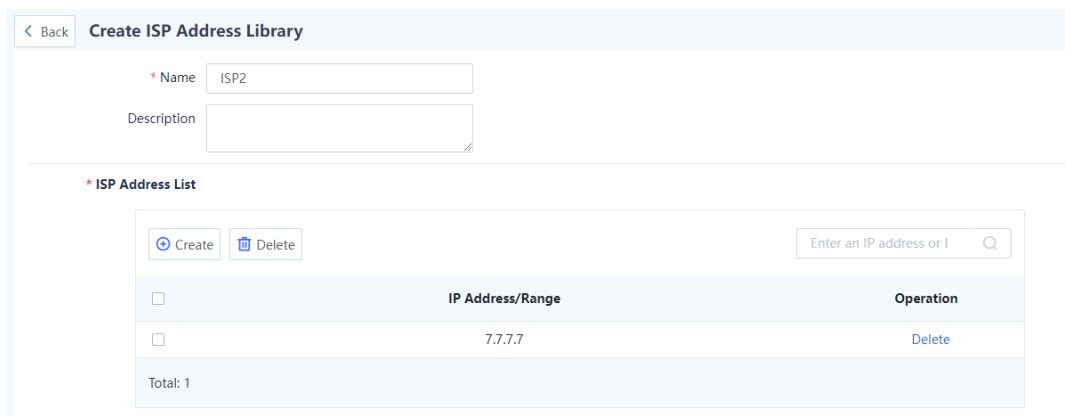
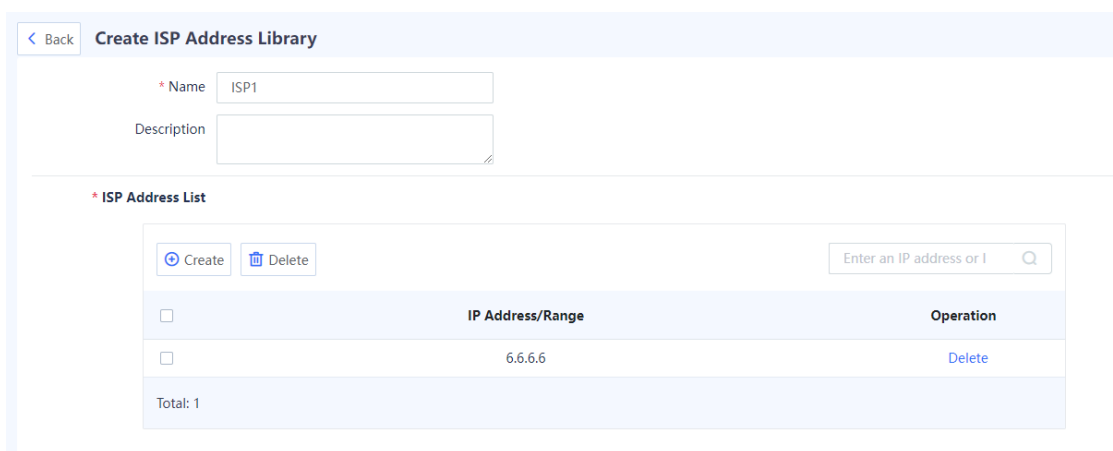
<input type="checkbox"/>	Ge0/2	-		Routing	untrust	IPv4: Static IP	1.1.1.1/24	-	1500	<input checked="" type="checkbox"/> Edit
<input type="checkbox"/>	Ge0/3	-		Routing	trust	IPv4: Static IP	10.10.10.1/24	-	1500	<input checked="" type="checkbox"/> Edit
<input type="checkbox"/>	Ge0/4	-		Routing	untrust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

- (2) Configure ISP address library.

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



- b Create address libraries of ISP 1 and ISP 2. Enter Server 1's IP address 6.6.6.6 for ISP1 and Server 2's IP address 7.7.7.7 for ISP 2.



- (3) Configure ISP routing (associating address library with interface).

Choose **Network > Physical Interface**, find out the row where G0/2 is located, and click **Edit**. Set the ISP address library to **ISP1**.

Advanced

ISP Address Library ISP1 ▼

ⓘ MTU

MAC Restore Default MAC

Link Detection ▼

- c Choose **Network > Physical Interface**, find out the row where G0/4 is located, and click **Edit**. Set the ISP address library to **ISP2**.

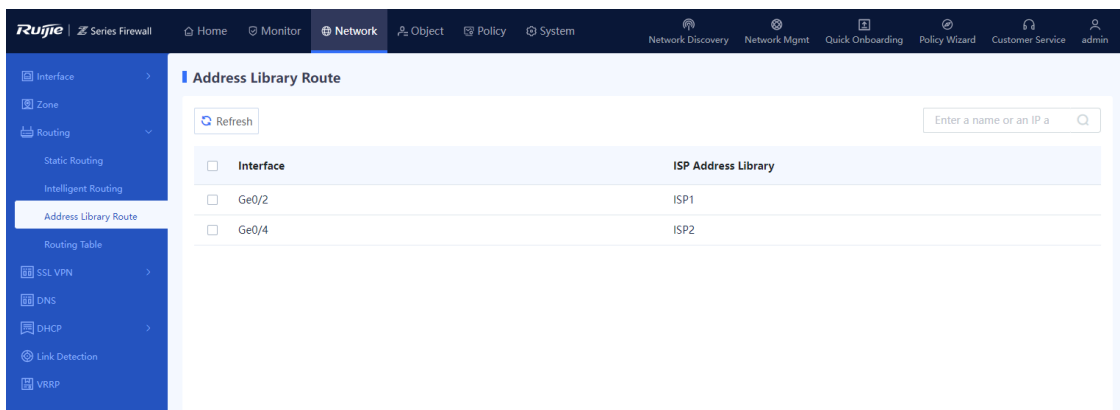
Advanced

ISP Address Library ISP2 ▼

ⓘ MTU

MAC Restore Default MAC

Link Detection ▼



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

< Back

Create Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group + Add Group

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

* Dest. Security Zone

* Dest. Address

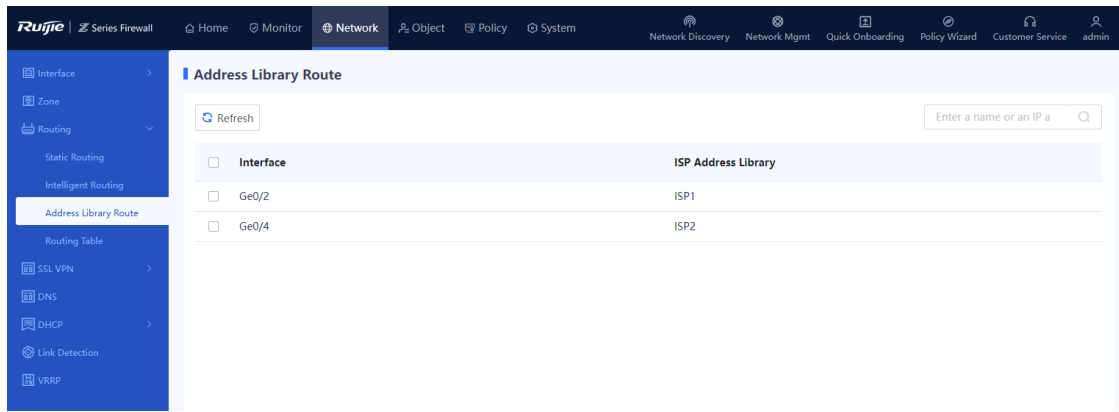
8.20.4 Viewing the Routing Table of Address Library

Application Scenario

The routes in address library are automatically generated after the ISP network to which the interface is connected is configured, and cannot be manually created. After an interface is associated with an ISP address set, routes are automatically generated in the address library, which are used for routing the packets. If the egress of a device is connected to multiple ISP networks, the packets destined for the specified ISP network can be forwarded through the specified outbound interface, avoiding inter-ISP access and improving traffic forwarding efficiency.

Procedure

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



8.21 Link Aggregation

Application Scenario

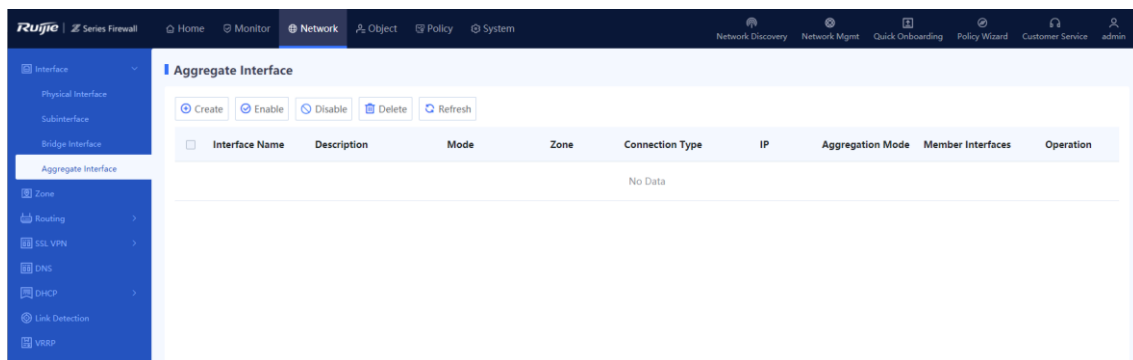
An aggregate interface binds multiple physical interfaces together to form a logical interface for link bandwidth expansion, which provides higher connection reliability.

An aggregate interface can increase link bandwidth and implement link redundancy backup.

- If the bandwidth of the link between two devices can reach 1,000 Mbps (assuming that the interface rate of both devices is 1,000 Mbps), when the service traffic carried on the link exceeds 1,000 Mbps, excess traffic is discarded. An aggregate interface can solve the problem of insufficient bandwidth in the following way: Use n network cables to connect two devices, and aggregate and bind these interfaces. In this way, these logically bound interfaces provide a maximum bandwidth of 1,000 Mbps \times n .
- When two devices are connected by a single network cable, if the link is disconnected, the services carried on the link will be interrupted. However, when multiple connected interfaces are aggregated and bound, if one member link is disconnected, the device automatically distributes the traffic of the faulty link to other member links. As long as one link is working, the services carried on these interfaces will not be interrupted.

Procedure

(1) Choose Network > Interface > Aggregate Interface.



(2) Click **Create**.

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

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

Basic Info

* Interface Name

Connection Status Enable Disable

Mode Routing Mode Transparent Mode Off-Path Mode

Zone [Add Security Zone](#)

Interface Type WAN Interface LAN Interface

Description

Member Interface

To-be-selected (0) Select All

- Ge0/3
- Ge0/4
- Ge0/5
- Ge0/6
- Ge0/7

Selected (0) [Clear](#)

Address

* Connection Type Static Address DHCP No IP Address

* IP/Mask

Next-Hop Address

Default Route

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 Defense

Permit HTTPS PING SSH

Advanced Settings

Aggregation Mode

ISP Address Library

[?](#) MTU

[?](#) MAC

Link Detection

Reverse Path Limited


[Save](#)

(3) Set parameters of aggregate interface.

Item	Description	Remarks
Interface Name	Name of the aggregate interface.	The interface name can contain only uppercase and lowercase letters and digits. [Example] Ag1
Connection Status	Enables or disables the interface.	[Example] Enable
Mode	Interface access mode. <ul style="list-style-type: none"> ● Routing Mode: forwards traffic based on IP addresses. ● Transparent Mode: forwards traffic based on MAC addresses. ● Off-Path Mode: only receives mirrored traffic, but does not forward traffic. 	[Example] Routing Mode
Bridge Interface	Bridge group to which the interface belongs in transparent mode.	This parameter is available when the transparent mode is used. [Example] br0
Zone	Security zone to which the interface belongs.	[Example] trust
Interface Type	Logical attribute of the interface.	[Example] LAN Interface
Description	Interface description, showing the purpose of the interface.	Characters such as `~!#%^&*+ \{};:"'<>?` are not allowed. [Example] Expand egress bandwidth.
Member Interface	Physical interface that is added to the aggregate interface.	Up to 8 member interfaces can be included. [Example] Ge0/1

Item	Description	Remarks
Connection Type	<p>IP address obtaining method of the interface. Valid values: Static Address and DHCP.</p> <p>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.</p>	<p>This parameter is available when the Routing Mode is used.</p> <p>[Example] Static Address</p>
IP/Mask	IPv4 address and mask of the interface.	<p>This parameter is available when Connection Type is set to Static Address.</p> <p>[Example] 192.168.1.1/24</p>
Next-Hop Address	<p>Next-hop address of the forwarded data. Generally, it is the address of the next routing device.</p>	<p>This parameter is available when Connection Type is set to Static Address.</p> <p>[Example] 192.168.1.2/24</p>
Default Route	Whether to generate the default route.	<p>[Example] Enabled</p>
Line Bandwidth	Limited interface bandwidth, including upload bandwidth and download bandwidth.	<p>Enter the bandwidth value and select a unit.</p> <p>The unit can be kbps or mbps.</p> <p>When kbps is selected as the unit, the value ranges from 1 to 100,000,000.</p> <p>When mbps is selected as the unit, the value ranges from 1 to 100,000.</p> <p>[Example] 100 kbps</p>


Item	Description	Remarks
Access Management	Whether the interface supports HTTPS, ping, and SSH.	The configuration takes effect when the interface mode is routing mode and local defense is enabled on the device. [Example] Select HTTPS .
Advanced Settings		
Aggregation Mode	For the manually configured aggregate interface, the aggregation mode is displayed as Static Aggregation .	Only the Static Aggregation is supported currently.
ISP Address Library	ISP network connected to the interface. The interface generates ISP routes based on the associated ISP address set, and the traffic with the destination addresses in different ISP networks is forwarded through the corresponding outbound interfaces.	This configuration takes effect only when the interface is configured as a WAN interface. [Example] CERNET
MTU	Maximum number of bytes in the packets sent on the interface. The default MTU value is 1500, namely, forwarding data at the highest speed. If the upper-level device limits the packet size, causing a network interruption or delay, you can reduce the MTU to 1492, 1400, or a smaller value.	An integer ranging from 64 to 1600. [Example] 1500
MAC	MAC address of the interface.	[Example] 30:0d:9e:41:d9:0b
Link Detection	Link detection policy associated with the local interface. This configuration can detect the network connectivity between the interface and the next hop in real time.	For details about link detection, see 8.22 Link Detection .

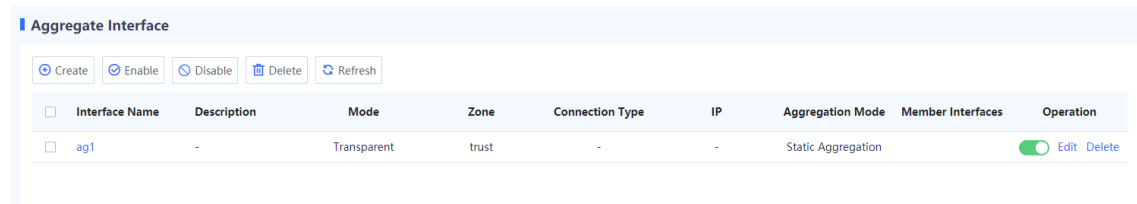
 Caution

- A management port cannot be added to an aggregate interface.
- The interface bound to other functions (such as security zone and routing entries) cannot be added to an aggregate interface.
- A maximum of 8 aggregate interfaces can be created.

(4) Click **Save**.

Follow-up Procedure

- On the aggregate interface management page (choose **Network > Interface > Aggregate Interface**), you can modify or delete the aggregate interfaces.
- To enable or disable an aggregate interface, you can click .
- To process multiple aggregate interfaces in a batch, select the interface entries and click **Enable**, **Disable**, or **Delete**.



8.22 Link Detection

Application Scenario


Link detection checks the connectivity of network links. When it is associated with static routing and PBR, automatic route switching can be implemented. If link detection is not associated with PBR or static routing, the static routes and default routes on the interface will not be invalid even if the detection result is abnormal.

Note

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

Procedure

(1) Choose **Network > Link Detection > Link Detection**.

(2) 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.

Link Detection
Detection Log

ⓘ When this function is enabled, the line state is periodically detected. If an exception is detected, the system immediately disables the line to ensure that application traffic can be transmitted over a normal line.
Note: When an exception is detected, a network interruption may occur. Please operate with caution.

Link Detection

Create
Delete
Refresh

Enter a name or an int... 🔍

<input type="checkbox"/>	Name	Interface	ICMP Probe	IP	Detection Result	Link Detection	Operation
No Data							

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

< Back
Add Link Detection

Basic Info

* Name

⊙ Minimum Survivability Nodes

Detection Node

⊙ Detection Node

Create
Delete

<input type="checkbox"/>	Node Name	Protocol	To-Be-Detected Dest. IP	Domain Name	Port Number	Outbound Interface	Next-Hop Address	Detection
No Data								

10 / Page Total:0
Go to < 1 >

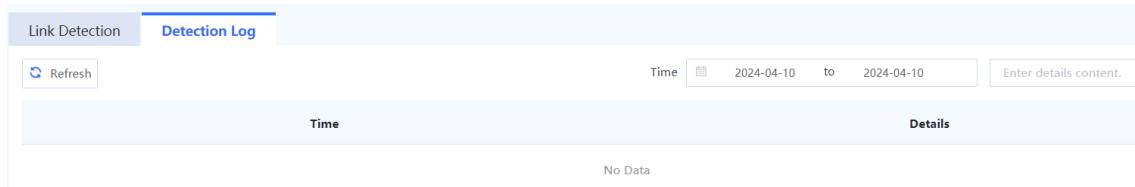
Save

Item	Description	Remarks
Basic Info		
Name	Name of 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

Item	Description	Remarks
Protocol	Detection protocol type.	[Example] ICMP
Enabled State	Whether to enable node detection.	[Example] Enable
To-Be-Detected Dest. IP	IP address of the detection node when the protocol type is ICMP.	[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.	[Example] 53
Outbound Interface	Outbound interface for node detection.	[Example] Ge0/2
Next-Hop Address	Next-hop IP address of the route destined for the detection node.	[Example] 192.168.2.1
Detection Frequency	Frequency of node detection or node recovery detection.	[Example] 6000 ms
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 goes 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

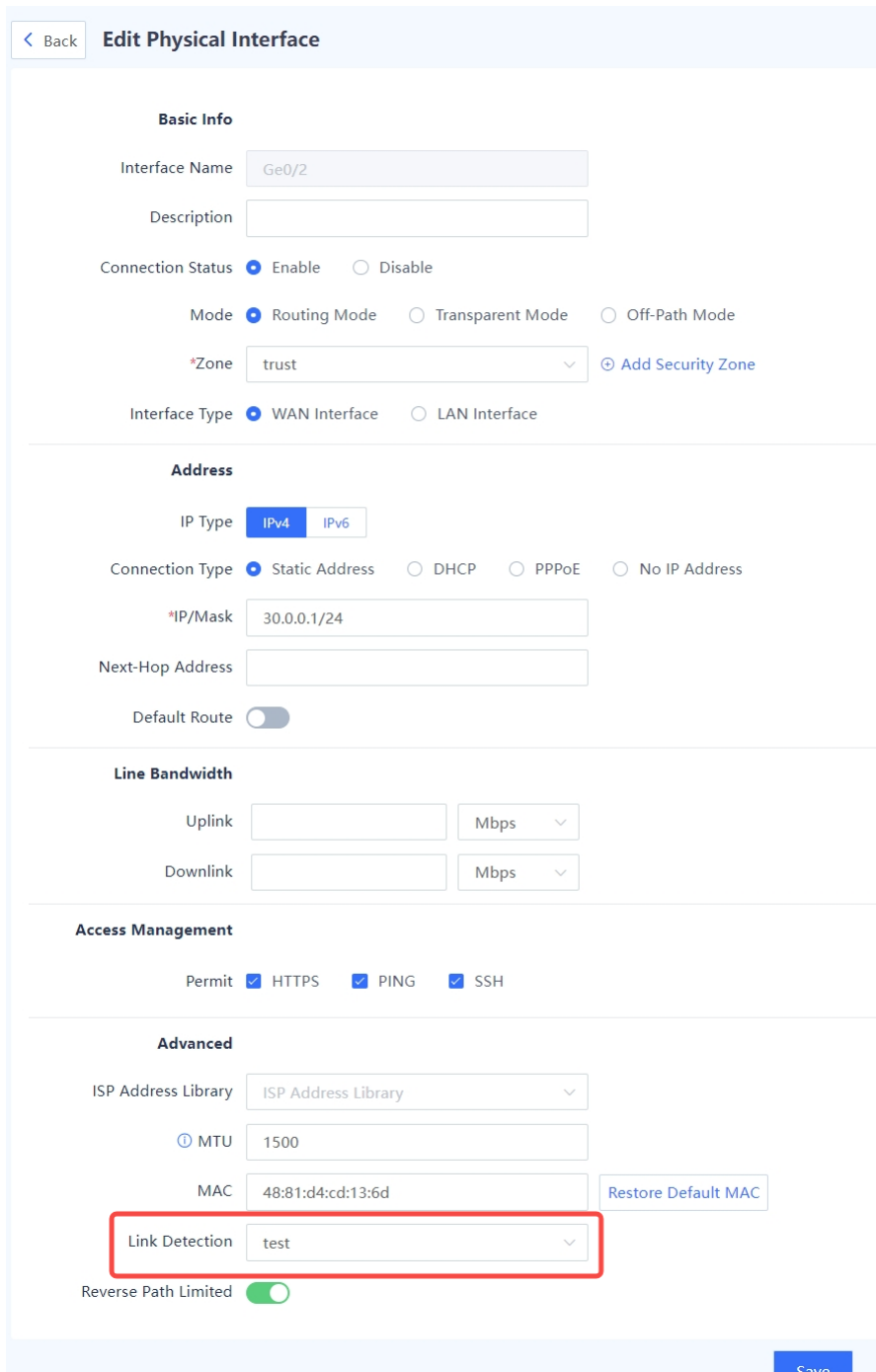
(4) Click **Save**.

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



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.



The screenshot shows the 'Edit Static Routing' configuration interface. At the top left, there is a '< Back' button. The title 'Edit Static Routing' is centered at the top. Below the title, the 'IP Type' is set to 'IPv4'. The configuration fields include:

- '* Dest. IP Range/Mask' with the value '60.0.0.0/24'.
- 'Next-Hop Address' (empty field).
- 'Interface' set to 'Ge0/2'.
- '* Priority' set to '5'.
- 'Link Detection' set to 'test' (this field is highlighted with a red border).
- 'Description' (empty text area).

8.23 Outbound Interface Load Balancing

8.23.1 Overview

When there are multiple equal-cost egresses or links for intranet users to access an extranet, you can enable Multi-Link Load Balance (MLLB) on the firewall to ensure service continuity and network quality.

MLLB does not directly forward data flows but serves as a common method for a routing module to select a proper outbound interface for data forwarding when multiple equal-cost routes to the destination network exist. Therefore, MLLB needs to be used with a routing module, including but not limited to:

- Static routing: When there are multiple static routes with the same priority and administrative distance to a destination network, multiple equal-cost static routes exist.
- ISP address library-based routing: When multiple interfaces reference an address library, multiple equal-cost routes exist.
- DNS transparent proxy: When the link to the Domain Name System (DNS) server is congested, multiple standby links exist.
- Intelligent routing: When traffic matches a policy, multiple egress links exist.

Application scenarios of MLLB

Scenario	Description
Static routing	Most scenarios with multiple egresses where MLLB is required among different types of links, such as private network, ISP, and VPN lines
ISP address library-based routing	Routing scenarios where multiple links support ISP address library-based routing and MLLB is required among the links
DNS transparent proxy	Routing scenarios where multiple links support ISP address library-based routing and when one of the links degrades, another link needs to be enabled for MLLB

Intelligent routing	Most scenarios with multiple egresses where traffic needs to be more accurately selected than specific routes
---------------------	---

MLLB modes

Balancing Mode	Description	Related Configurations
Based on the source IP address	Select a link based on the hash value of the source IP address. Services with the same source address are transmitted over the same link.	N/A
Based on source and destination IP addresses	Select a link based on the hash value of the source and destination IP addresses. Services with the same source and destination IP addresses are transmitted over the same link.	N/A
Based on bandwidth	Select a link based on the bandwidth ratio or bandwidth usage.	Configure the uplink and downlink bandwidths for an interface (a link).
Based on the link priority	Select a link with the highest priority.	Configure the priority for an interface (a link).
Based on the link weight	Select a link based on the link weight. Links with larger weights are prioritized in load balancing.	Configure the weight for an interface (a link).
Based on sessions	Select a link with the lowest session usage (the number of real-time sessions divided by the configured maximum number of sessions).	Configure the maximum number of sessions for an interface (a link).
Based on bandwidth and sessions	Select a link with the lowest session usage (the number of real-time sessions divided by the configured maximum number of sessions) and with a downlink bandwidth lower than the threshold.	Configure the downlink bandwidth threshold and maximum number of sessions for an interface (a link).

8.23.2 Configuring MLLB Based on Uplink Bandwidth for a Network with Specific Routes

1. Applicable Products and Versions

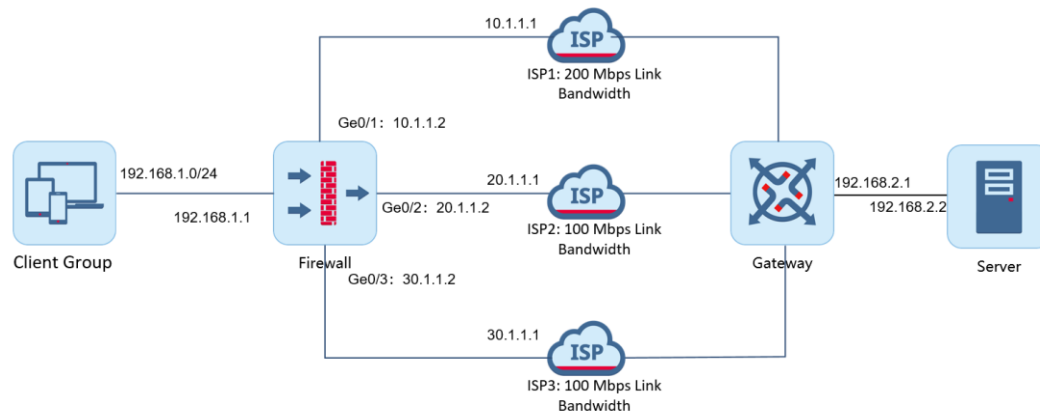
Table 8-17 Products and Versions

Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R8 or later

2. Service Demands

As shown in [Figure 8-15](#), a client group needs to access the server through the firewall. There are multiple links from the firewall to the server and their available bandwidths are different. To ensure service continuity and network quality, MLLB can be enabled for static routing to perform load balancing based on the bandwidth ratio.

Figure 8-15 Topology of a Network with Specific Routes



i Note

The server in the figure is for illustrative purposes only. It can be any other device such as a host.

3. Restrictions and Guidelines

- On the RG-WALL 1600 series firewall, one IP address cannot be assigned to multiple interfaces.

4. Prerequisites

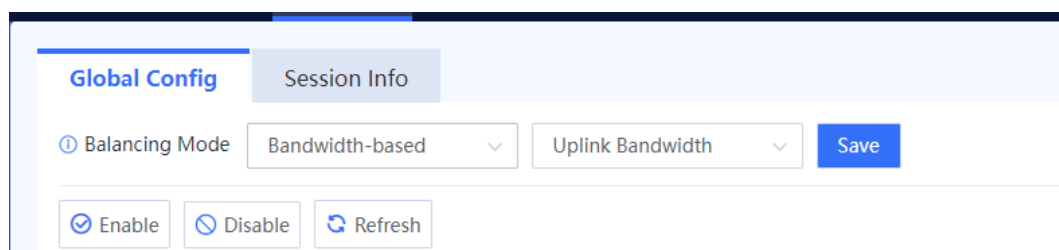
You have completed basic network configurations for the clients and the server, including interface IP addresses and static routes. Pay attention to the following points during configuration:

- After the firewall is connected to different ISP networks, ensure that direct next hops are correctly configured.
- After the firewall is connected to different ISP networks, configure static routes (outbound interfaces and next hops) to the server.

5. Procedure

(1) Configuring the MLLB Mode

- Choose **Network > Routing > Egress Load Balancing > Global Config**.
- Select **Bandwidth-based** and **Uplink Bandwidth** from the **Balancing Mode** drop-down lists.



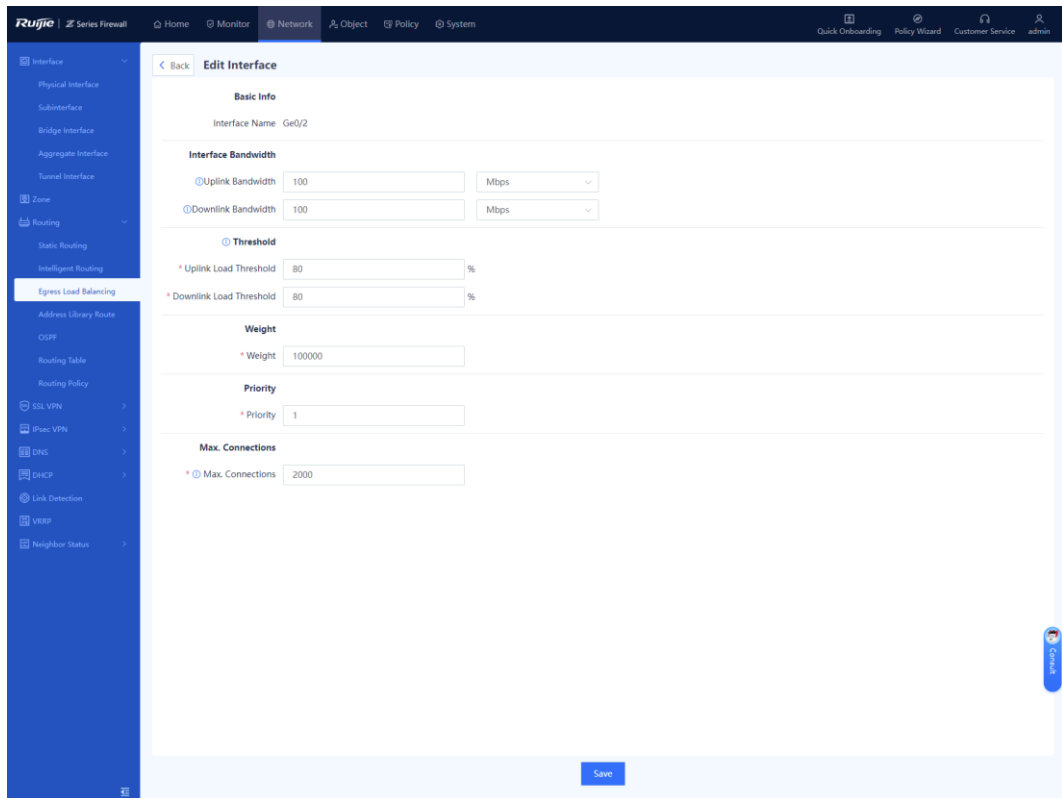
- c Click **Save**.
- (2) Configuring Interface Bandwidth for MLLB
- a Choose **Network > Routing > Egress Load Balancing > Global Config**.
 - b Click **Edit** in the **Operation** column of an interface to configure outbound interface parameters.
Configure the parameters for Ge0/1 and click **Save**.

The screenshot displays the 'Edit Interface' configuration page for Ge0/1 in the Ruijie Series Firewall web interface. The page is organized into several sections:

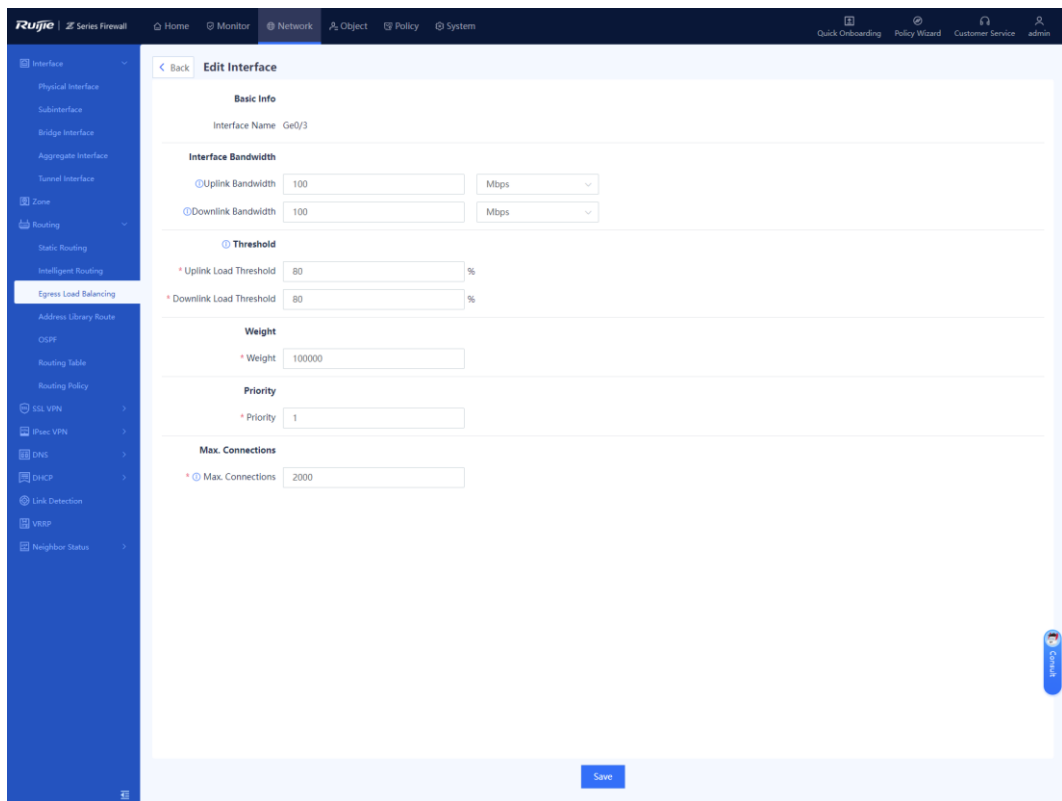
- Basic Info:** Interface Name: Ge0/1
- Interface Bandwidth:**
 - Uplink Bandwidth: 200 Mbps
 - Downlink Bandwidth: 200 Mbps
- Threshold:**
 - Uplink Load Threshold: 80%
 - Downlink Load Threshold: 80%
- Weight:**
 - Weight: 200000
- Priority:**
 - Priority: 1
- Max. Connections:**
 - Max. Connections: 2000

A 'Save' button is located at the bottom right of the configuration area.

Configure the parameters for Ge0/2 and click **Save**.



Configure the parameters for Ge0/3 and click **Save**.



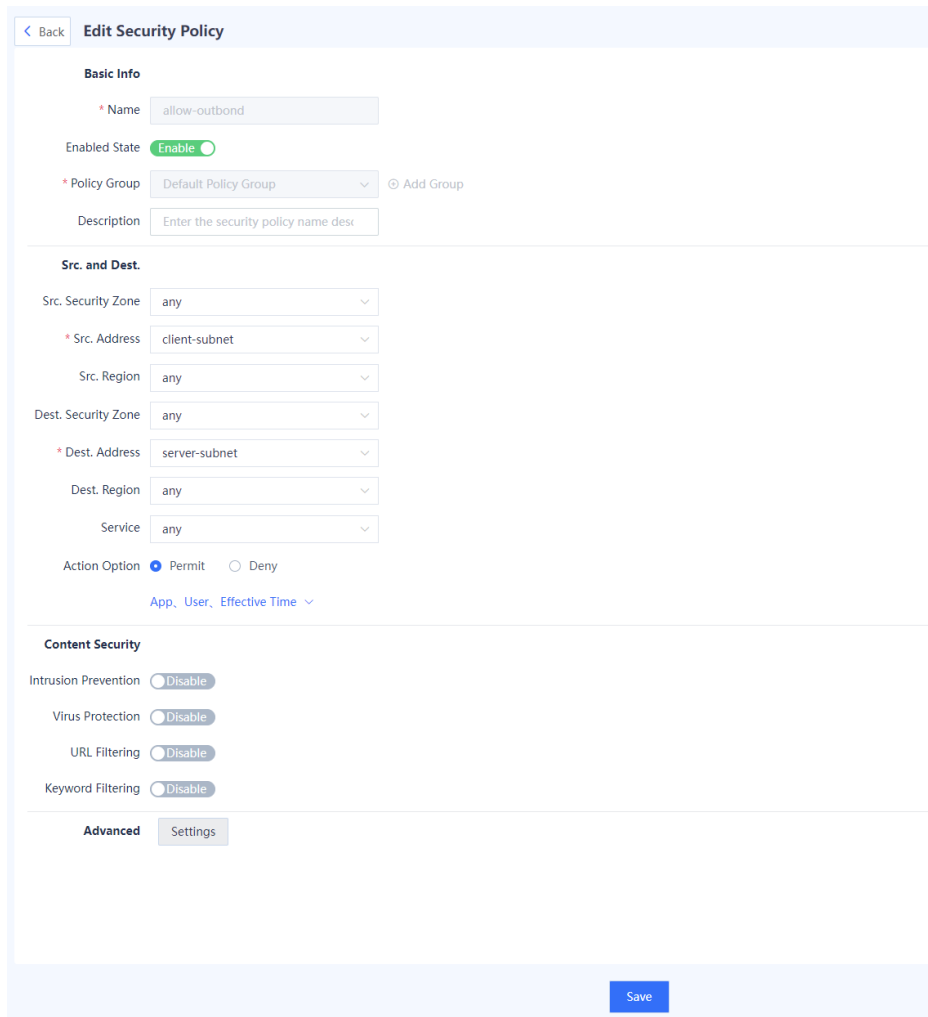
(3) Configuring a Security Policy and Static Routing

- a Configure a security policy.

Choose **Object > Address > IPv4 Address** and click **Create** to create address object 192.168.1.0/24 for the clients and address object 192.168.2.0/24 for the server.



Choose **Policy > Security Policy > Security Policy** and click **Create** to create a security policy.



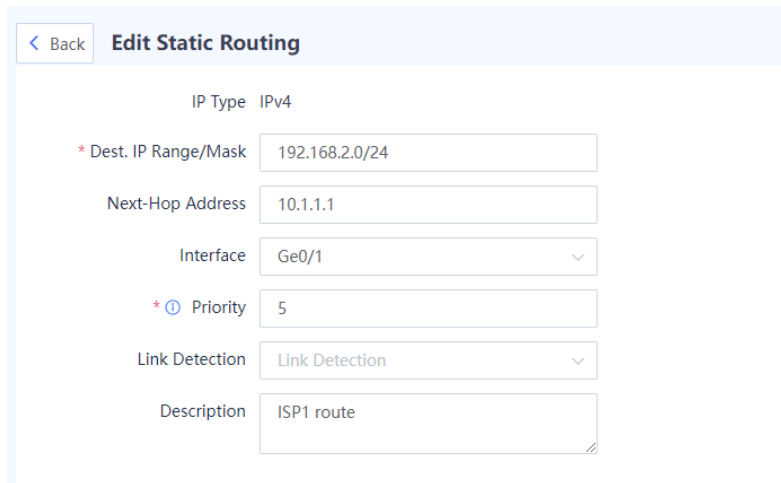
Click **Save**.

- b Configure static routing.

Choose **Network > Routing > Static Routing > IPv4**.

Click **Create** to create a static route to the server.

Create a static route to the server through the ISP1 link and click **Save**.




[< Back](#) **Edit Static Routing**

IP Type IPv4

* Dest. IP Range/Mask

Next-Hop Address

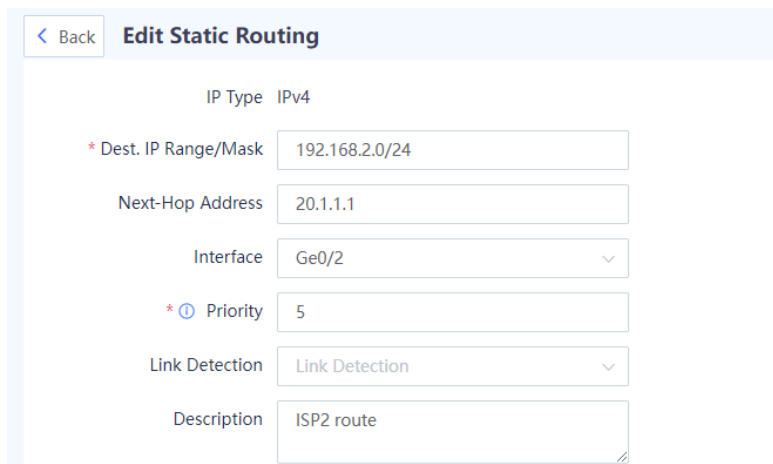
Interface

*  Priority

Link Detection

Description

Create a static route to the server through the ISP2 link and click **Save**.




[< Back](#) **Edit Static Routing**

IP Type IPv4

* Dest. IP Range/Mask

Next-Hop Address

Interface

*  Priority

Link Detection

Description

Create a static route to the server through the ISP3 link and click **Save**.

Edit Static Routing

IP Type IPv4

* Dest. IP Range/Mask 192.168.2.0/24

Next-Hop Address 30.1.1.1

Interface Ge0/3

* Priority 5

Link Detection Link Detection

Description ISP3 route

6. Verification

- Checking the MLLB Configuration

Choose **Network > Routing > Egress Load Balancing > Global Config** to check the MLLB mode and interface bandwidth configurations.

Global Config Session Info

Balancing Mode: Bandwidth-based Uplink Bandwidth: Save

Enable Disable Refresh

Interface Name	Uplink Bandwidth	Downlink Bandwidth	Uplink Load Threshold	Downlink Load Threshold	Operation
Ge0/2	100Mbps	100Mbps	80	80	Enable Edit
Ge0/3	100Mbps	100Mbps	80	80	Enable Edit
Ge0/1	200Mbps	200Mbps	80	80	Enable Edit

- Checking Static Routes

Choose **Network > Routing > Routing Table > IPv4** to check the equal-cost routes.

Static route	192.168.2.0/24	10.1.1.1	5	Ge0/1
Static route	192.168.2.0/24	20.1.1.1	5	Ge0/2
Static route	192.168.2.0/24	30.1.1.1	5	Ge0/3

- Checking Traffic Steering Effects

Concurrent traffic from multiple clients on the 192.168.1.0/24 network segment is sent to the server through the firewall. On the firewall web UI, choose **Monitor > Traffic Monitoring > Real-Time Traffic** and view the traffic trend graph. Select **Ge0/1**, **Ge0/2**, and **Ge0/3** in the **Interface** drop-down list to display the traffic ratio, which is 2:1:1.



8.23.3 Configuring MLLB Based on Uplink Bandwidth for DNS Transparent Proxy

1. Applicable Products and Versions

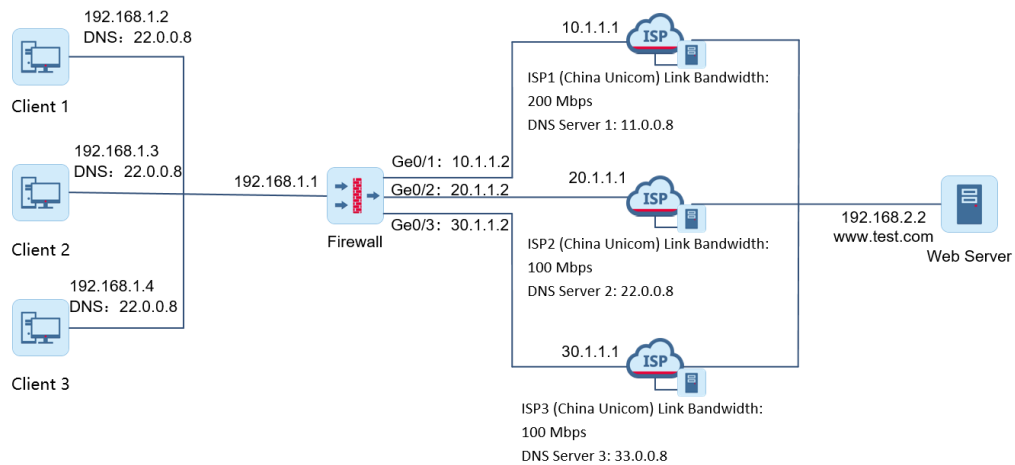
Table 8-18 Products and Versions

Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R8 or later

2. Service Demands

As shown in [Figure 8-16](#), in a multi-ISP routing scenario, if the DNS servers configured for intranet clients are limited in number and DNS requests initiated by the clients are always transmitted through the ISP2 link, the ISP2 link will be prone to congestion. This affects the online experience of users. In addition, other ISP links are idle, causing resource waste. In this case, you can enable DNS transparent proxy on the firewall to allow ISP1 and ISP3 links to forward the requests when the ISP2 link degrades, thereby optimally utilizing network resources.

Figure 8-16 Topology of DNS Transparent Proxy



Note

- The device does not provide predefined ISP address libraries. Choose **Object > ISP Address Library** to create or import an address library. The address libraries used in this example are for illustrative purposes only.
- The web server in the figure is for illustrative purposes only. It can be any other host or server that needs to be accessed through DNS resolution.

3. Restrictions and Guidelines

- Typically, DNS transparent proxy is used together with ISP-based routing.

4. Prerequisites

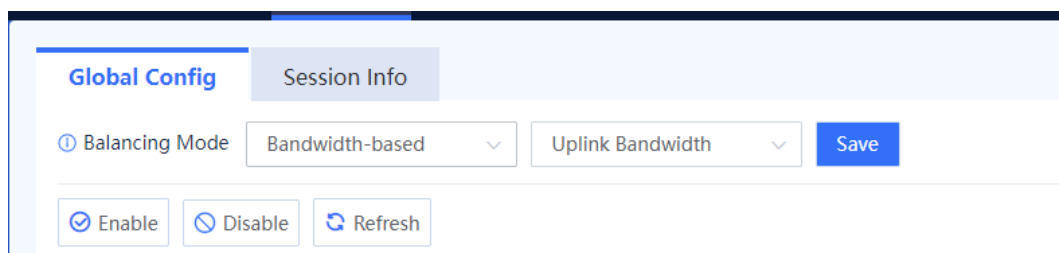
You have completed basic network configurations for the clients and the web server, including interface IP addresses, default routes, and DNS servers. Pay attention to the following points during configuration:

- Ensure that the destination of the traffic sent by the clients is the domain name of the web server.
- Ensure that the DNS server address configured for a client is fixed, such as 22.0.0.8.

5. Procedure

(1) Configuring the MLLB Mode

- Choose **Network > Routing > Egress Load Balancing > Global Config**.
- Select **Bandwidth-based** and **Uplink Bandwidth** from the **Balancing Mode** drop-down lists.



- Click **Save**.

(2) Configuring Interface Bandwidth for MLLB

- a Choose **Network > Routing > Egress Load Balancing > Global Config**.
- b Click **Edit** in the **Operation** column of an interface to configure outbound interface parameters.

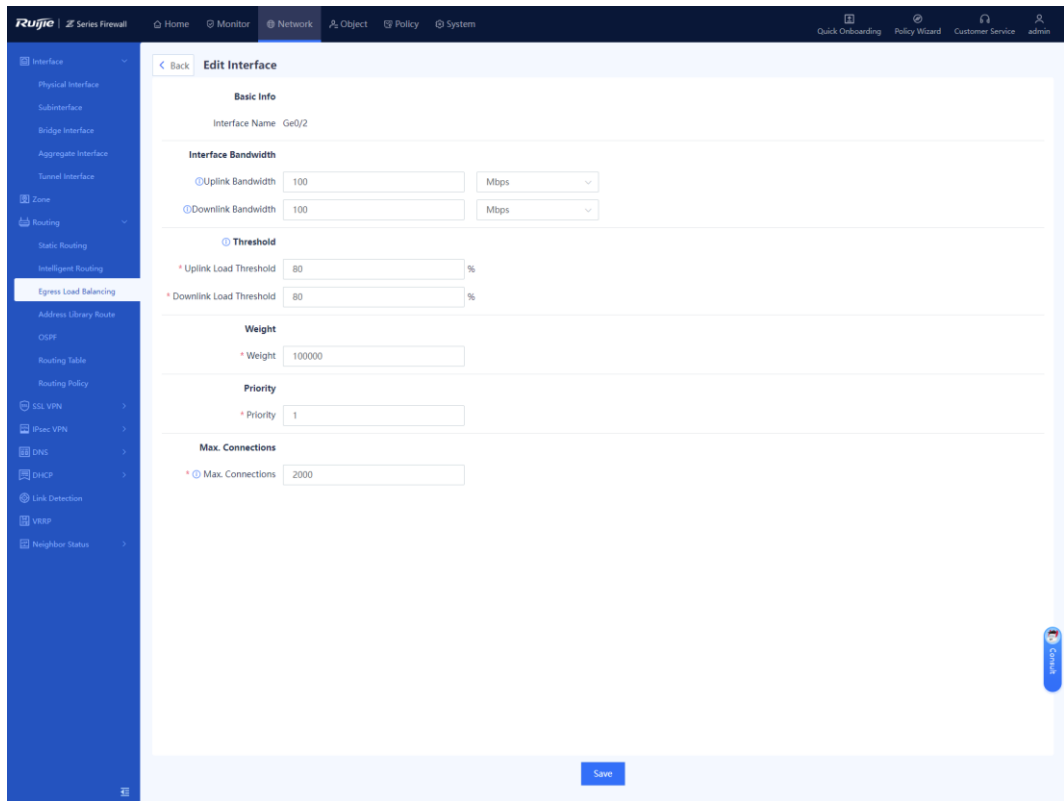
Configure the parameters for Ge0/1 and click **Save**.

The screenshot shows the 'Edit Interface' configuration page for interface Ge0/1. The left sidebar contains a navigation menu with categories like Interface, Zone, Routing, and Address Library Route. The 'Egress Load Balancing' option is selected. The main content area is titled 'Edit Interface' and shows the following configuration fields:

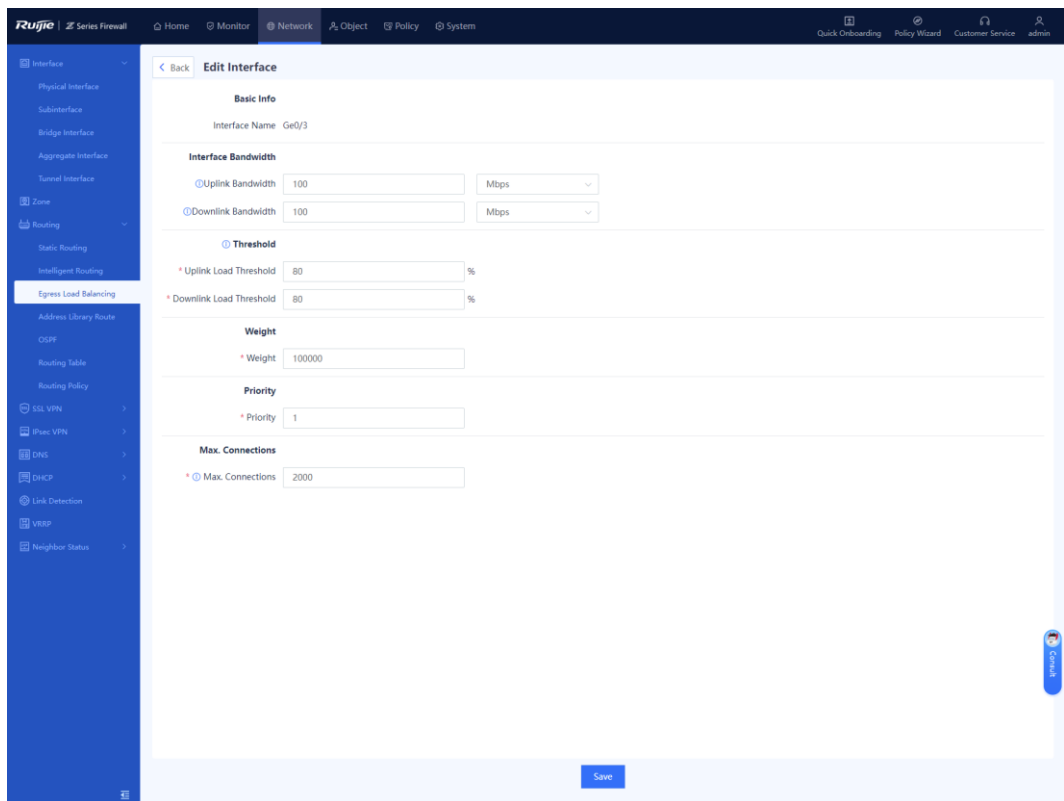
- Basic Info:** Interface Name: Ge0/1
- Interface Bandwidth:**
 - Uplink Bandwidth: 200 Mbps
 - Downlink Bandwidth: 200 Mbps
- Threshold:**
 - Uplink Load Threshold: 80 %
 - Downlink Load Threshold: 80 %
- Weight:**
 - Weight: 200000
- Priority:**
 - Priority: 1
- Max. Connections:**
 - Max. Connections: 2000

A 'Save' button is located at the bottom right of the configuration area.

Configure the parameters for Ge0/2 and click **Save**.



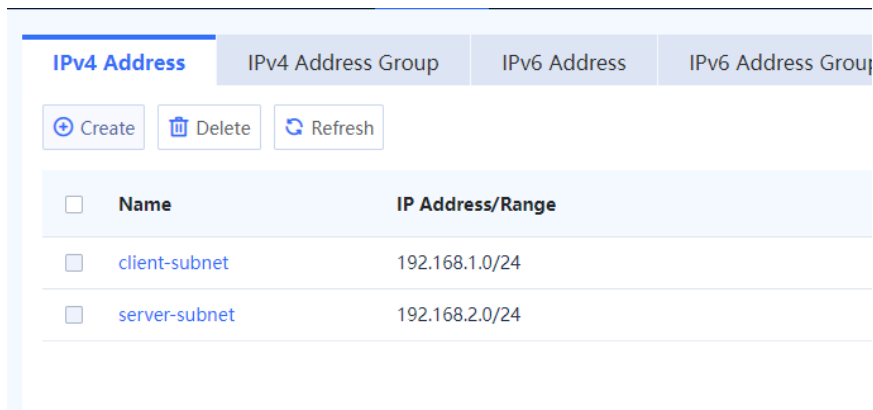
Configure the parameters for Ge0/3 and click **Save**.



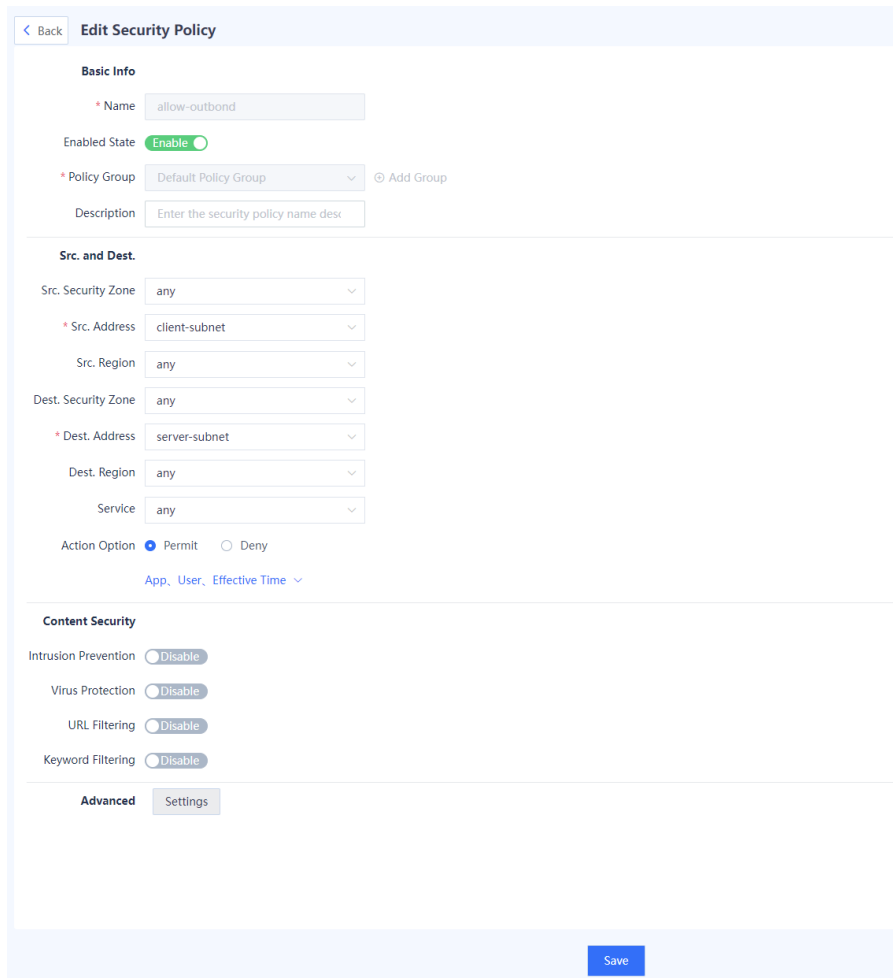
(3) Configuring a Security Policy and ISP Routing

- a Configure a security policy.

Choose **Object > Address > IPv4 Address** and click **Create** to create address object 192.168.1.0/24 for the clients and address object 192.168.2.0/24 for the server.



Choose **Policy > Security Policy > Security Policy** and click **Create** to create a security policy.



Click **Save**.

- b Configure ISP routing.

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

Click **Edit** in the **Operation** column of Ge0/1 and associate the interface with the address library of China Unicom.

Advanced

ISP Address Library

① MTU

MAC [Restore Default MAC](#)

Link Detection

Reverse Path Limited

[Save](#)

Click **Edit** in the **Operation** column of Ge0/2 and associate the interface with the address library of China Telecom.

Advanced

ISP Address Library

① MTU

MAC [Restore Default MAC](#)

Link Detection

Reverse Path Limited

[Save](#)

Click **Edit** in the **Operation** column of Ge0/3 and associate the interface with the address library of China Telecom.

Advanced

ISP Address Library

① MTU

MAC [Restore Default MAC](#)

Link Detection

Reverse Path Limited

[Save](#)

(4) Configuring DNS Transparent Proxy

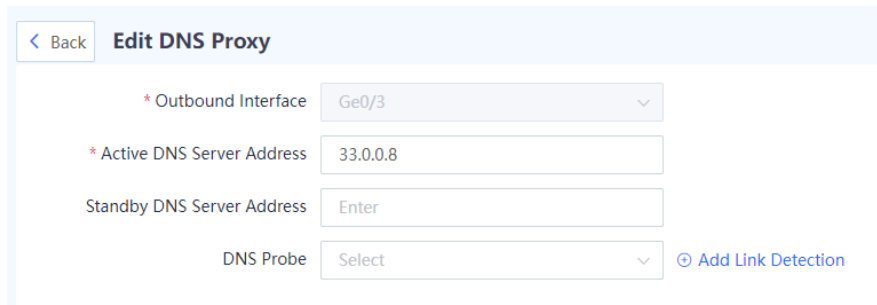
- a Choose **Network > DNS > DNS > DNS Transparent Proxy** to enable DNS transparent proxy.
- b Configure a proxy policy and click **Save**.

c Configure a proxy interface.

Set the primary DNS server address of Ge0/1 to 11.0.0.8 and click **Save**.

Set the primary DNS server address of Ge0/2 to 22.0.0.8 and click **Save**.

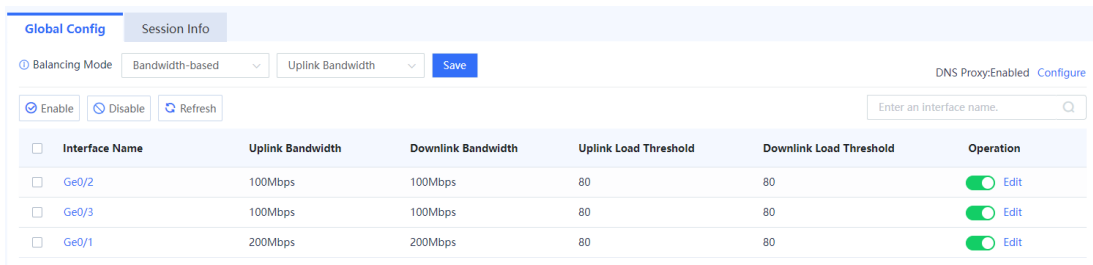
Set the primary DNS server address of Ge0/3 to 33.0.0.8 and click **Save**.



6. Verification

- Checking the MLLB Configuration

Choose **Network > Routing > Egress Load Balancing** to check the balancing mode and interface bandwidth.



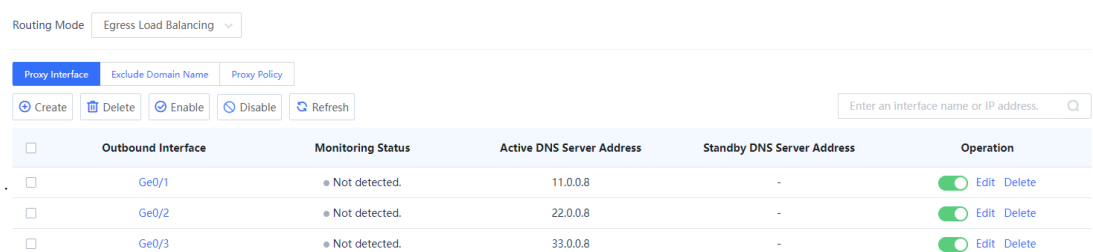
- Checking ISP Routes

Choose **Network > Routing > Address Library Route** to check ISP equal-cost routes.

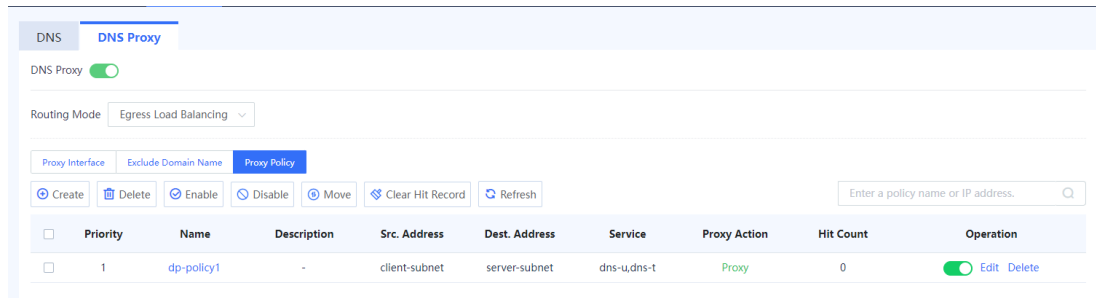


- Checking the DNS Transparent Proxy Configuration

Choose **Network > DNS > DNS > DNS Transparent Proxy** and click the **Proxy Interface** tab to check the outbound interface configuration.

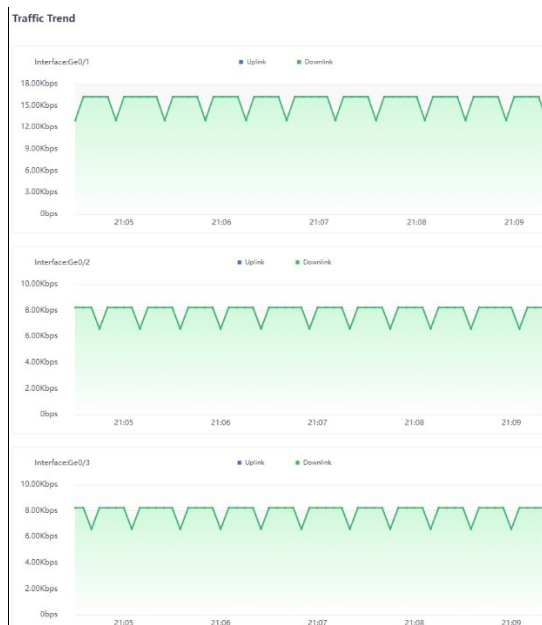


Choose **Network > DNS > DNS > DNS Transparent Proxy** and click the **Proxy Policy** tab to check the policy configuration.



- **Checking Traffic Effects**

Concurrent traffic from multiple clients on the network segment 192.168.1.0/24 is sent to the server through the firewall. Choose **Monitor > Traffic Monitoring > Real-Time Traffic** on the web page of the firewall to display the traffic trend graph and click on Ge0/1, Ge0/2, and Ge0/3 to display the traffic ratio, which is 2:1:1.



8.23.4 Configuring MLLB Based on Link Priority for Intelligent Routing

1. Applicable Products and Versions

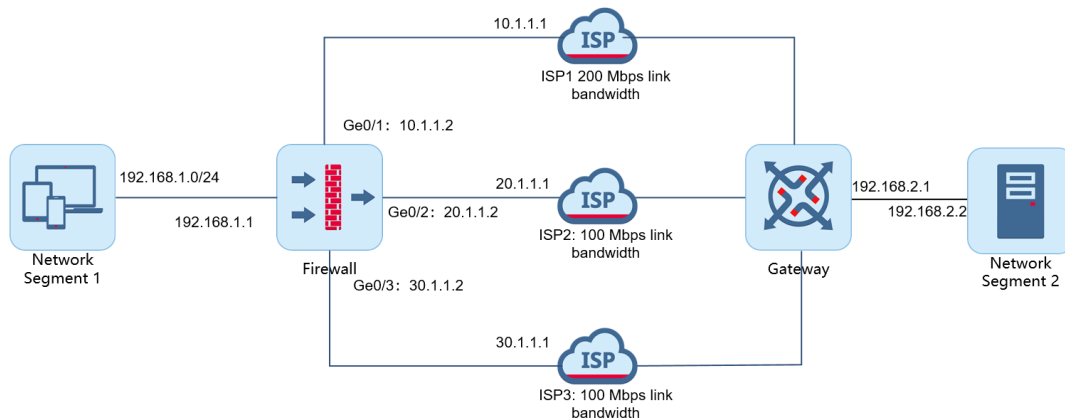
Table 8-19 Products and Versions

Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R8 or later

2. Service Demands

In the multi-egress routing scenario shown in [Figure 8-17](#), traffic is further classified based on the existing routing table by source address, inbound interface, application type, and user type. Packets with different parameters are directed to different outbound interfaces. This process is known as intelligent routing. When the intelligent routing policy requires multiple outbound interfaces, traffic can be forwarded hierarchically based on bandwidth, source or destination IP addresses, and link priority, ensuring a good user experience.

Figure 8-17 Topology of Intelligent Routing



3. Restrictions and Guidelines

- When the static outbound interface address is used in intelligent routing, the next-hop address must be configured.

4. Prerequisites

You have completed basic network configurations for network segments 1 and 2, including interface addresses and default routes.

5. Procedure

(1) Configure a security policy.

- Choose **Object > Address > IPv4 Address** and click **Create** to create two address objects: network segment 1 with 192.168.1.0/24 and network segment 2 with 192.168.2.0/24.



- b Choose **Policy > Security Policy > Security Policy** and click **Create** to create a security policy.

Edit Security Policy

Basic Info

* Name

Enabled State Enable

* Policy Group [Add Group](#)

Description

Src. and Dest.

Src. Security Zone

* Src. Address

Src. Region

Dest. Security Zone

* Dest. Address

Dest. Region

Service

Action Option Permit Deny

[App, User, Effective Time](#)

Content Security

Intrusion Prevention Disable

Virus Protection Disable

URL Filtering Disable

Keyword Filtering Disable

Advanced

- c Click **Save**.

(2) Configure intelligent routing.

- a Choose **Network > Routing > Intelligent Routing**.
- b Click **Create** to configure **Matching Conditions**, **Action Option**, and **Outbound Interface Type**.

[< Back](#) **Edit Intelligent Routing**

Basic Info

* Name

Enabled State Enable Disable

Adjacent Policy

Description

Matching Conditions

Inbound Interface

Src. Address

Dest. Address

Service

User

App

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

Action Settings

Action Option Forwarding No Intelligent Routing

Outbound Interface Type Single Interface Multiple Interfaces

* Intelligent Routing Mode

Outbound Interface List

- c Click **Create** in the **Outbound Interface List** menu, and add Ge0/1, Ge0/2, and Ge0/3 in sequence and configure their parameters.

Add Outbound Interface ⊗

Basic Info

* Interface Name

* Next-Hop Address

Threshold

Uplink Load Threshold %

Downlink Load Threshold %

Weight

Weight

Priority

Priority

Max. Connections

Max. Connections

Add Outbound Interface ⊗

Basic Info

* Interface Name

* Next-Hop Address

Threshold

Uplink Load Threshold %

Downlink Load Threshold %

Weight

Weight

Priority

Priority

Max. Connections

Max. Connections

Add Outbound Interface ⊗

Basic Info

* Interface Name

* Next-Hop Address

Threshold

Uplink Load Threshold %

Downlink Load Threshold %

Weight

Weight

Priority

Priority

Max. Connections

Max. Connections

6. Verification

- Checking Intelligent Routes

Choose **Network > Routing > Intelligent Routing** to check the intelligent routes. Click **Edit** in the **Operation** column to view details about the outbound interface list.

Intelligent Routing

1. Different matching conditions in a rule are in an AND relationship. That is, a packet matches this rule only when all the conditions are met.
 2. Different values configured for a matching condition are in an OR relationship. That is, this condition is met when any value is matched.

<input type="checkbox"/>	Priority	Name	Inbound Interface	Src. Address	Dest. Address	Service	App	User	Effective Time	Action	Intelligent Routing Mode	Outbound Interface
<input type="checkbox"/>	1	pbr_001	any	client-subnet	server-subnet	any	Interne...	any	any	Forwarding	Based on Link Priority	Ge0/1,Ge0/2,Ge0/3

Action Settings

Action Option Forwarding No Intelligent Routing

Outbound Interface Type Single Interface Multiple Interfaces

* Intelligent Routing Mode Based on Link Priority

Outbound Interface List

[Create](#) [Delete](#) [Refresh](#)

<input type="checkbox"/>	Interface	Priority	Next-Hop Address	Uplink Load Threshold	Downlink Load Threshold	Operation
<input type="checkbox"/>	Ge0/1	10	10.1.1.1	80%	80%	Edit Delete
<input type="checkbox"/>	Ge0/2	5	20.1.1.1	80%	80%	Edit Delete
<input type="checkbox"/>	Ge0/3	1	30.1.1.1	80%	80%	Edit Delete
Total: 3						

Link Detection [Add Link Detection](#)

[Save](#)

● Checking Traffic Effects

Concurrent traffic from multiple clients on the 192.168.1.0/24 network segment is sent to the server through the firewall. Choose **Monitor > Traffic Monitoring > Real-Time Traffic** on the web page of the firewall to display the traffic trend graph. Click on Ge0/1, Ge0/2, and Ge0/3 to display the traffic ratio. The following figure shows that all traffic on Ge0/1 is load balanced based on link priority.



8.23.5 Configuring MLLB Based on Bandwidth and Sessions for a Network with Specific Routes

1. Applicable Products and Versions

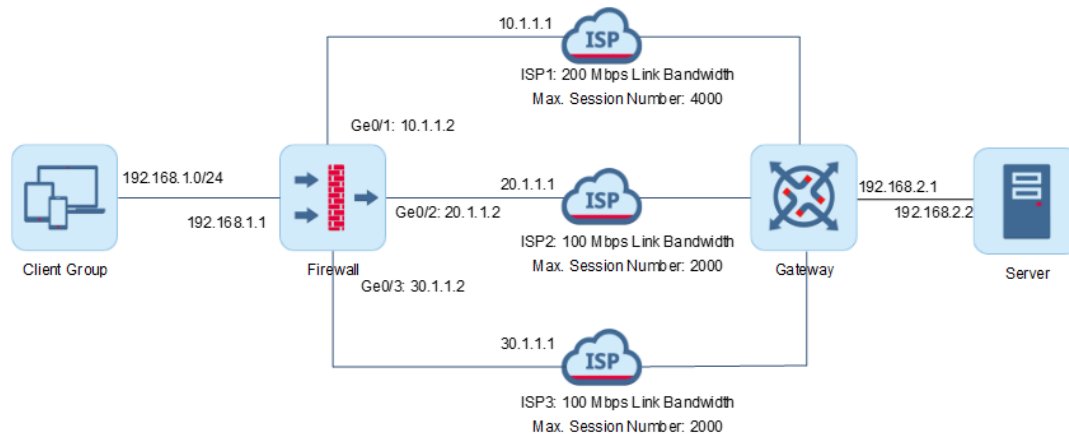
Table 8-20 Products and Versions

Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R8P1 or later

2. Service Demands

As shown in [Figure 8-18](#), a client group needs to access the server through the firewall. There are multiple links from the firewall to the server and their available bandwidths and supported session numbers are similar. To effectively distribute session traffic across these lines when session traffic is uneven, you are advised to configure load balancing based on both the bandwidth usage and session usage.

Figure 8-18 Topology of a Network with Specific Routes



Note

The server in the figure is for illustrative purposes only. It can be any other device such as a host.

3. Restrictions and Guidelines

- On the RG-WALL 1600 series firewall, one IP address cannot be assigned to multiple interfaces.

4. Prerequisites

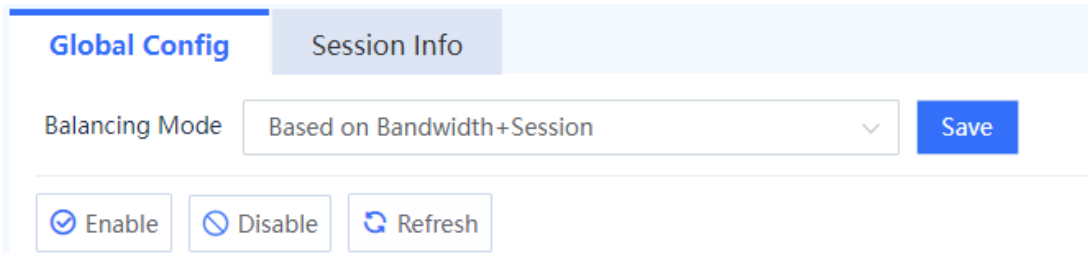
You have completed basic network configurations for the clients and the server, including interface IP addresses and static routes. Pay attention to the following points during configuration:

- After the firewall is connected to different ISP networks, ensure that direct next hops are correctly configured.
- After the firewall is connected to different ISP networks, configure static routes (outbound interfaces and next hops) to the server.

5. Procedure

(1) Configuring the MLLB Mode

- Choose **Network > Routing > Egress Load Balancing > Global Config**.
- Select **Based on Bandwidth+Session** from the **Balancing Mode** drop-down list.



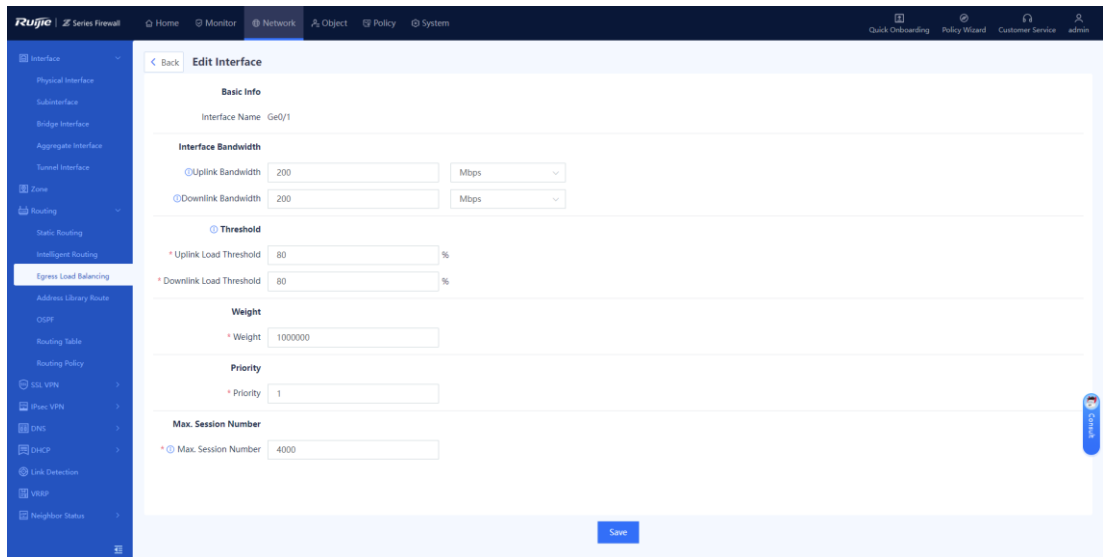
c Click **Save**.

(2) Configuring Interface Bandwidth and Max. Session Number for MLLB

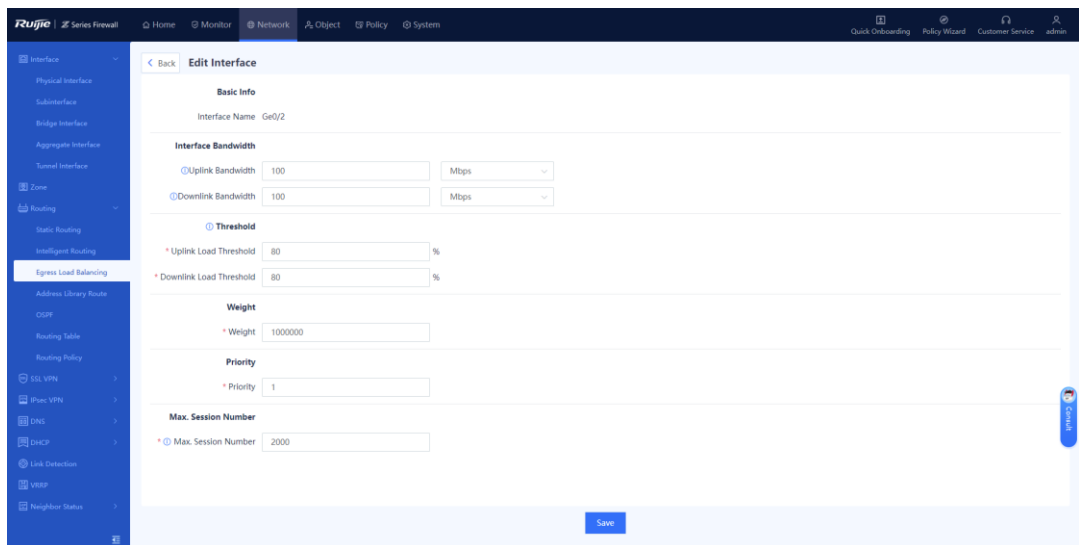
a Choose **Network > Routing > Egress Load Balancing > Global Config**.

b Click **Edit** in the **Operation** column of an interface to configure outbound interface parameters.

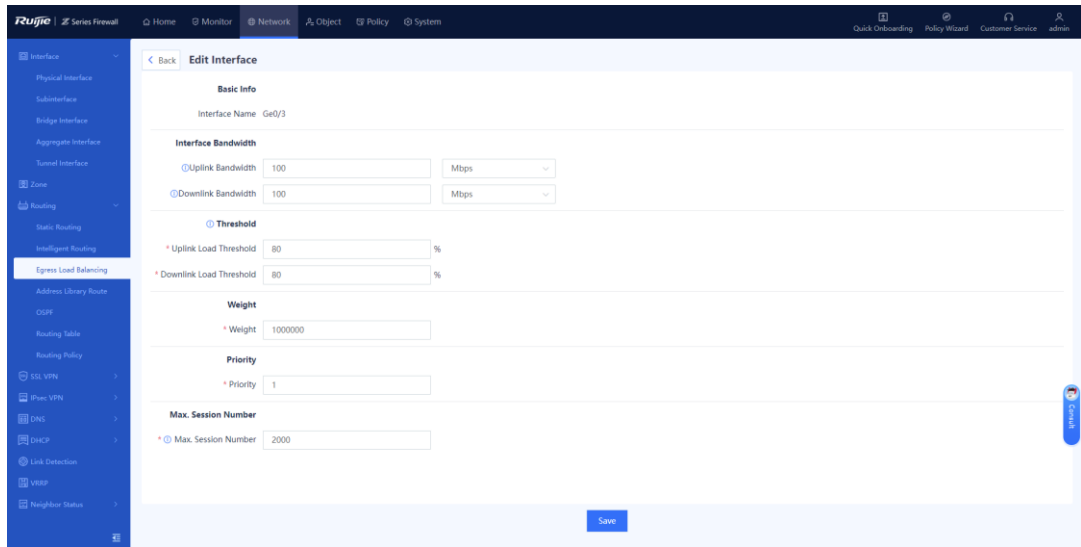
Configure the parameters for Ge0/1 and click **Save**.



Configure the parameters for Ge0/2 and click **Save**.



Configure the parameters for Ge0/3 and click **Save**.



(3) Configuring a Security Policy and Static Routing

a Configure a security policy.

Choose **Object > Address > IPv4 Address** and click **Create** to create address object 192.168.1.0/24 for the clients and address object 192.168.2.0/24 for the server.



Choose **Policy > Security Policy > Security Policy** and click **Create** to create a security policy.

<
Edit Security Policy

Basic Info

* Name

Enabled State Enable

* Policy Group ⊕ Add Group

Description

Src. and Dest.

Src. Security Zone

* Src. Address

Src. Region

Dest. Security Zone

* Dest. Address

Dest. Region

Service

Action Option Permit Deny

App, User, Effective Time v

Content Security

Intrusion Prevention Disable

Virus Protection Disable

URL Filtering Disable

Keyword Filtering Disable

Advanced

Click **Save**.

- b Configure static routing.

Choose **Network > Routing > Static Routing > IPv4**.

Click **Create** to create a static route to the server.

Create a static route to the server through the ISP1 link and click **Save**.

<
Edit Static Routing

IP Type IPv4

* Dest. IP Range/Mask

Next-Hop Address

Interface

* ⓘ Priority

Link Detection

Description

Create a static route to the server through the ISP2 link and click **Save**.

Edit Static Routing

IP Type IPv4

* Dest. IP Range/Mask 192.168.2.0/24

Next-Hop Address 20.1.1.1

Interface Ge0/2

* Priority 5

Link Detection Link Detection

Description ISP2 route

Create a static route to the server through the ISP3 link and click **Save**.

Edit Static Routing

IP Type IPv4

* Dest. IP Range/Mask 192.168.2.0/24

Next-Hop Address 30.1.1.1

Interface Ge0/3

* Priority 5

Link Detection Link Detection

Description ISP3 route

6. Verification

- Checking the MLLB Configuration

Choose **Network > Routing > Egress Load Balancing > Global Config** to check the MLLB mode and interface bandwidth configurations.

Global Config Session Info

Balancing Mode Based on Bandwidth+Session Save

Enable Disable Refresh Enter an interface name. Q

Interface Name	Max. Session Number	Uplink Bandwidth	Downlink Bandwidth	Uplink Load Threshold	Downlink Load Threshold	Operation
Ge0/1	4000	200Mbps	200Mbps	80%	80%	Edit
Ge0/2	2000	100Mbps	100Mbps	80%	80%	Edit
Ge0/3	2000	100Mbps	100Mbps	80%	80%	Edit

- Checking Static Routes

Choose **Network > Routing > Routing Table > IPv4** to check the equal-cost routes.

Static route	192.168.2.0/24	10.1.1.1	5	Ge0/1
Static route	192.168.2.0/24	20.1.1.1	5	Ge0/2
Static route	192.168.2.0/24	30.1.1.1	5	Ge0/3

- **Checking Traffic Steering Effects**

Concurrent traffic from multiple clients on the 192.168.1.0/24 network segment is sent to the server through the firewall. On the firewall web UI, choose **Monitor > Traffic Monitoring > Real-Time Traffic** and view the traffic trend graph. Select **Ge0/1**, **Ge0/2**, and **Ge0/3** in the **Interface** drop-down list to display the traffic ratio, which is 2:1:1.



8.23.6 Common Faults Diagnosis

Common MLLB faults include:

- Load balancing based on the bandwidth or weight results in proportional loading errors.
- MLLB fails and load balancing is ineffective.

1. Proportional Loading Error

In scenarios with high concurrent user traffic and uneven flow, significant proportional loading errors may occur. Configuring load balancing based on weight, uplink bandwidth, or downlink bandwidth may cause traffic imbalance. Therefore, you are advised to configure load balancing based on uplink load, downlink load, or bidirectional load. These load balancing modes consider the real-time rate (load), offering greater flexibility in load balancing.

2. Load Balancing Failure

MLLB is optional, and may become ineffective in some special scenarios:

- Traffic is always sent to other normal links because the DNS routing interface is abnormal .
- MLLB is disabled on some equal-cost interfaces of the static route on the MLLB page (as indicated by the toggle button on the right in the following figure), thus only some interfaces carry traffic load.

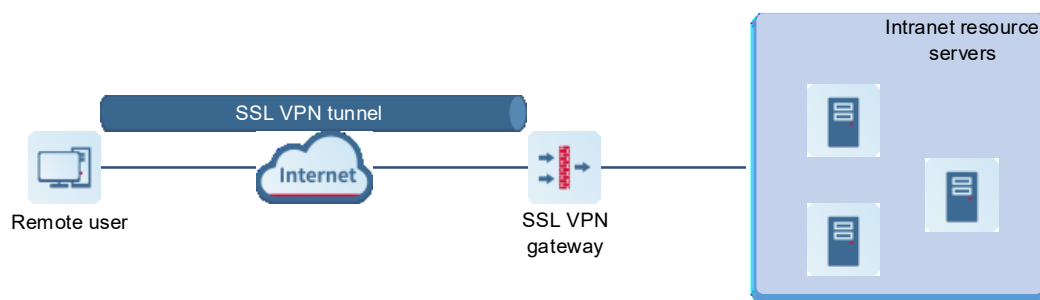
<input type="checkbox"/>	Interface Name	Uplink Bandwidth	Downlink Bandwidth	Uplink Load Threshold	Downlink Load Threshold	Operation
<input type="checkbox"/>	Ge0/1	200Mbps	200Mbps	80%	80%	<input checked="" type="checkbox"/> Edit
<input type="checkbox"/>	Ge0/2	100Mbps	100Mbps	80%	80%	<input type="checkbox"/> Edit
<input type="checkbox"/>	Ge0/3	100Mbps	100Mbps	80%	80%	<input checked="" type="checkbox"/> Edit

- Intelligent routing supports wideband LAN interfaces and tunnel interfaces that cannot be configured with interface bandwidth in MLLB mode. Therefore, you are not advised to use the bandwidth-based load balancing mode in this scenario.

8.24 SSL VPN

8.24.1 Overview

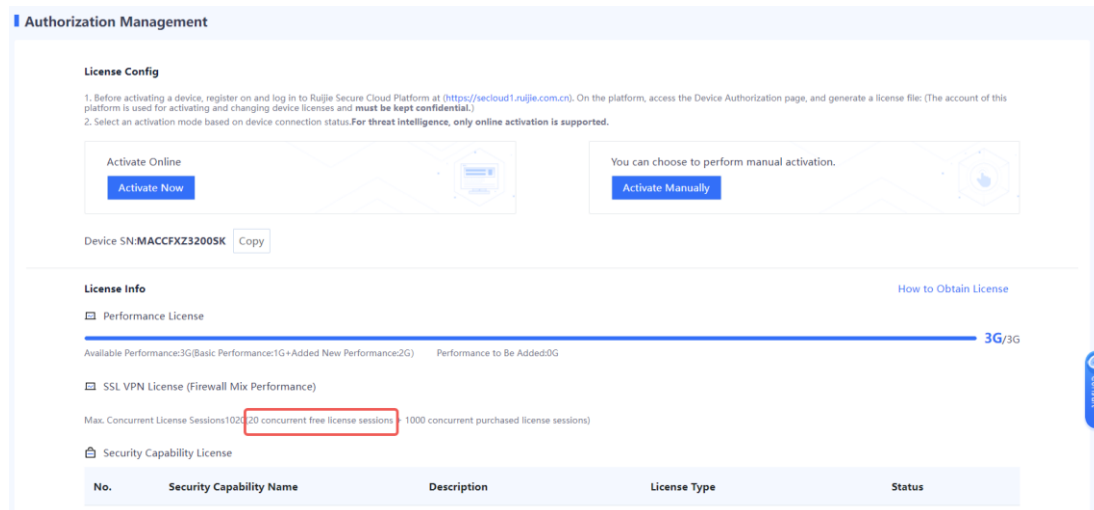
Secure Sockets Layer Virtual Private Network (SSL VPN) is an SSL-based remote access VPN technology, which uses a public network such as the Internet to establish an encrypted and secure remote access connection. In scenarios such as mobile office or remote office, customers and employees can securely access internal resources through an SSL VPN tunnel.



Principles of SSL VPN are as follows:

- (1) Remote users initiate remote access requests to the SSL VPN gateway on the SSL VPN client.
- (2) After receiving a request, the SSL VPN gateway authenticates the identity of the user (two authentication methods: username/password and username/password used together with hardware signature) and authorizes the user to access specific resources.
- (3) Upon being authorized, the user sends a resource access request to the SSL VPN gateway.
- (4) The SSL VPN gateway forwards the resource access request to the intranet resource server.
- (5) The SSL VPN gateway receives the response from the intranet resource server and forwards it to the user.

By default, the maximum number of concurrent users of the SSL VPN virtual gateway varies with each firewall model. To view details, choose **System > System Config > Authorization Management**. After the maximum number of concurrent users is exceeded, new users can no longer log in to the SSL VPN gateway. You can increase the number of concurrent users by purchasing and activating SSL VPN licenses. (The number of concurrent users can be accumulated if you import multiple licenses).



8.24.2 Application Scenario

SSL VPN is a secure remote access technology based on the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol. It protects communications using encryption and identity authentication and features fine-grained access control and application transparency. SSL VPN offers a secure, flexible, and convenient remote access solution for users to securely connect to internal network resources while protecting data confidentiality and integrity.

Scenario	Remarks
Egress deployment for remote office (local authentication)	Users access the company intranet through an SSL VPN tunnel.
Deployment on the intranet side of a NAT device for remote office	The gateway address is fixed. The gateway is configured with a public address and an actual fixed intranet address of the outbound interface. The customer needs to configure a DNAT policy on the device on the extranet side of the

(local authentication)	gateway to translate public addresses into intranet addresses for users to log in to the VPN from a public network.
Single gateway and multiple lines (local authentication)	Cross-ISP communication affects the VPN service experience. In actual implementation, multiple lines are deployed. In this scenario, the SSL VPN virtual gateway needs to support multiple gateway addresses and ports.
RADIUS authentication access	When users access an enterprise intranet through an SSL VPN tunnel, the SSL VPN gateway performs user authentication through the RADIUS server.
Off-path deployment mode (local authentication)	A firewall is connected to the core switch in off-path mode, and the SSL VPN service is deployed without changing the enterprise's existing network topology.
SMS two-factor authentication	In SMS two-factor authentication, when a user accesses the intranet through an SSL VPN, in addition to username and password verification, a random verification code is also verified. The verification code is sent to the login user through SMS. The user can access the intranet only after authentication succeeds. SMS two-factor authentication applies to SSL VPN access in local authentication and LDAP authentication scenarios.

8.24.3 Typical Configuration of Egress Deployment for Remote Office (Local Authentication)

1. Applicable Products and Versions

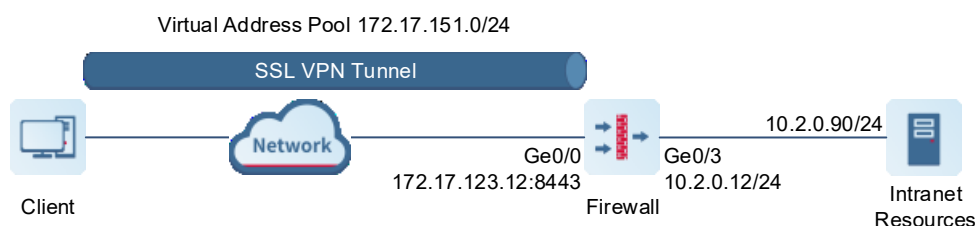
Table 8-21 Products and Versions

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS1.0R5 or later

2. Service Demands

The following figure shows an enterprise network. The enterprise authenticates remote office users based on local authentication on the firewall. Authenticated users can obtain access to the enterprise intranet.

The customer requests **user1** in user group **group1** in the default authentication domain to obtain an intranet address and access enterprise intranet resources like accessing resources on a LAN.



Item	Description	Remarks
Network interface	<ul style="list-style-type: none"> ● Interface: Ge0/0 (172.17.123.12), untrust ● Interface: Ge0/3 (10.2.0.12), trust 	
SSL VPN gateway configuration	Interface: Ge0/0 (172.17.123.12:8443)	
Authentication mode	Local authentication	
SSL VPN user	<ul style="list-style-type: none"> ● User group: group1 ● Username: user1 ● Password: test@123 	
Virtual address pool	172.17.151.0/24	Upon successful login, the client obtains an IP address from the virtual address pool. In the address pool, 172.17.151.1 is a device-side virtual address and is reserved.
Intranet resource subnet	10.2.0.0/24	Intranet resource subnet that can be accessed by the client.

3. Restrictions and Guidelines

- The subnets of the virtual address pool and firewall physical interface cannot be the same.

4. Prerequisites

- Intranet resources have been configured and can be accessed from the firewall.
- The routes from intranet resources to the subnet 172.17.151.0/24 where the SSL VPN client address pool resides are reachable.
- Remote office users have installed RG-SSLVPN_Client_2.0.

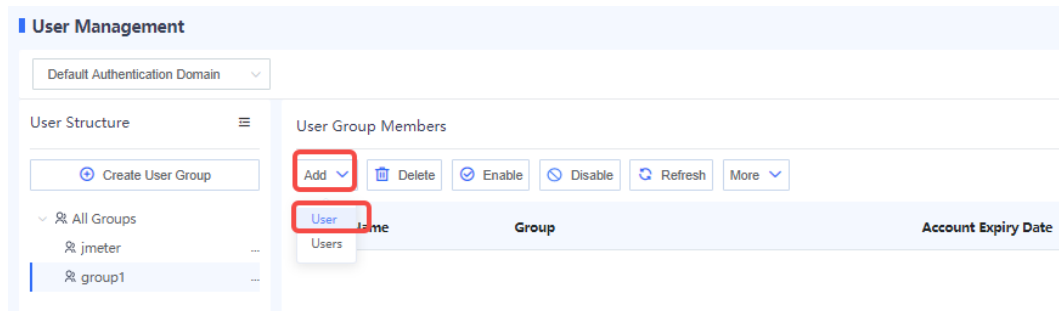
5. Procedure

(1) Configuring Interfaces and Security Zones

- a Log in to the firewall web UI, and choose **Network > Interface > Physical Interface**.
- b Click **Edit** in the **Operation** column of Ge0/0 to modify the configuration.
 - o Zone: **untrust**
 - o IP/Mask: **172.17.123.12/24**
 - o Next-Hop Address: Enter the actual address. In this example, **172.17.123.1**.
 - o Use the default configuration for the other parameters.

- c Click **Save**.
 - d Configure Ge0/3 in a similar way. Set **Zone** to **trust**, select **IPv4**, and set **IP/Mask** to **10.2.0.12/24**.
- (2) Configuring a User Group and Users
- a Choose **Object > User Authentication > User Management**.
 - b Click **Create User Group** to add a user group **group1**.

- c Click **Save**.
- d Click **Add** and choose **User**.



- e Configure user information as follows:
 - o Login Username: **user1**
 - o Parent Group: **/default/group1**
 - o Password: **test@123**

- f Click **Save**.

(3) Configuring an SSL VPN Gateway

- a Perform Basic Configuration

Choose **Network > SSL VPN > SSL VPN Gateway**.

Click **Create** and create an SSL VPN gateway as follows:

- o Set the gateway address to **Ge0/0** and use the default port number **8443**.
- o Configure **Max. Concurrent Users** according to the actual allowed authorized user number.
- o Use the default configuration for the other parameters.

[Back](#) **Add SSL VPN Gateway**

Basic Config Login Control

Network Config

* Gateway Name

Gateway Type Exclusive Shared

* Gateway Address Port Number

[Create](#)

Domain Name

Intranet DNS

[Create](#)

Preferred DNS Intranet DNS Customer DNS

Advanced

Protocol

* Protocol Version TLS1.2 TLS1.1 TLS1.0

* Algorithm Suite TLS-ECDHE-RSA-WITH-AES128-CBC-SHA256 TLS-ECDHE-RSA-WITH-AES256-CBC-SHA384 TLS-RSA-WITH-AES256-CBC-SHA

Gateway Certificate

Concurrency Control

* Max. Concurrent Users

Click **Next**.

b Perform Authentication Configuration

The default authentication domain is used. Therefore, use the default configuration for parameters on this page.

The screenshot shows the 'Add SSL VPN Gateway' configuration interface. At the top, there is a 'Back' button and the title 'Add SSL VPN Gateway'. Below this, a progress bar indicates that 'Basic Config' is completed and 'Login Control' is the current step. The 'Login Control' section is divided into several sub-sections:

- Authentication:** Includes a 'User Authentication Domain' dropdown set to 'default' and a 'Create User Authentication Domain' link.
- Prevent Brute-Force Attack:** Contains two lockout settings:
 - User Lockout:** A toggle switch is turned on. Below it, 'Max. User Attempts' is set to 5 and 'Lockout Period' is set to 300 seconds.
 - Single IP Lockout:** A toggle switch is turned on. Below it, 'Max. Single IP Attempts' is set to 5 and 'Lockout Period' is set to 300 seconds.
- Login Verification:** Includes several toggle switches:
 - Graphic Verification:** Turned off.
 - Enable upon:** Set to 0 consecutive input errors.
 - Hardware Signature Verification:** Turned off.
 - Maximum Signatures Bound to Each User:** Set to 3.
 - Auto Hardware Signature Approval:** Turned off.
 - Auto User Unbinding:** Turned off.
 - Auto Approval of Trusted Public Terminals:** Turned off.
- Idle Timeout:** A setting for 'The idle status will time out after' is set to 30 minutes.
- Client Version Control:** Includes radio buttons for 'Any Version' (selected), 'Latest Version on Secure Cloud', and 'Custom Config (The earliest version for clients on each platform can be specified)'.

Click **Next**.

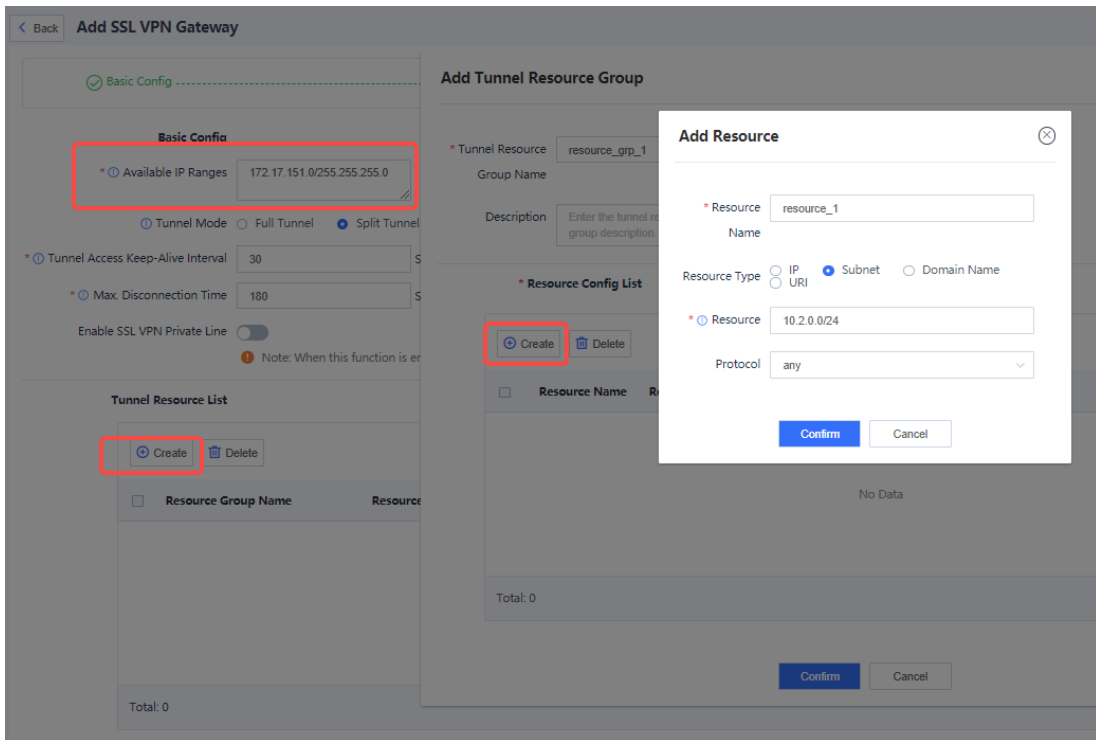
c Add Resources

Set **Available IP Ranges** to **172.17.151.0/255.255.255.0**.

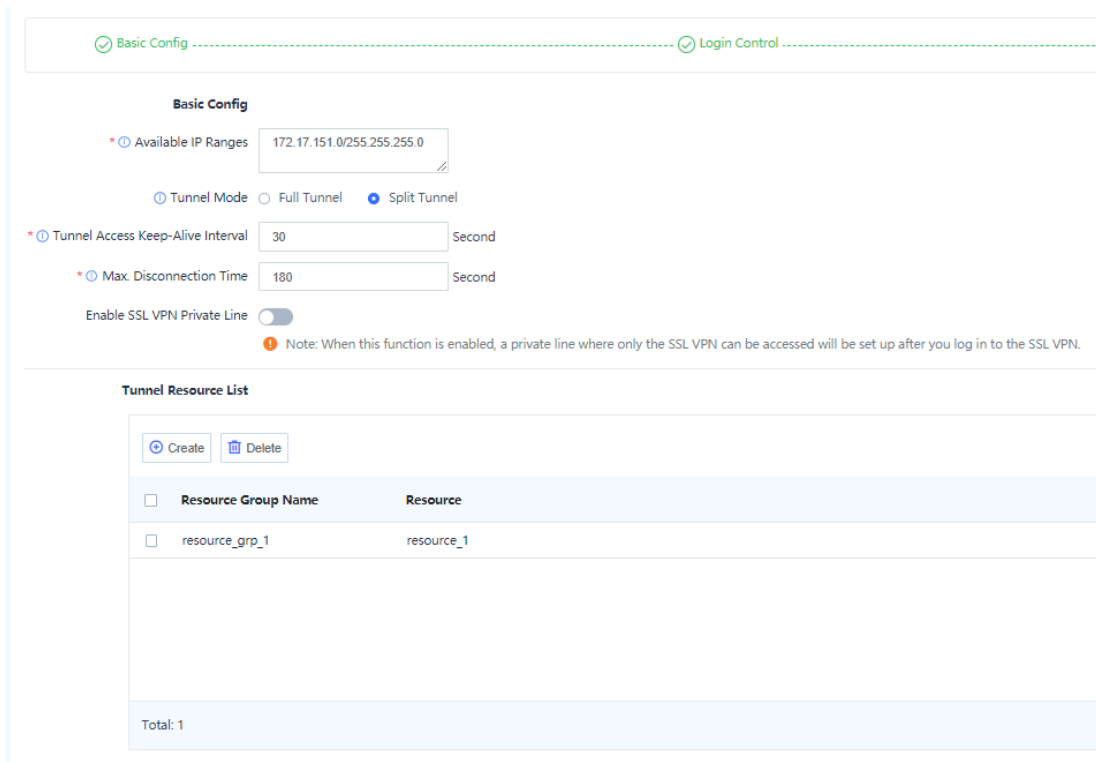
Use the default configuration for **Tunnel Access Keep-Alive Interval** and **Max. Disconnection Time**.

In the **Tunnel Resource List** area, click **Create** to create a tunnel resource group **resource_grp_1** and add a resource to the group:

- o Resource Name: **resource_1**
- o Resource Type: **Subnet**
- o Resource: **10.2.0.0/24**
- o Protocol: **any**



Click **Confirm** to create the resource. Then click **Confirm** to create the resource group, as shown in the following figure.



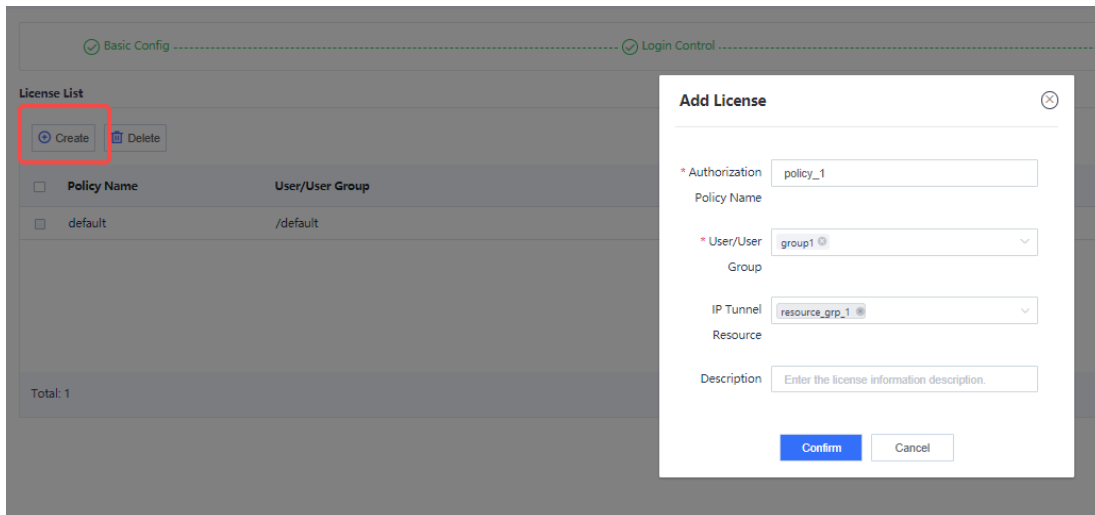
Click **Next**.

d Bind Resources

By default, the device provides a default policy. In this policy, the user/user group is fixed to the currently configured root authentication domain (**default** in this example) and cannot be edited. The default policy is not bound with any resources and cannot be deleted. You can choose to edit the default policy or directly create a policy. In this example, a new policy **policy_1** is created.

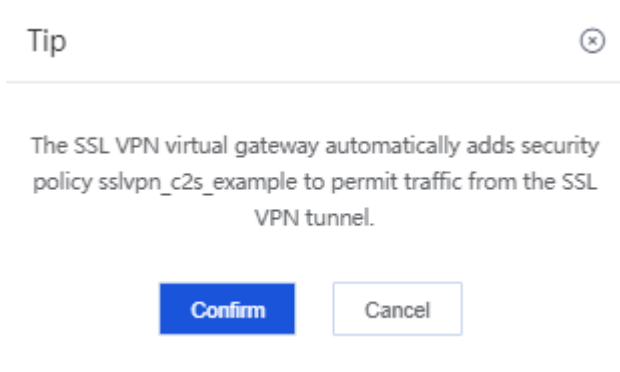
Click **Create** and create an authorization policy as follows:

- o Authorization Policy Name: **policy_1**
- o User/User Group: **group1**
- o IP Tunnel Resource: **resource_grp_1**



Click **Confirm** to save the authorization policy.

Click **Finish**. In the dialog box that is displayed, click **Confirm**.



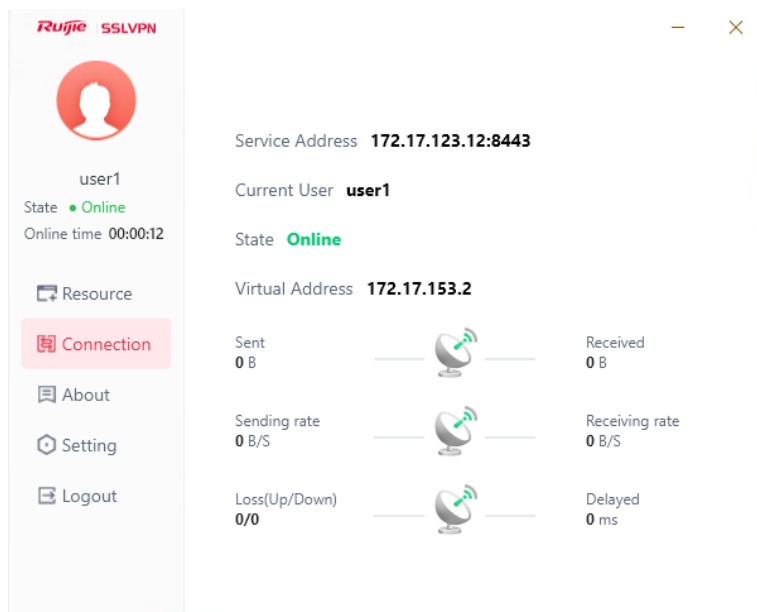
6. Verification

(1) Verifying the Result on the Client

- a Open the SSL VPN client, enter the configured SSL VPN gateway address, username, and password, and click **Login**.



b After login succeeds, the client obtains the assigned virtual address.



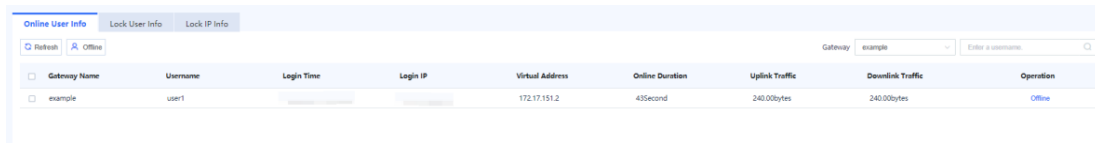
c Open a browser, and check whether intranet resources can be accessed by the client. The following figure uses a web server address as an example.



This is a web server

(2) Verifying the Result on the Device

- o Choose **Network > SSL VPN > Operation Monitoring** and check online user information. If there are multiple gateways, you can switch gateways in the upper right corner of the page to view online user information.



The screenshot shows a web interface for 'Online User Info'. At the top, there are tabs for 'Lock User Info' and 'Lock IP Info'. Below the tabs are 'Refresh' and 'Offline' buttons. On the right, there is a 'Gateway' dropdown menu set to 'example' and an 'Enter a username' search box. The main content is a table with the following columns: Gateway Name, Username, Login Time, Login IP, Virtual Address, Online Duration, Uplink Traffic, Downlink Traffic, and Operation. A single row of data is visible, showing a user named 'user1' with a login time of '2023-10-27 10:00:00', login IP of '172.17.151.2', online duration of '43Second', uplink traffic of '240.00bytes', and downlink traffic of '240.00bytes'. The 'Operation' column for this user is 'Online'.

Gateway Name	Username	Login Time	Login IP	Virtual Address	Online Duration	Uplink Traffic	Downlink Traffic	Operation
example	user1	2023-10-27 10:00:00	172.17.151.2		43Second	240.00bytes	240.00bytes	Online

- o Choose **Monitor > Log Monitoring > SSL VPN Log**. On the page that is displayed, check SSL VPN login logs.

8.24.4 Typical Configuration of Deployment on the Intranet Side of a NAT Device for Remote Office (Local Authentication)

1. Applicable Products and Versions

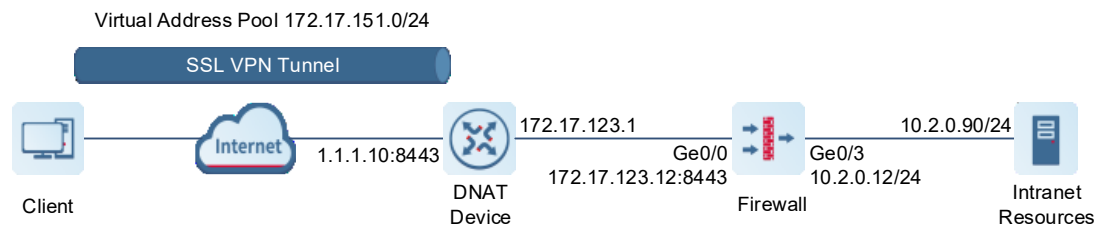
Table 8-22 Products and Versions

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS1.0R5 or later

2. Service Demands

The firewall is deployed as an SSL VPN gateway on the intranet side of a DNAT device, as shown in the following figure. Remote office users access the firewall from a public network, and the firewall authenticates the users through local authentication. Authenticated users can obtain access to the enterprise intranet.

The customer requests **user1** in user group **group1** in the default authentication domain to obtain an intranet address and access enterprise intranet resources like accessing resources on a LAN.



Item	Description	Remarks
DNAT	<ul style="list-style-type: none"> Public address: 1.1.1.10, SSL VPN gateway address Private address: 172.17.123.12 Public network TCP/UDP port: 8443 Private network TCP/UDP port: 8443 	This mapping enables traffic from extranet users to 1.1.1.10:8443 to be forwarded to the SSL VPN gateway (firewall).
Network interface	<ul style="list-style-type: none"> Interface: Ge0/0 (172.17.123.12), untrust Interface: Ge0/3 (10.2.0.12), trust 	
SSL VPN gateway configuration	<ul style="list-style-type: none"> Manually configured address: 1.1.1.10:8443 Interface: Ge0/0 (172.17.123.12:8443) 	
Authentication mode	Local authentication	
SSL VPN user	<ul style="list-style-type: none"> User group: group1 Username: user1 Password: test@123 	

Virtual address pool	172.17.151.0/24	Upon successful login, the client obtains an IP address from the virtual address pool. In the address pool, 172.17.151.1 is a device-side virtual address and is reserved.
Intranet resource subnet	10.2.0.0/24	Intranet resource subnet that can be accessed by the client.

3. Restrictions and Guidelines

- The subnets of the virtual address pool and firewall physical interface cannot be the same.

4. Prerequisites

- Intranet resources have been configured and can be accessed through the firewall.
- The routes from intranet resources to the subnet 172.17.151.0/24 where the SSL VPN client address pool resides are reachable.
- Remote office users have installed RG-SSLVPN_Client_2.0.
- A DNAT policy has been configured on the DNAT device.

5. Procedure

(1) Configuring Interfaces and Security Zones

- a Log in to the firewall web UI, and choose **Network > Interface > Physical Interface**.
- b Click **Edit** in the **Operation** column of Ge0/0 to modify the configuration.
 - o Zone: **untrust**
 - o IP/Mask: **172.17.123.12/24**
 - o Next-Hop Address: Enter the actual address. In this example, **172.17.123.1**.
 - o Use the default configuration for the other parameters.

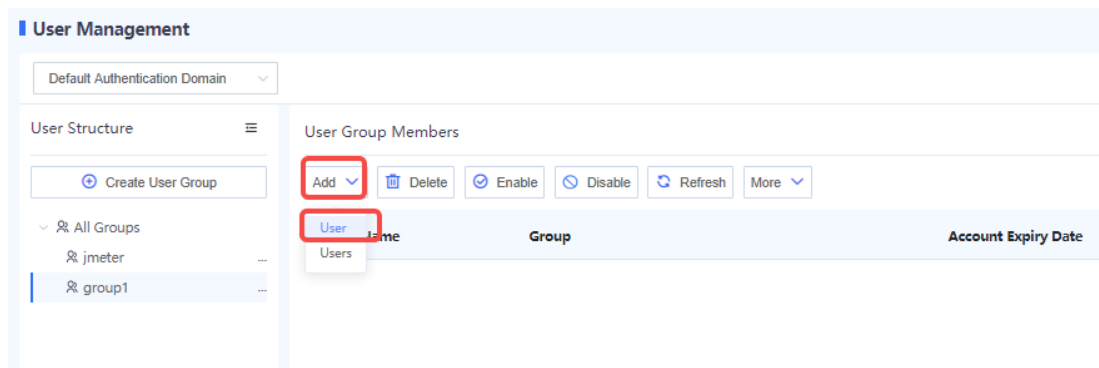
- c Click **Save**.
- d Configure Ge0/3 in a similar way. Set **Zone** to **trust**, select **IPv4**, and set **IP/Mask** to **10.2.0.12/24**.

(2) Configuring a User Group and Users

- a Choose **Object > User Authentication > User Management**.
- b Click **Create User Group** to add a user group **group1**.

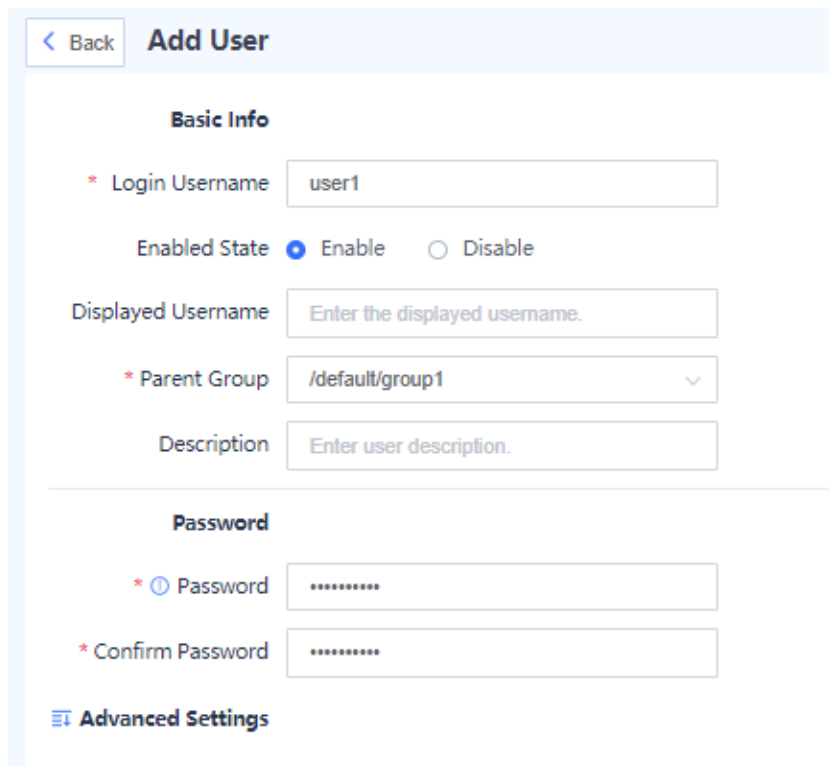
- c Click **Save**.

d Click **Add** and choose **User**.



e Configure user information as follows:

- o Login Username: **user1**
- o Parent Group: **/default/group1**
- o Password: **test@123**



f Click **Save**.

(3) Configuring a Gateway

a Perform Basic Configuration

Choose **Network > SSL VPN > SSL VPN Gateway**.

Click **Create** and create an SSL VPN gateway as follows:

- o Set gateway address 1 to **Ge0/0** and use the default port number **8443**.
- o Set gateway address 2 to **Manually Configure IP** and enter the public address **1.1.1.10** configured in

DNAT.

- o Configure **Max. Concurrent Users** according to the actual allowed authorized user number.
- o Use the default configuration for the other parameters.

The screenshot displays a configuration page with the following sections:

- Basic Config**: Includes a breadcrumb for "Login Control".
- Network Config**:
 - * Gateway Name: example
 - Gateway Type: Exclusive (selected), Shared
 - * Gateway Address: Ge0/0(Off) | 172.17.123.12/26 (dropdown), 172.17.123.12 (input), Port Number: 8443
 - Manually Configure IP: 1.1.1.10 (input), Port Number: 8443, Delete button
 - Create button
 - Domain Name: Enter a domain name. (input)
 - Intranet DNS: Enter an intranet DNS server address. (input), Create button
 - Preferred DNS: Intranet DNS, Customer DNS (selected)
- Advanced**:
 - Protocol**:
 - * Protocol Version: TLS1.2 (checked), TLS1.1, TLS1.0
 - * Algorithm Suite: TLS-ECDHE-RSA-WITH-AES128-CBC-SHA256 (checked), TLS-ECDHE-RSA-WITH-AES256-CBC-SHA384 (checked), TLS-RSA-WITH-AES256-CBC-SHA (checked)
 - Gateway Certificate: default (dropdown)
 - Concurrency Control**:
 - * Max. Concurrent Users: 20 (input)

Click **Next**.

b Perform Authentication Configuration

The default authentication domain is used. Therefore, use the default configuration for parameters on this page.

[Back](#) **Add SSL VPN Gateway**

Basic Config Login Control

Authentication

* User Authentication Domain [Create User Authentication Domain](#)

Prevent Brute-Force Attack

User Lockout

* Max. User Attempts Time * Lockout Period Second

Single IP Lockout

* Max. Single IP Attempts Time * Lockout Period Second

Login Verification

Graphic Verification

* Enable upon Consecutive Input Errors

Hardware Signature Verification

* Maximum Signatures Bound to Each User

Auto Hardware Signature Approval

Auto User Unbinding

Auto Approval of Trusted Public Terminals

Idle Timeout

* The idle status will time out after minutes.

Client Version Control

Available Client Versions Any Version Latest Version on Secure Cloud Custom Config (The earliest version for clients on each platform can be specified.)

Click **Next**.

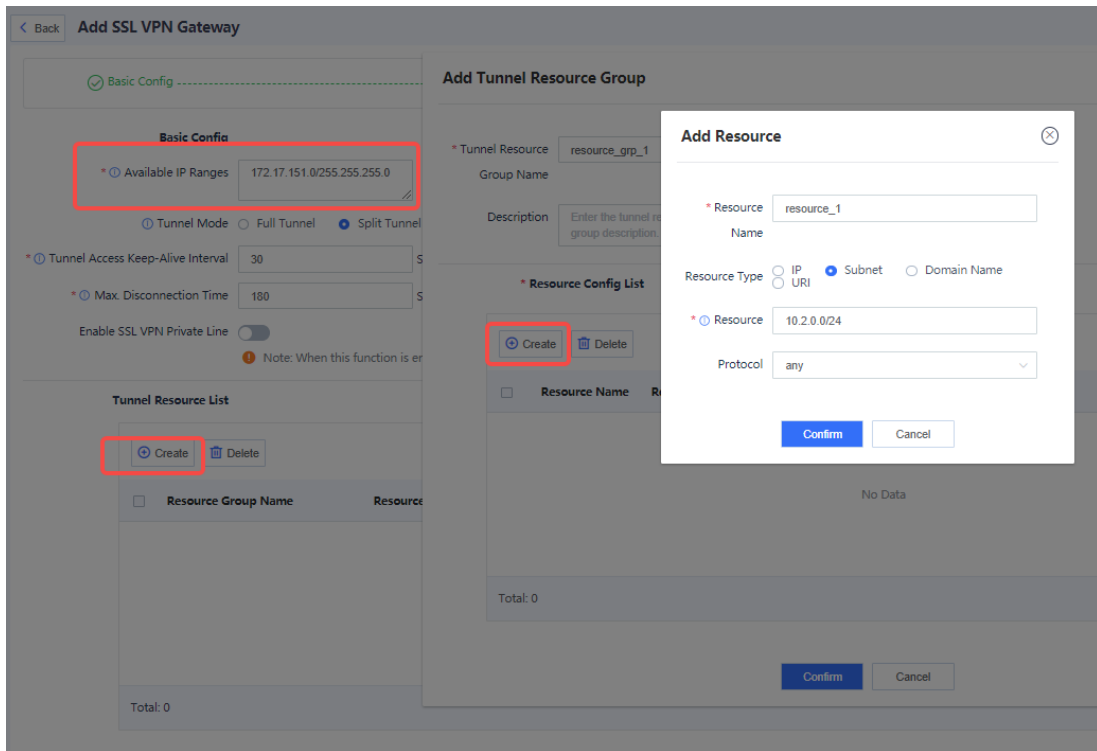
c Add Resources

Set **Available IP Ranges** to **172.17.151.0/255.255.255.0**.

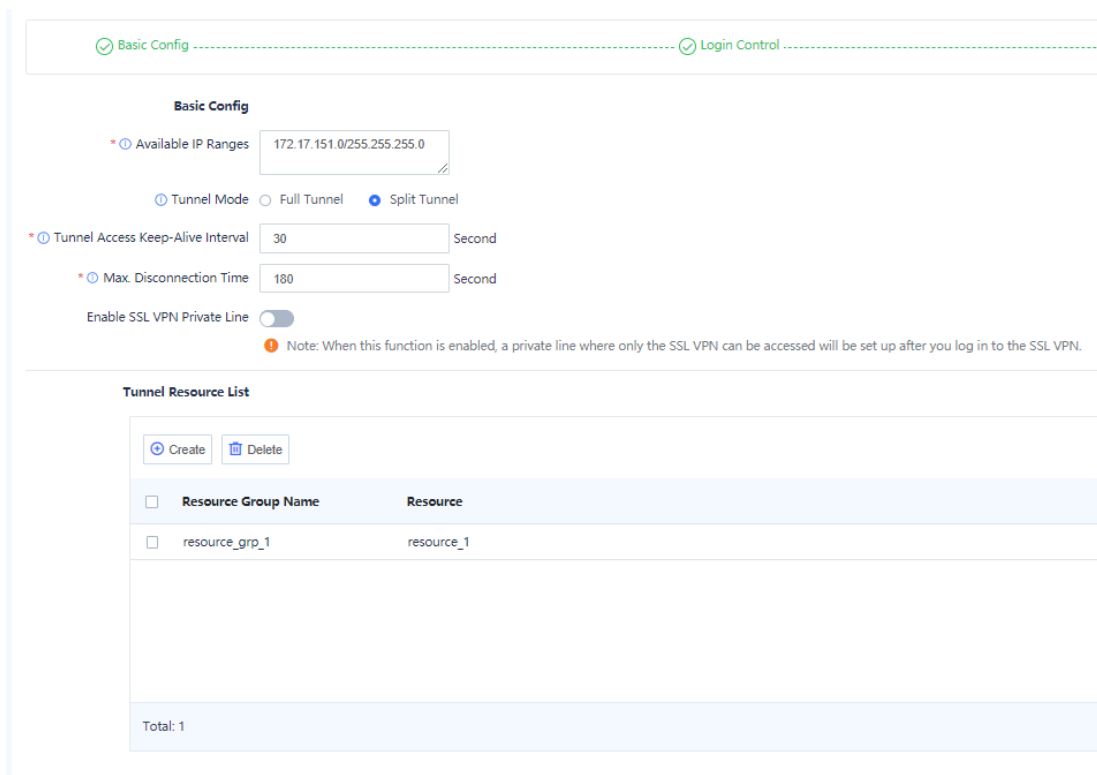
Use the default configuration for **Tunnel Access Keep-Alive Interval** and **Max. Disconnection Time**.

In the **Tunnel Resource List** area, click **Create** to create a tunnel resource group **resource_grp_1** and add a resource to the group:

- o Resource Name: **resource_1**
- o Resource Type: **Subnet**
- o Resource: 10.2.0.0/24
- o Protocol: **any**



Click **Confirm** to create the resource. Then click **Confirm** to create the resource group, as shown in the following figure.



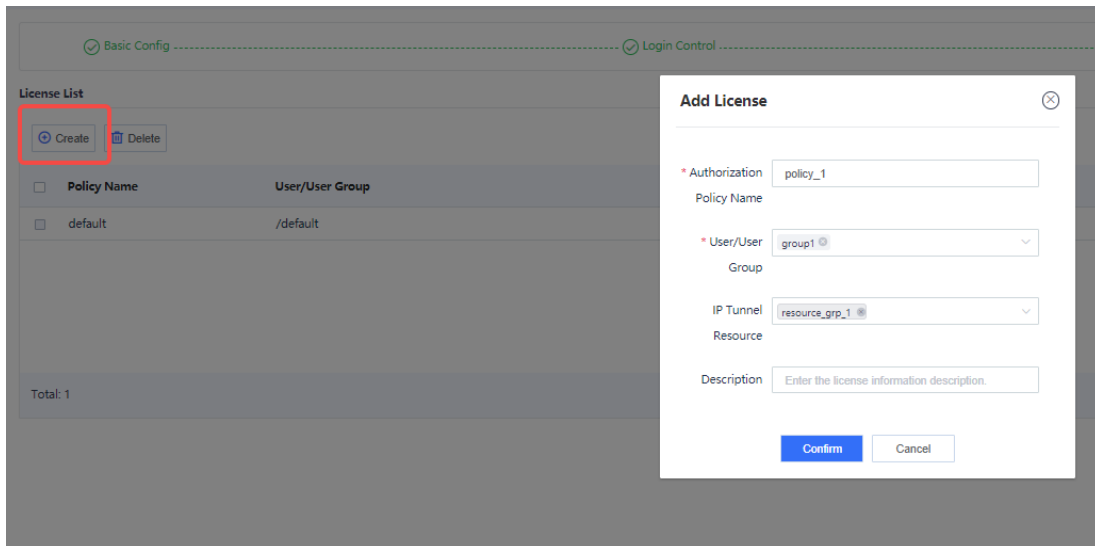
Click **Next**.

d Bind Resources

By default, the device provides a default policy. In this policy, the user/user group is fixed to the currently configured root authentication domain (**default** in this example) and cannot be edited. The default policy is not bound with any resources and cannot be deleted. You can choose to edit the default policy or directly create a policy. In this example, a new policy **policy_1** is created.

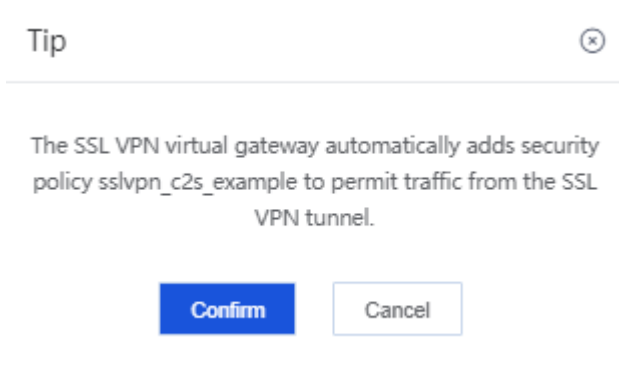
Click **Create** and create an authorization policy as follows:

- o Authorization Policy Name: **policy_1**
- o User/User Group: **group1**
- o IP Tunnel Resource: **resource_grp_1**



Click **Confirm** to save the authorization policy.

Click **Finish**. In the dialog box that is displayed, click **Confirm**.



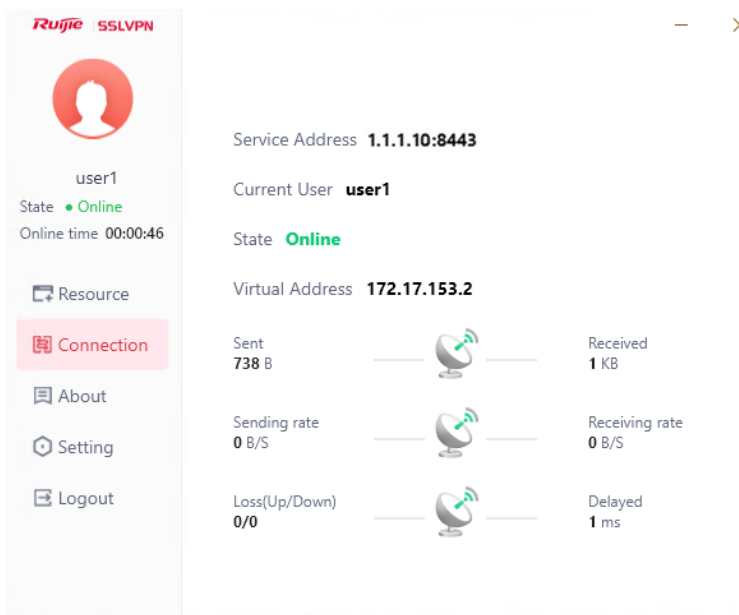
6. Verification

(1) Verifying the Result on the Client

- a Open the client, enter the configured public address of the SSL VPN gateway, username, and password, and click **Login**.



b After login succeeds, the client obtains the assigned virtual address.



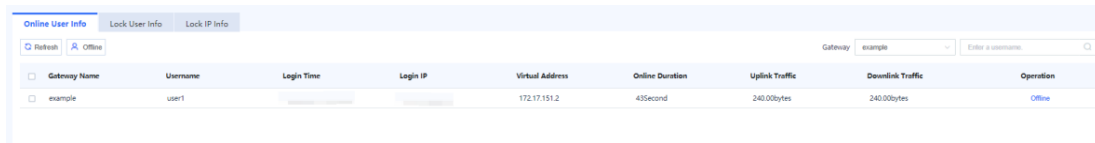
c Open a browser, and check whether intranet resources can be accessed by the client. The following figure uses a web server address as an example.



This is a web server

(2) Verifying the Result on the Device

- o Choose **Network > SSL VPN > Operation Monitoring** and check online user information. If there are multiple gateways, you can switch gateways in the upper right corner of the page to view online user information.



The screenshot shows a web interface for 'Online User Info'. At the top, there are tabs for 'Lock User Info' and 'Lock IP Info'. Below the tabs are 'Refresh' and 'Offline' buttons. On the right, there is a 'Gateway' dropdown menu set to 'example' and an 'Enter a username' search field. The main content is a table with the following columns: Gateway Name, Username, Login Time, Login IP, Virtual Address, Online Duration, Uplink Traffic, Downlink Traffic, and Operation. A single row is visible with the following data: Gateway Name: example, Username: user1, Login Time: [blurred], Login IP: [blurred], Virtual Address: 172.17.151.2, Online Duration: 43Second, Uplink Traffic: 240.00bytes, Downlink Traffic: 240.00bytes, and Operation: Online.

Gateway Name	Username	Login Time	Login IP	Virtual Address	Online Duration	Uplink Traffic	Downlink Traffic	Operation
example	user1	[blurred]	[blurred]	172.17.151.2	43Second	240.00bytes	240.00bytes	Online

- o Choose **Monitor > Log Monitoring > SSL VPN Log**. On the page that is displayed, check SSL VPN login logs.

8.24.5 Typical Configuration of Off-Path Deployment Mode (Local Authentication)

1. Applicable Products and Versions

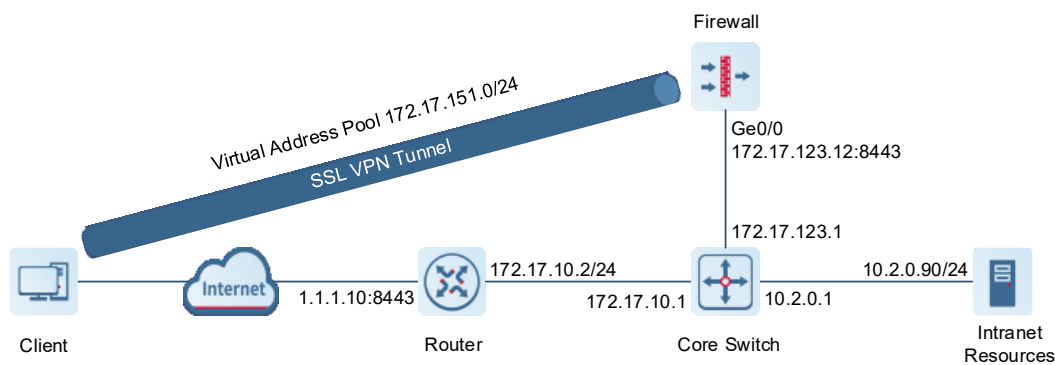
Table 8-23 Products and Versions

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS1.0R5 or later

2. Service Demands

The following figure shows an enterprise network. A firewall is connected to the core switch in off-path mode, and the SSL VPN service is deployed on the firewall without changing the enterprise's existing network topology. The enterprise authenticates remote office users based on local authentication on the firewall. Authenticated users can obtain access to the enterprise intranet.

The customer requests **user1** in user group **group1** in the default authentication domain to obtain an intranet address and access enterprise intranet resources like accessing resources on a LAN.



Item	Description	Remarks
Router (egress DNAT device)	<ul style="list-style-type: none"> Public address: 1.1.1.10, public address of the SSL VPN gateway Address after DNAT: 172.17.123.12, private address of the SSL VPN gateway Intranet address: 172.17.10.2 Public network TCP/UDP port: 8443 Private network TCP/UDP port: 8443 	DNAT enables traffic from extranet users to 1.1.1.10:8443 to be forwarded to the SSL VPN gateway (firewall) through the router.
Core switch	<ul style="list-style-type: none"> Intranet egress gateway: 172.17.10.1 Firewall: 172.17.123.1 Intranet resource gateway: 10.2.0.1 Specific route to the virtual address pool subnet 172.17.151.0/24, next-hop address: 172.17.123.12 	A specific route needs to be configured if no SNAT policy is used.
Network interface	Interface: Ge0/0 (172.17.123.12), trust	

SSL VPN gateway configuration	<ul style="list-style-type: none"> Manually configured address: 1.1.1.10:8443 Interface: Ge0/0 (172.17.123.12:8443) SNAT policy 	An SNAT policy needs to be configured if no route is configured on the core switch.
Authentication mode	Local authentication	
SSL VPN user	<ul style="list-style-type: none"> User group: group1 Username: user1 Password: test@123 	
Virtual address pool	172.17.151.0/24	Upon successful login, the client obtains an IP address from the virtual address pool. In the address pool, 172.17.151.1 is a virtual firewall address and is reserved.
Intranet resource subnet	10.2.0.0/24	Intranet resource subnet that can be accessed by the client.

3. Restrictions and Guidelines

- The subnets of the virtual address pool and firewall physical interface cannot be the same.

4. Prerequisites

- Intranet resources have been configured and can be accessed through the firewall.
- The routes from intranet resources to the subnet 172.17.151.0/24 where the SSL VPN client address pool resides are reachable.
- Remote office users have installed RG-SSLVPN_Client_2.0.
- A DNAT policy has been configured on the egress device (router).
- A specific route to the virtual address pool has been configured on the core switch (if no SNAT policy is configured on the firewall).

To enable response packets of intranet resources to be correctly forwarded to the firewall through the core switch, you need to configure a specific route to the virtual address pool on the core switch, or add an SNAT policy on the firewall to translate the source address of an access request packet from the virtual address pool to the firewall address. You are advised to configure a specific route, because an SNAT policy will prevent the intranet server from obtaining actual user addresses.

5. Procedure

(1) Configuring Interfaces and Security Zones

- a Log in to the firewall web UI, and choose **Network > Interface > Physical Interface**.
- b Click **Edit** in the **Operation** column of Ge0/0 to modify the configuration.
 - o Zone: **trust**
 - o Interface Type: **LAN Interface**
 - o IPv4/Mask: **172.17.123.12/24**

- o Use the default configuration for the other parameters.

Edit Physical Interface

Basic Info

Interface Name:

Description:

Connection Status: Enable Disable

Mode: Routing Mode Transparent Mode Off-Path Mode

* Zone: [Add Security Zone](#)

Interface Type: WAN Interface LAN Interface

Address

IP Type: IPv4 IPv6

Connection Type: Static Address DHCP PPPoE

* IP/Mask:

Line Bandwidth

Uplink:

Downlink:

Access Management

Permit: HTTPS PING SSH

Advanced

MTU:

MAC:

- c Click **Save**.

(2) Configuring an IPv4 Static Route

- a Choose **Network > Routing > Static Routing > IPv4**.
- b Click **Create** and configure a static route according to the following figure.
 - o Dest. IP Range/Mask: **0.0.0.0/0**
 - o Next-Hop Address (gateway address): **172.17.123.1**
 - o Interface: **Ge0/0**
 - o Use the default configuration for the other parameters.

Create Static Routing

IP Type IPv4

* Dest. IP Range/Mask 0.0.0.0/0

Next-Hop Address 172.17.123.1

Interface Ge0/0

* ① Priority 5

Link Detection Link Detection

Description

c Click **Save**.

(3) Configuring a User Group and Users

a Choose **Object > User Authentication > User Management**.

b Click **Create User Group** to add a user group **group1**.

User Management

Default Authentication Domain

User Structure

Create User Group

User Group Members

Add Delete Enable Disable Refresh

Name Group

Create User Group

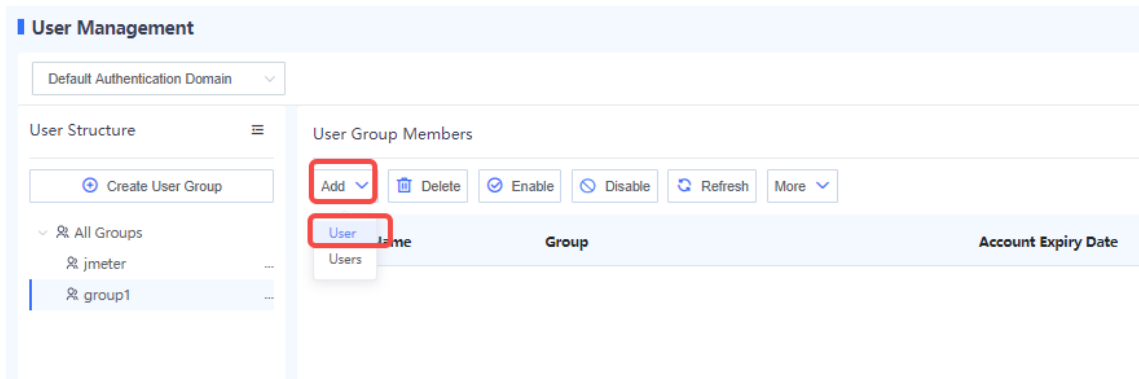
* User Group Name group1

Parent Group Enter or select a value.

Save Cancel

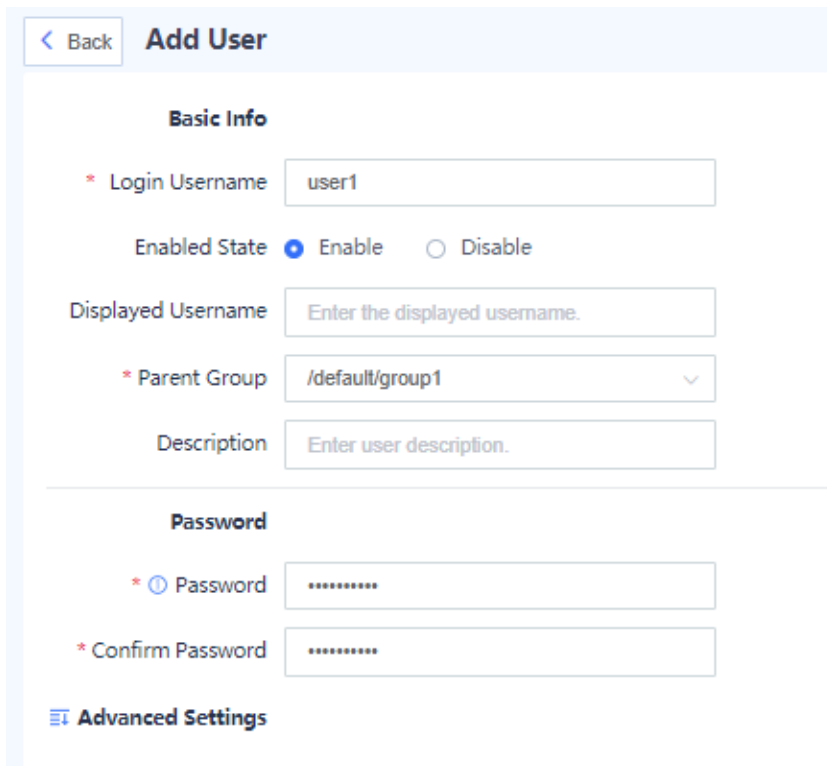
c Click **Save**.

d Click **Add** and choose **User**.



e Configure user information as follows:

- o Login Username: **user1**
- o Parent Group: **/default/group1**
- o Password: **test@123**



f Click **Save**.

(4) Configuring a Gateway

a Perform Basic Configuration

Choose **Network > SSL VPN > SSL VPN Gateway**.

Click **Create** and create an SSL VPN gateway as follows:

- o Set gateway address 1 to **Ge0/0** and use the default port number **8443**.
- o Set gateway address 2 to **Manually Configure IP** and enter the public address **1.1.1.10** configured in DNAT.

- o Configure **Max. Concurrent Users** according to the actual allowed authorized user number.
- o Use the default configuration for the other parameters.

Basic Config
 Login Control

Network Config

* Gateway Name

① Gateway Type Exclusive Shared

* Gateway Address ① Port Number

① Port Number [Delete](#)

[Create](#)

Domain Name

Intranet DNS

[Create](#)

Preferred DNS Intranet DNS Customer DNS

[Advanced](#)

Protocol

* Protocol Version TLS1.2 TLS1.1 TLS1.0

* Algorithm Suite TLS-ECDHE-RSA-WITH-AES128-CBC-SHA256 TLS-ECDHE-RSA-WITH-AES256-CBC-SHA384 TLS-RSA-WITH-AES256-CBC-SHA

Gateway Certificate

Concurrency Control

* ① Max. Concurrent Users

Click **Next**.

b Perform Authentication Configuration

The default authentication domain is used. Therefore, use the default configuration for parameters on this page.

Add SSL VPN Gateway

Basic Config Login Control

Authentication

* User Authentication Domain: default [Create User Authentication Domain](#)

Prevent Brute-Force Attack

User Lockout:

* Max. User Attempts: 5 Time * Lockout Period: 300 Second

Single IP Lockout:

* Max. Single IP Attempts: 5 Time * Lockout Period: 300 Second

Login Verification

Graphic Verification

* Enable upon: 0 Consecutive Input Errors

Hardware Signature Verification

* Maximum Signatures Bound to Each User: 3

Auto Hardware Signature Approval

Auto User Unbinding

Auto Approval of Trusted Public Terminals

Idle Timeout

* The idle status will time out after: 30 minutes.

Client Version Control

Available Client Versions: Any Version Latest Version on Secure Cloud Custom Config (The earliest version for clients on each platform can be specified.)

Click **Next**.

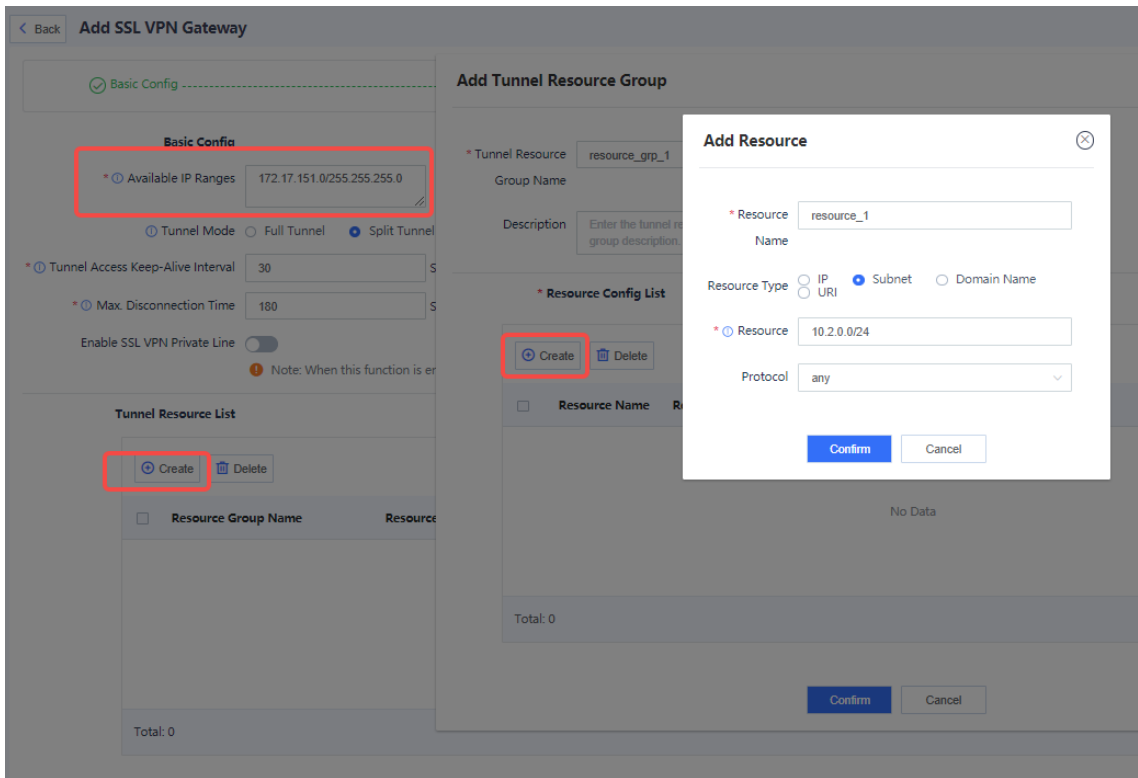
c Add Resources

Set **Available IP Ranges** to 172.17.151.0/255.255.255.0.

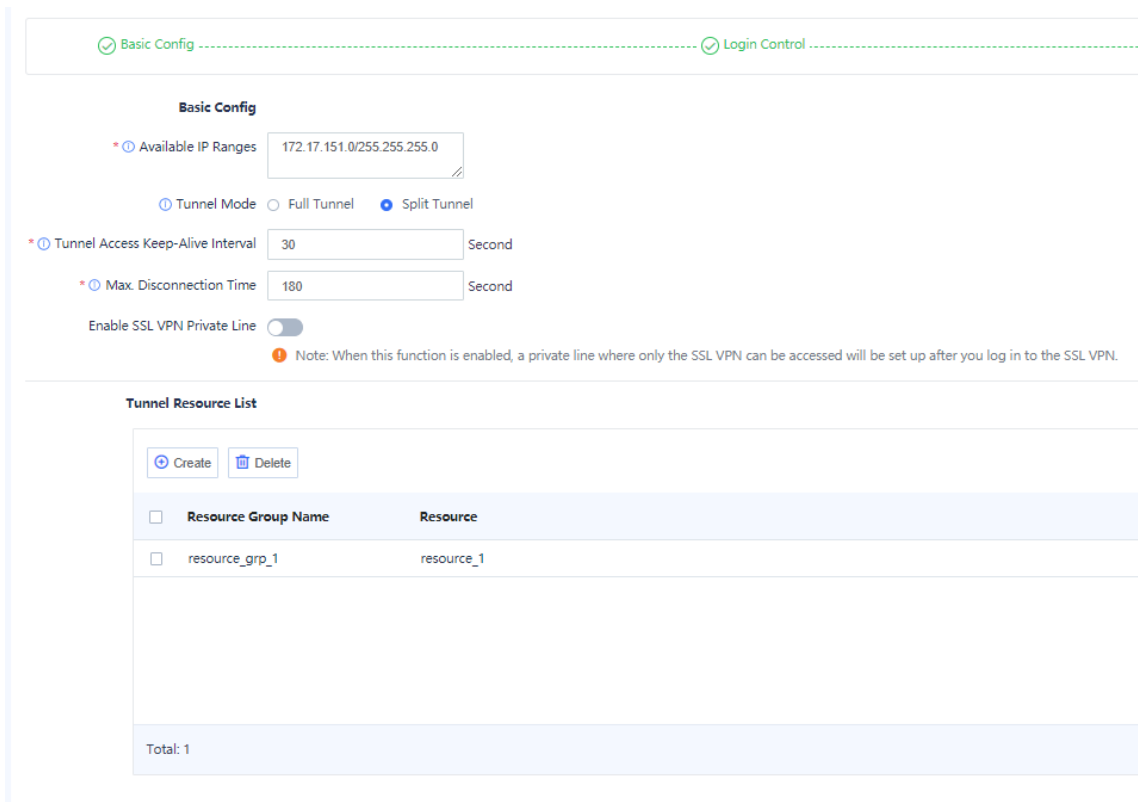
Use the default configuration for **Tunnel Access Keep-Alive Interval** and **Max. Disconnection Time**.

In the **Tunnel Resource List** area, click **Create** to create a tunnel resource group **resource_grp_1** and add a resource to the group:

- o Resource Name: **resource_1**
- o Resource Type: **Subnet**
- o Resource: **10.2.0.0/24**
- o Protocol: **any**



Click **Confirm** to create the resource. Then click **Confirm** to create the resource group, as shown in the following figure.



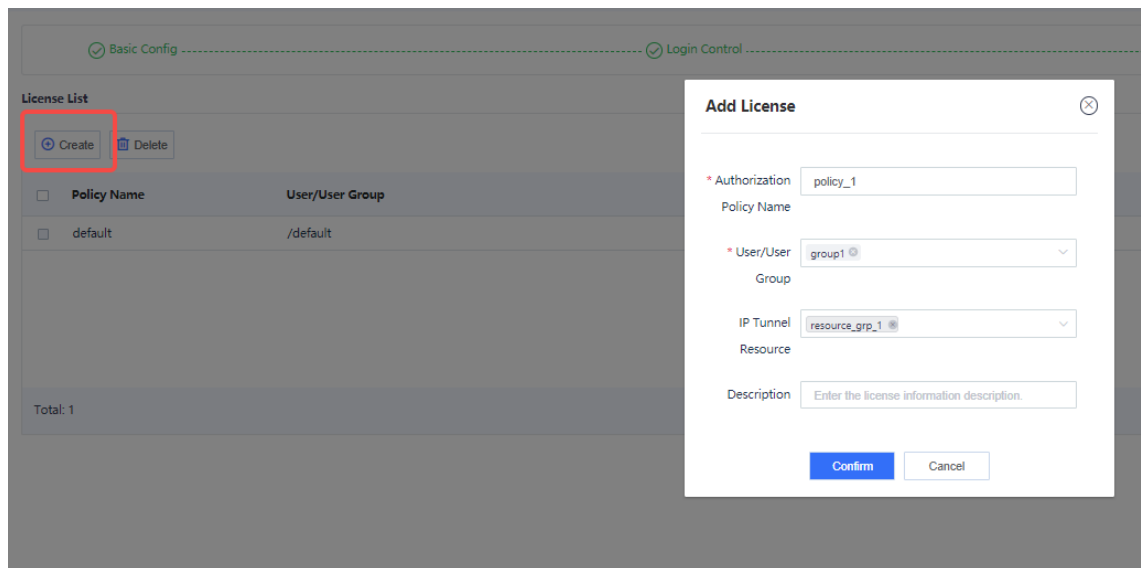
Click **Next**.

d Bind Resources

By default, the device provides a default policy. In this policy, the user/user group is fixed to the currently configured root authentication domain (**default** in this example) and cannot be edited. The default policy is not bound with any resources and cannot be deleted. You can choose to edit the default policy or directly create a policy. In this example, a new policy **policy_1** is created.

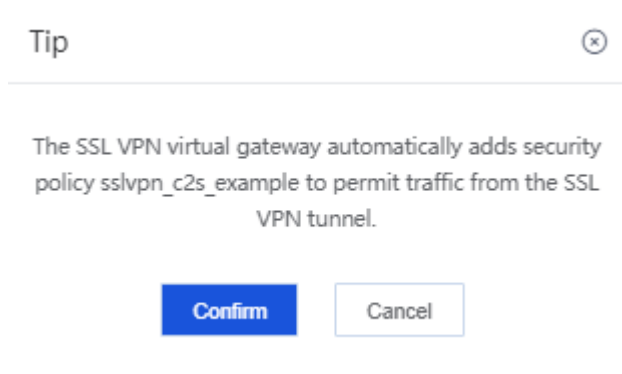
Click **Create** and create an authorization policy as follows:

- o Authorization Policy Name: **policy_1**
- o User/User Group: **group1**
- o IP Tunnel Resource: **resource_grp_1**



Click **Confirm** to save the authorization policy.

Click **Finish**. In the dialog box that is displayed, click **Confirm**.



(5) Configuring an SNAT Policy

⚠ Caution

- Skip this section if a specific route to the virtual address pool has been configured on the core switch.
- An SNAT policy needs to be configured on the firewall only when no specific route is configured on the core switch. An SNAT policy enables intranet response packets to be correctly forwarded to the

firewall. In this case, the source address of packets received on the intranet server is the firewall address, but not the actual user address. Therefore, SNAT policy configuration is not recommended.

- a Choose **Policy > NAT Policy > NAT**.
 - b Click **Create**. Configure a NAT policy as follows:
-

 **Note**

When an SSL VPN gateway is created successfully, the device automatically creates two address objects: the virtual gateway address object **ippool_{Gateway name}** and the resource address object **res_{Gateway name}**. In this example, the gateway name is **example**, so the created object names are **ippool_example** and **res_example**.

- o Src. Security Zone: **untrust**
- o Src. Address: **ippool_example**
- o Dest. Security Zone: **trust**
- o Dest. Address: **res_example**
- o Service: **any**
- o Packet After NAT: Outbound Interface Address

[< Back](#) **Edit NAT**

NAT Mode

NAT Mode SNAT DNAT Twice Nat

Basic Info

* Name

Enabled State Enable Disable

Description

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

Packet Before NAT

* Src. Security Zone

* Src. Address

* Dest. Security Zone

* Dest. Address

* Service

Packet After NAT

Src. Address Translated Address Pool Designated IP Outbound Interface Address

to

c Click **Save**.

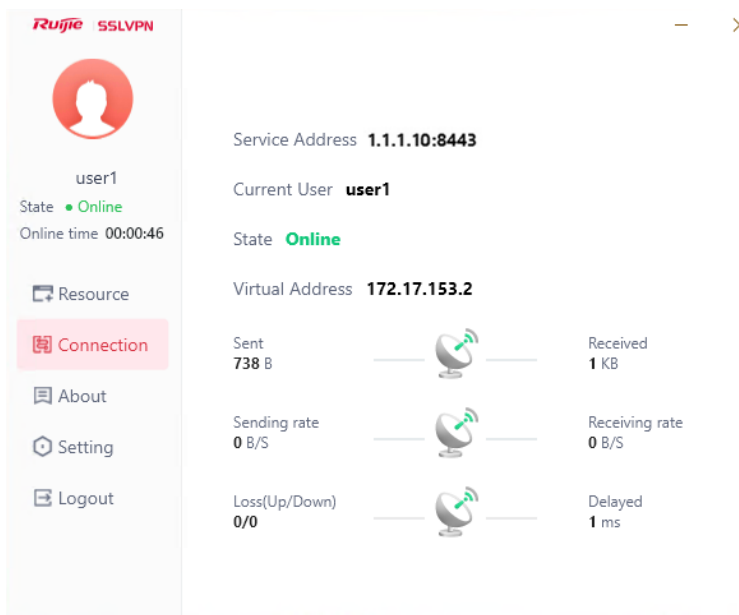
6. Verification

(1) Verifying the Result on the Client

- a Open the client, enter the configured public address of the SSL VPN gateway, username, and password, and click **Login**.



b After login succeeds, the client obtains the assigned virtual address.



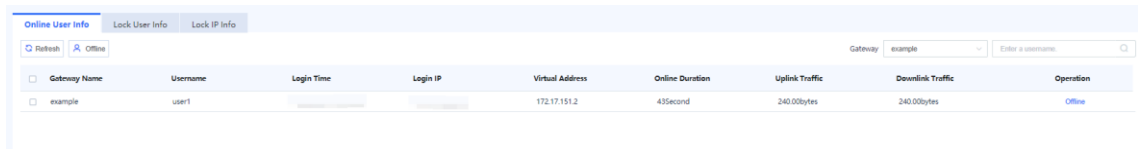
c Open a browser, and check whether intranet resources can be accessed by the client. The following figure uses a web server address as an example.



This is a web server

(2) Verifying the Result on the Device

- o Choose **Network > SSL VPN > Operation Monitoring** and check online user information. If there are multiple gateways, you can switch gateways in the upper right corner of the page to view online user information.



Gateway Name	Username	Login Time	Login IP	Virtual Address	Online Duration	Uplink Traffic	Downlink Traffic	Operation
example	user1			172.17.151.2	43Second	240.00bytes	240.00bytes	Online

- o Choose **Monitor > Log Monitoring > SSL VPN Log**. On the page that is displayed, check SSL VPN login logs.

8.24.6 Typical Configuration of SSL VPN Access Using a Domain Name over Multiple Lines (Local Authentication)

1. Applicable Products and Versions

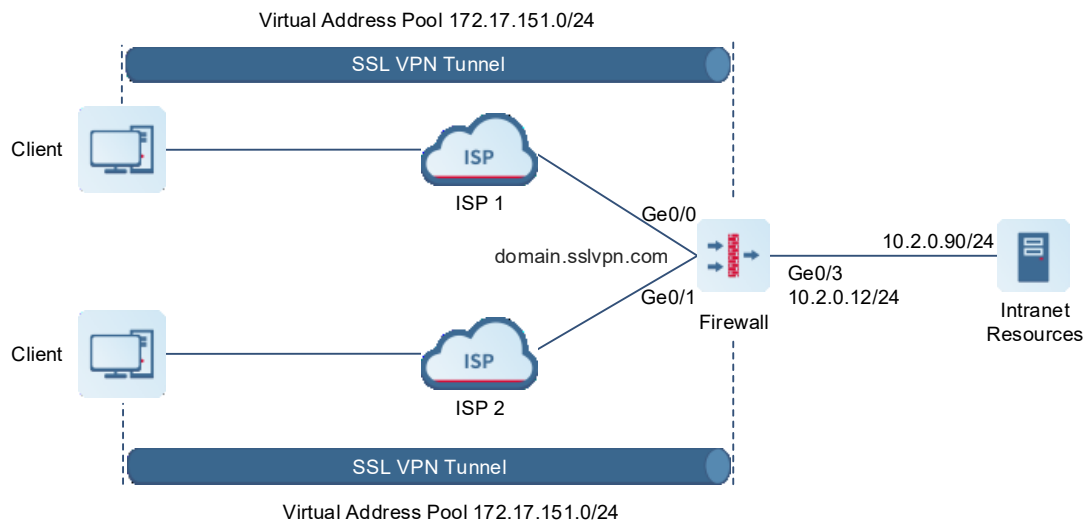
Table 8-24 Products and Versions

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS1.0R5 or later

2. Service Demands

The following figure shows an enterprise network. Cross-ISP communication affects the SSL VPN service experience. In actual deployment, multiple lines are recommended. The device is configured with multiple interfaces to access different ISPs, and remote office users use the domain name **domain.sslvpn.com** (example) for unified access. The enterprise authenticates remote office users based on local authentication on the firewall. Authenticated users can obtain access to the enterprise intranet.

The customer requests **user1** in user group **group1** in the default authentication domain to obtain an intranet address and access enterprise intranet resources like accessing resources on a LAN.



Item	Description	Remarks
Network interface	<ul style="list-style-type: none"> Interface: Ge0/0 (172.17.123.12), untrust Interface: Ge0/1 (172.17.124.12), untrust Interface: Ge0/3 (10.2.0.12), trust 	
SSL VPN gateway configuration	<ul style="list-style-type: none"> Interface 1: Ge0/0:8443 Interface 2: Ge0/1:8443 Domain name: domain.sslvpn.com 	

Authentication mode	Local authentication	
SSL VPN user	<ul style="list-style-type: none"> ● User group: group1 ● Username: user1 ● Password: test@123 	
Virtual address pool	172.17.151.0/24	Upon successful login, the client obtains an IP address from the virtual address pool. In the address pool, 172.17.151.1 is a device-side virtual address and is reserved.
Intranet resource subnet	10.2.0.0/24	Intranet resource subnet that can be accessed by the client.

3. Restrictions and Guidelines

- The subnets of the virtual address pool and firewall physical interface cannot be the same.
- If the SSL VPN gateway is configured with a domain name, its port numbers must be the same.
- If DNAT is required, verify that a DNAT policy has been configured on the DNAT device.
- Domain name resolution over the intranet is not supported. The intelligent domain name resolution service is provided by a domain name service provider.

4. Prerequisites

- Intranet resources have been configured and can be accessed through the firewall.
- The routes from intranet resources to the subnet 172.17.151.0/24 where the SSL VPN client address pool resides are reachable.
- Remote office users have installed RG-SSLVPN_Client_2.0.
- A domain name has been applied for and intelligent domain name resolution based on lines has been configured.

5. Procedure

(1) Configuring Interfaces and Security Zones

- a Log in to the firewall web UI, and choose **Network > Interface > Physical Interface**.
- b Click **Edit** in the **Operation** column of Ge0/0 to modify the configuration.
 - o Zone: **untrust**
 - o IP/Mask: **172.17.123.12/24**
 - o Next-Hop Address: Enter the actual address. In this example, **172.17.123.1**.
 - o Use the default configuration for the other parameters.

[Back](#) **Edit Physical Interface**

Basic Info

Interface Name

Description

Connection Status Enable Disable

Mode Routing Mode Transparent Mode Off-Path Mode

* Zone [Add Security Zone](#)

Interface Type WAN Interface LAN Interface

Address

IP Type IPv4 IPv6

Connection Type Static Address DHCP PPPoE

* IP/Mask

* Next-Hop Address

Default Route

Line Bandwidth

Uplink

Downlink

Access Management

Permit HTTPS PING SSH

Advanced

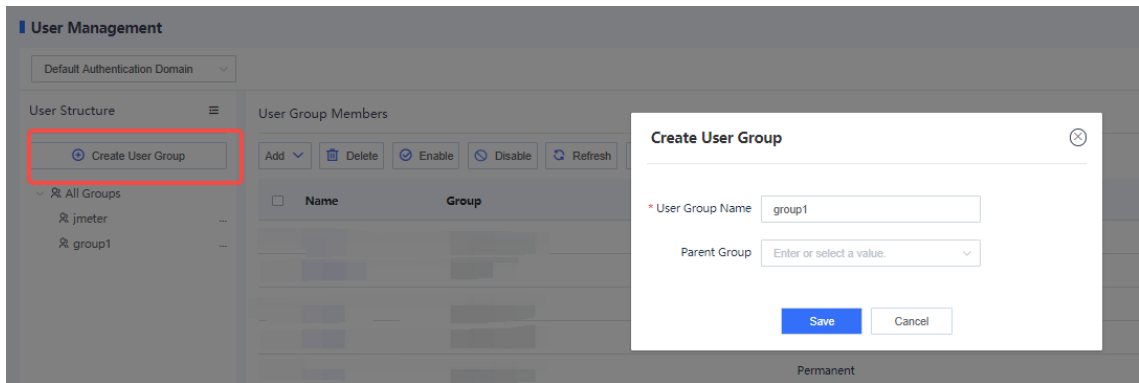
ISP Address Library

MTU

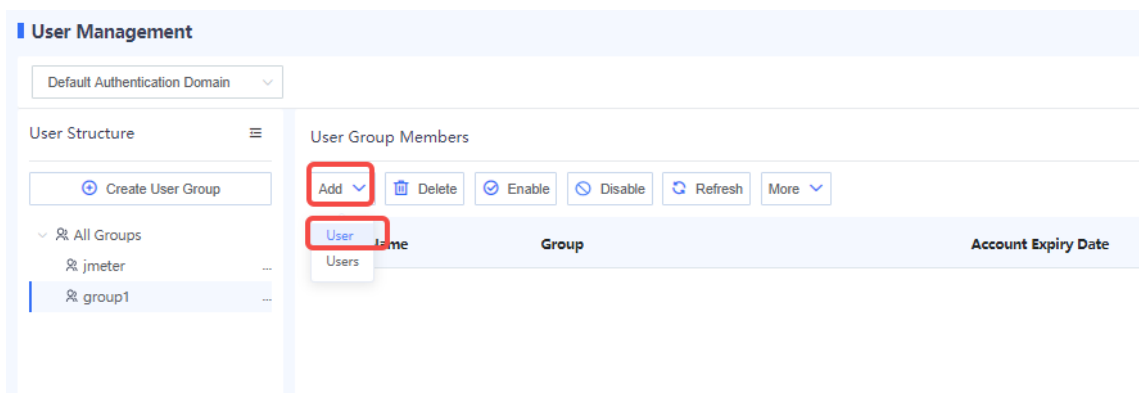
MA

Link Detection

- c Click **Save**.
 - d Configure Ge0/1 in a similar way. Set **Zone** to **untrust**, select **IPv4**, and set **IP/Mask** to **172.17.124.12/24**.
 - e Configure Ge0/3 in a similar way. Set **Zone** to **trust**, select **IPv4**, and set **IP/Mask** to **10.2.0.12/24**.
- (2) Configuring a User Group and Users
- a Choose **Object > User Authentication > User Management**.
 - b Click **Create User Group** to add a user group **group1**.



- c Click **Save**.
- d Click **Add** and choose **User**.



- e Configure user information as follows:
 - o Login Username: **user1**
 - o Parent Group: **/default/group1**
 - o Password: **test@123**

[< Back](#) **Add User**

Basic Info

* Login Username

Enabled State Enable Disable

Displayed Username

* Parent Group

Description

Password

* Password

* Confirm Password

[Advanced Settings](#)

f Click **Save**.

(3) Configuring a Gateway

a Perform Basic Configuration

Choose **Network > SSL VPN > SSL VPN Gateway**.

Click **Create** and create an SSL VPN gateway as follows:

- o Set gateway address 1 to **Ge0/0** and use the default port number 8443.
- o Set gateway address 2 to **Ge0/1** and use the default port number 8443.
- o Set the domain name to **domain.sslvpn.com**.
- o Configure **Max. Concurrent Users** according to the actual allowed authorized user number.
- o Use the default configuration for the other parameters.

The screenshot shows a configuration page with two main sections: **Basic Config** and **Advanced**. The **Basic Config** section includes:

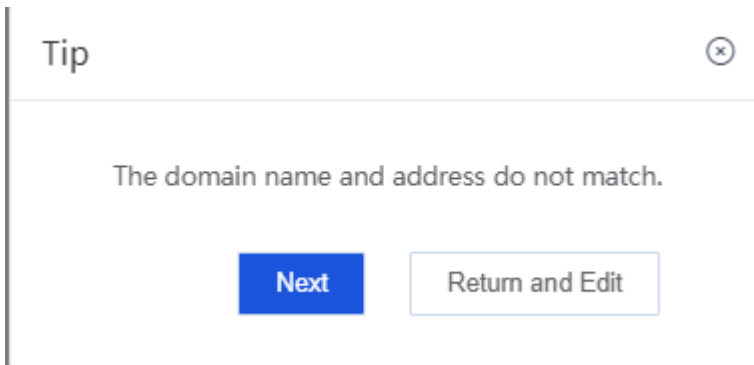
- Network Config**
 - * Gateway Name:
 - Gateway Type: Exclusive Shared
 - * Gateway Address: Two entries are shown. The first has interface `Ge0/0(On | 172.17.123.12/24)`, IP `172.17.123.12`, and Port Number `8443`. The second has interface `Ge0/1(On | 172.17.124.12/24)`, IP `172.17.124.12`, and Port Number `8443`. A `Delete` button is next to the second entry.
 -
 - Domain Name:
 - Intranet DNS:
 -
 - Preferred DNS: Intranet DNS Customer DNS

The **Advanced** section includes:

- Protocol**
 - * Protocol Version: TLS1.2 TLS1.1 TLS1.0
 - * Algorithm Suite: TLS-ECDHE-RSA-WITH-AES128-CBC-SHA256 TLS-ECDHE-RSA-WITH-AES256-CBC-SHA384 TLS-RSA-WITH-AES256-CBC-SHA
 - Gateway Certificate:
- Concurrency Control**
 - * :

Click **Next**.

If the configured domain name cannot be resolved by DNS into the corresponding address, the system displays the following prompt message. You can click **Next** to continue the configuration or choose to return to modify the configuration.



b Perform Authentication Configuration

The default authentication domain is used. Therefore, use the default configuration for parameters on this page.

[Back](#) **Add SSL VPN Gateway**

Basic Config **Login Control**

Authentication

* User Authentication Domain [Create User Authentication Domain](#)

Prevent Brute-Force Attack

User Lockout

* Max. User Attempts Time * Lockout Period Second

Single IP Lockout

* Max. Single IP Attempts Time * Lockout Period Second

Login Verification

Graphic Verification

* Enable upon Consecutive Input Errors

Hardware Signature Verification

* Maximum Signatures Bound to Each User

Auto Hardware Signature Approval

Auto User Unbinding

Auto Approval of Trusted Public Terminals

Idle Timeout

* The idle status will time out after minutes.

Client Version Control

Available Client Versions Any Version Latest Version on Secure Cloud Custom Config (The earliest version for clients on each platform can be specified.)

Click **Next**.

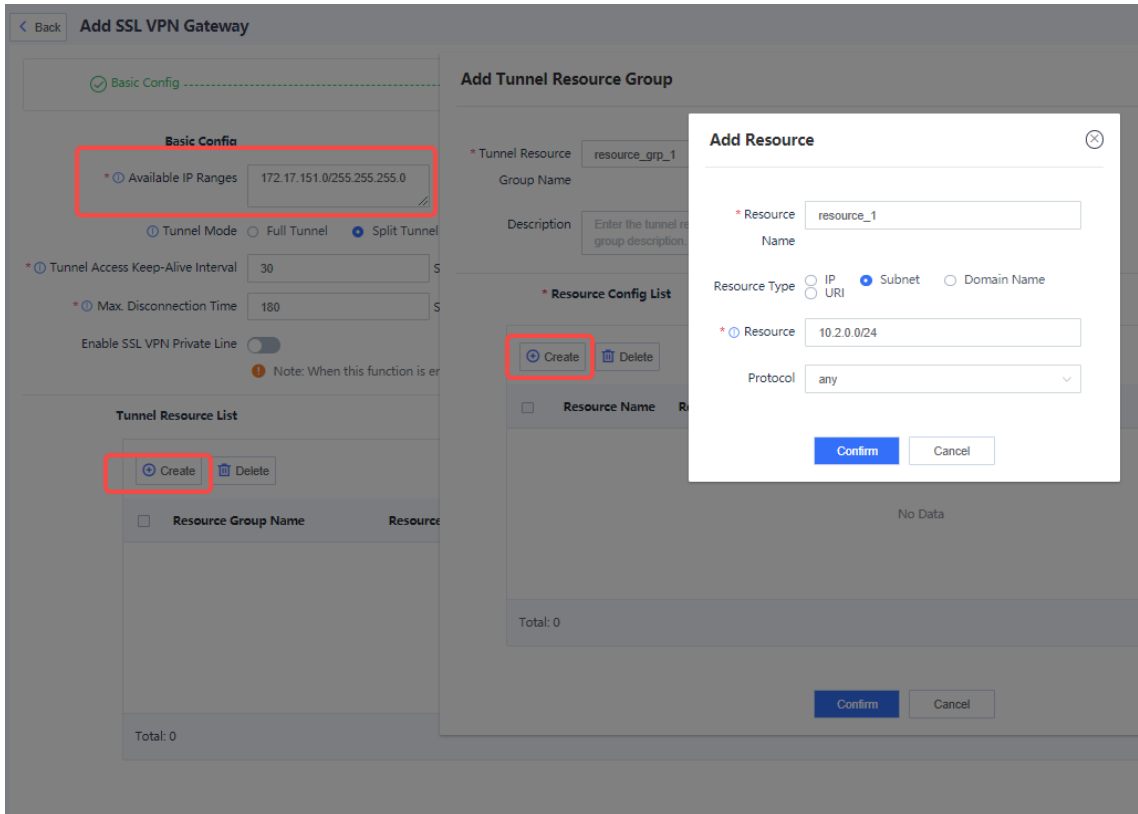
c Add Resources

Set **Available IP Ranges** to **172.17.151.0/255.255.255.0**.

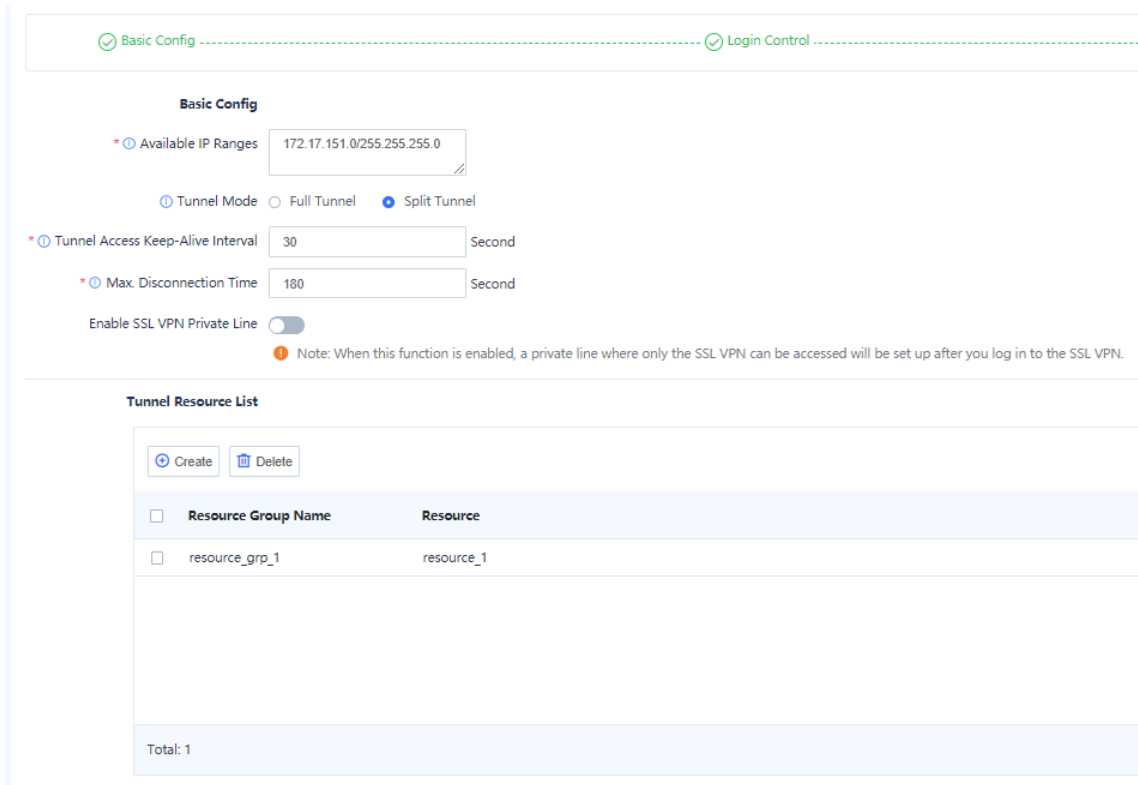
Use the default configuration for **Tunnel Access Keep-Alive Interval** and **Max. Disconnection Time**.

In the **Tunnel Resource List** area, click **Create** to create a tunnel resource group **resource_grp_1** and add a resource to the group:

- o Resource Name: **resource_1**
- o Resource Type: **Subnet**
- o Resource: **10.2.0.0/24**
- o Protocol: **any**



Click **Confirm** to create the resource. Then click **Confirm** to create the resource group, as shown in the following figure.



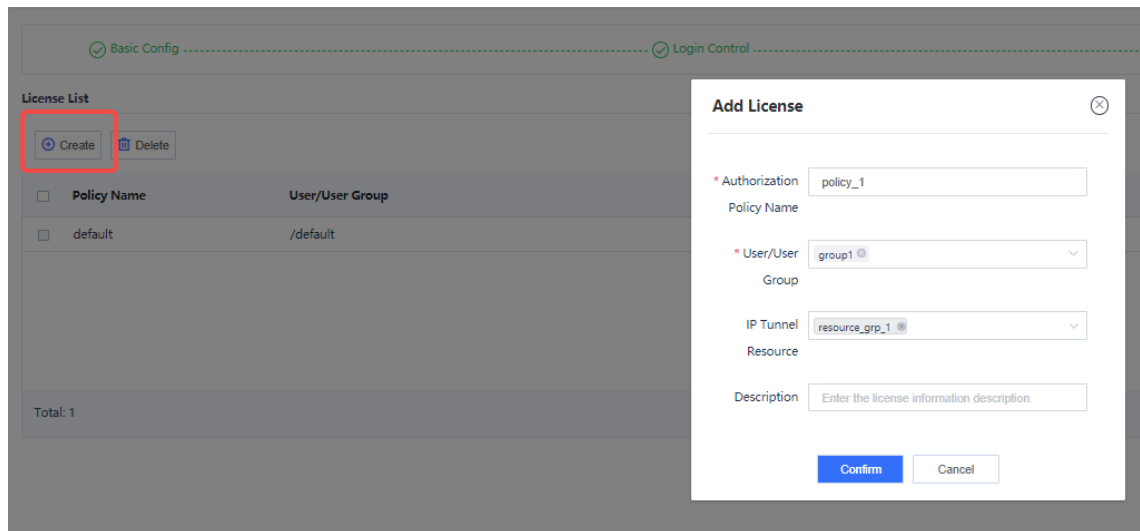
Click **Next**.

d Bind Resources

By default, the device provides a default policy. In this policy, the user/user group is fixed to the currently configured root authentication domain (**default** in this example) and cannot be edited. The default policy is not bound with any resources and cannot be deleted. You can choose to edit the default policy or directly create a policy. In this example, a new policy **policy_1** is created.

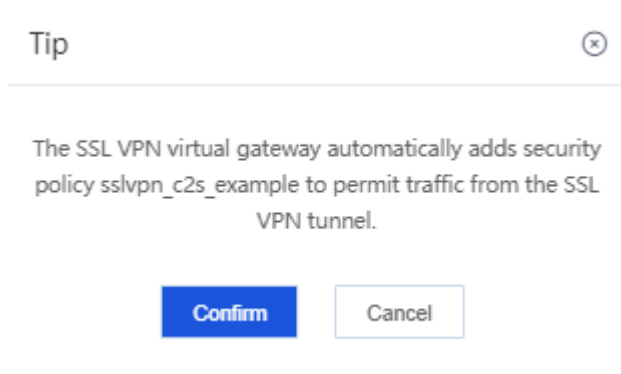
Click **Create** and create an authorization policy as follows:

- o Authorization Policy Name: **policy_1**
- o User/User Group: **group1**
- o IP Tunnel Resource: **resource_grp_1**



Click **Confirm** to save the authorization policy.

Click **Finish**. In the dialog box that is displayed, click **Confirm**.



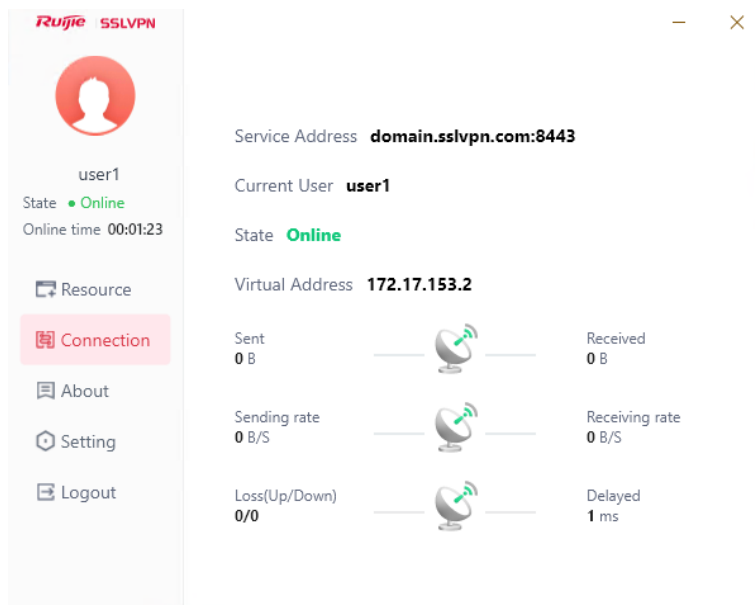
6. Verification

(1) Verifying the Result on the Client

- a Open the client, enter the configured domain name of the SSL VPN gateway, username, and password, and click **Login**.



b After login succeeds, the client obtains the assigned virtual address.



c Open a browser, and check whether intranet resources can be accessed by the client. The following figure uses a web server address as an example.



This is a web server

(2) Verifying the Result on the Device

- o Choose **Network > SSL VPN > Operation Monitoring** and check online user information. If there are multiple gateways, you can switch gateways in the upper right corner of the page to view online user

information.

Gateway Name	Username	Login Time	Login IP	Virtual Address	Online Duration	Uplink Traffic	Downlink Traffic	Operation
example	user1			172.17.151.2	435second	240.00bytes	240.00bytes	Offline

- o Choose **Monitor > Log Monitoring > SSL VPN Log**. On the page that is displayed, check SSL VPN login logs.

8.24.7 Typical Configuration of RADIUS Authentication Access

1. Applicable Products and Versions

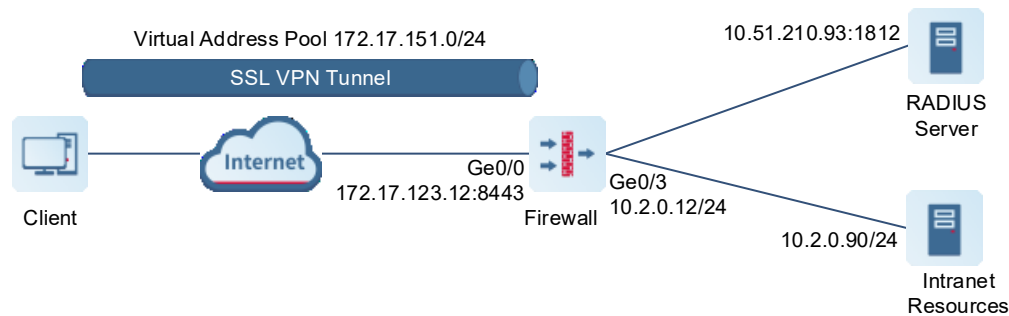
Table 8-25 Products and Versions

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS1.0R5 or later

2. Service Demands

An enterprise uses an external RADIUS server (Ruijie Networks RG-SMP security management platform in this example) to authenticate remote office users. Authenticated users can obtain access to the enterprise intranet.

The customer requests **user1** in the external authentication domain **smp** to obtain an intranet address and access enterprise intranet resources like accessing resources on a LAN.



Item	Description	Remarks
RADIUS server	<ul style="list-style-type: none"> Server address: 10.51.210.93 Authentication port: 1812 Accounting port: 1813 	In this example, Ruijie Networks RG-SMP security management platform provides the authentication service.
Network interface	<ul style="list-style-type: none"> Interface: Ge0/0 (172.17.123.12), untrust Interface: Ge0/3 (10.2.0.12), trust 	
SSL VPN gateway configuration	Interface: Ge0/0:8443	
Authentication mode	External authentication	
RADIUS user	<ul style="list-style-type: none"> Username: user1 Password: test@123 	

Virtual address pool	172.17.151.0/24	Upon successful login, the client obtains an IP address from the virtual address pool. In the address pool, 172.17.151.1 is a device-side virtual address and is reserved.
Intranet resource subnet	10.2.0.0/24	Intranet resource subnet that can be accessed by the client.

3. Restrictions and Guidelines

- The subnets of the virtual address pool and firewall physical interface cannot be the same.

4. Prerequisites

- Intranet resources have been configured and can be accessed through the firewall.
- The routes from intranet resources to the subnet 172.17.151.0/24 where the SSL VPN client address pool resides are reachable.
- Remote office users have installed RG-SSLVPN_Client_2.0.
- The RADIUS server has been configured and can be accessed.
- The authentication information on **uesr1** has been configured on the RADIUS server.

5. Procedure

(1) Configuring Interfaces and Security Zones

- a Log in to the firewall web UI, and choose **Network > Interface > Physical Interface**.
- b Click **Edit** in the **Operation** column of Ge0/0 to modify the configuration.
 - o Zone: **untrust**
 - o IP/Mask: **172.17.123.12/24**
 - o Next-Hop Address: Enter the actual address. In this example, **172.17.123.1**.
 - o Use the default configuration for the other parameters.

Edit Physical Interface

Basic Info

Interface Name: Ge0/0

Description:

Connection Status: Enable Disable

Mode: Routing Mode Transparent Mode Off-Path Mode

* Zone: untrust

Interface Type: WAN Interface LAN Interface

Address

IP Type: IPv4 IPv6

Connection Type: Static Address DHCP PPPoE

* IP/Mask: 172.17.123.12/24

* Next-Hop Address: 172.17.123.1

Default Route:

Line Bandwidth

Uplink:

Downlink:

Access Management

Permit: HTTPS PING SSH

Advanced

ISP Address Library:

MTU: 1500

MA:

Link Detection:

- c Click **Save**.
 - d Configure Ge0/3 in a similar way. Set **Zone** to **trust**, select **IPv4**, and set **IP/Mask** to **10.2.0.12/24**.
- (2) Configuring an Authentication Server and Authentication Domain
- a Configure a RADIUS Server
- Choose **Object** > **User Authentication** > **Authentication Server**.
- Click **Create** and configure an authentication server according to the following figure.

Basic Info

* Server Name

* Shared Password

* Active Authentication Server IP Authentication Port Accounting Port Tx Interface

Standby Authentication Server IP Authentication Port Accounting Port Tx Interface

Advanced Settings

Retransmission Times

Unit

Response Timeout

Enable Active Detection

Click **Save**.

b Configure an Authentication Domain

Choose **Object > User Authentication > Authentication Domain**.

Click **Create** and configure an authentication domain according to the following figure.

- o Scenario: Enable services as required. In this example, only **SSL VPN Access** is enabled.
- o Authentication Server: Select the server **smp** created in the previous step.
- o Domain Name Removal: If this function is disabled, the firewall sends both the username and domain name to the authentication server. In this example, the login username is **user1** and the authentication domain is **smp**. If the domain name is not removed, the username received by the authentication server is **user1@smp**. If the domain name is removed, the username received by the authentication server is **user1**. In this example, the username configured on the RADIUS server is **user1** (without a domain name). Therefore, **Domain Name Removal** needs to be toggled on. Enable or disable this function as required.

Basic Info

* Name

Enabled State Enable Disable

Description

*** Scenario**

SSL VPN Access User Location Authentication Server

WEBAUTH

Advanced Settings

Domain Name Removal

Default Online User
Group

After completing the configuration, click **Save**.

(3) Configuring a Gateway

a Perform Basic Configuration

Choose **Network > SSL VPN > SSL VPN Gateway**.

Click **Create** and create an SSL VPN gateway as follows:

- o Set the gateway address to **Ge0/0** and use the default port number **8443**.
- o Configure **Max. Concurrent Users** according to the actual allowed authorized user number.
- o Use the default configuration for the other parameters.

[Back](#) **Add SSL VPN Gateway**

Basic Config Login Control

Network Config

* Gateway Name

Gateway Type Exclusive Shared

* Gateway Address Port Number

Domain Name

Intranet DNS

Preferred DNS Intranet DNS Customer DNS

Protocol

* Protocol Version TLS1.2 TLS1.1 TLS1.0

* Algorithm Suite TLS-ECDHE-RSA-WITH-AES128-CBC-SHA256 TLS-ECDHE-RSA-WITH-AES256-CBC-SHA384 TLS-RSA-WITH-AES256-CBC-SHA

Gateway Certificate

Concurrency Control

* Max. Concurrent Users

Click **Next**.

b Perform Authentication Configuration

Set **User Authentication Domain** to the authentication domain **smp** configured in the previous step, and use the default configuration for the other parameters.

Basic Config Login Control

Authentication

* ⓘ User Authentication Domain ⓘ Create User Authentication Domain

Prevent Brute-Force Attack

User Lockout

* ⓘ Max. User Attempts Time * ⓘ Lockout Period Second

Single IP Lockout

* ⓘ Max. Single IP Attempts Time * ⓘ Lockout Period Second

Login Verification

ⓘ Graphic Verification

* ⓘ Enable upon Consecutive Input Errors

ⓘ Hardware Signature Verification

* ⓘ Maximum Signatures Bound to Each User

ⓘ Auto Hardware Signature Approval

ⓘ Auto User Unbinding

ⓘ Auto Approval of Trusted Public Terminals

Idle Timeout

* ⓘ The idle status will time out after minutes.

Click **Next**.

i Note

If the authentication domain of an existing gateway is modified, the system displays the following prompt message. Click **Confirm** to continue with the configuration.

Tip



Resources bound to the authentication domain will be reset. Are you sure you want to modify the authentication domain?

Confirm

Cancel

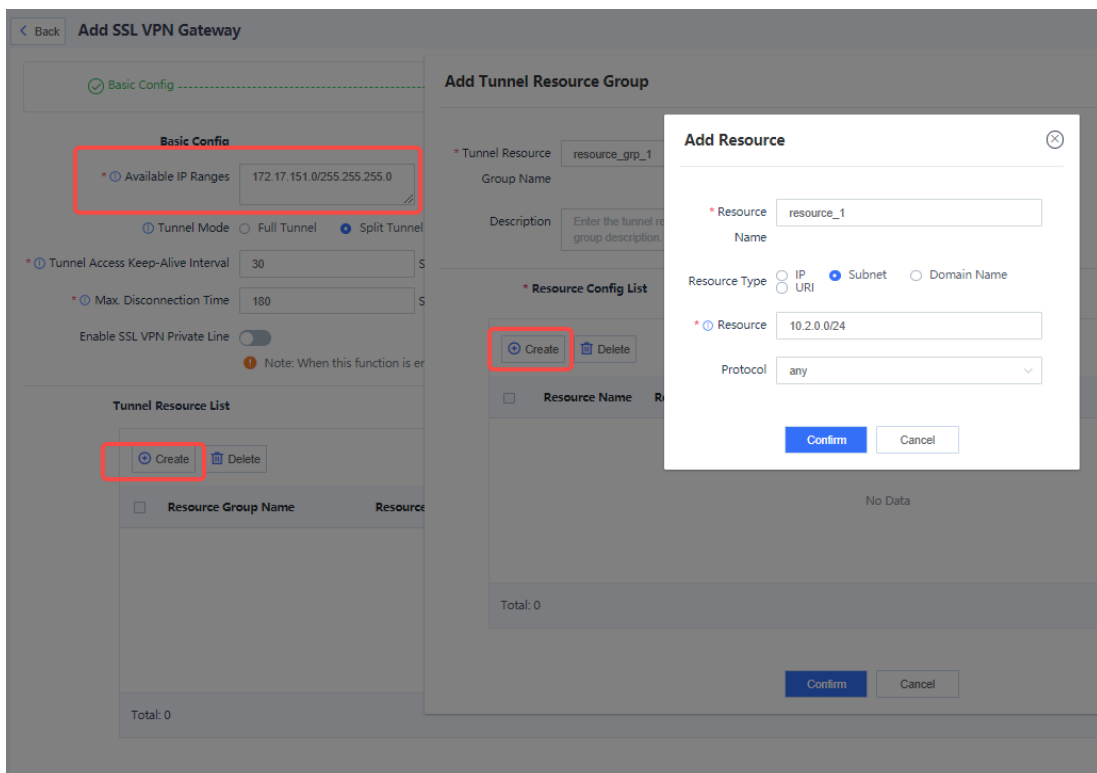
c Add Resources

Set **Available IP Ranges** to **172.17.151.0/255.255.255.0**.

Use the default configuration for **Tunnel Access Keep-Alive Interval** and **Max. Disconnection Time**.

In the **Tunnel Resource List** area, click **Create** to create a tunnel resource group **resource_grp_1** and add a resource to the group:

- o Resource Name: **resource_1**
- o Resource Type: **Subnet**
- o Resource: **10.2.0.0/24**
- o Protocol: **any**



Click **Confirm** to create the resource. Then click **Confirm** to create the resource group, as shown in the following figure.

The screenshot displays a configuration page for VPN settings. At the top, there are two tabs: 'Basic Config' (active) and 'Login Control'. Under 'Basic Config', the following settings are visible:

- Available IP Ranges:** 172.17.151.0/255.255.255.0
- Tunnel Mode:** Radio buttons for Full Tunnel and Split Tunnel (selected).
- Tunnel Access Keep-Alive Interval:** 30 Second
- Max. Disconnection Time:** 180 Second
- Enable SSL VPN Private Line:** A toggle switch is currently turned off.

A note below the toggle switch states: "Note: When this function is enabled, a private line where only the SSL VPN can be accessed will be set up after you log in to the SSL VPN."

The 'Tunnel Resource List' section contains a table with the following data:

<input type="checkbox"/>	Resource Group Name	Resource
<input type="checkbox"/>	resource_grp_1	resource_1

At the bottom of the table, it indicates 'Total: 1'. Above the table, there are 'Create' and 'Delete' buttons.

Click **Next**.

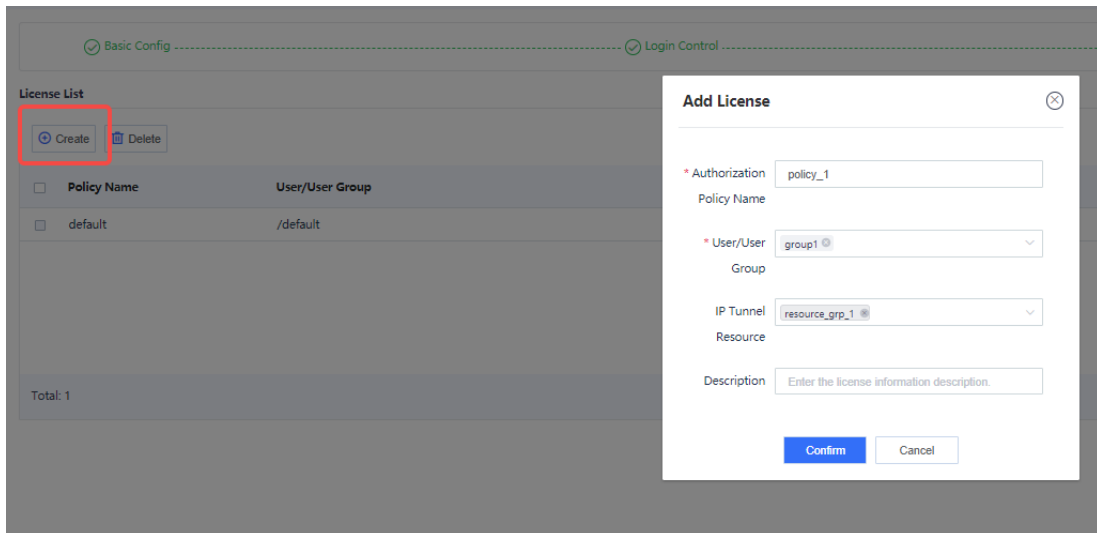
d Bind Resources

By default, the device provides a default policy. In this policy, the user/user group is fixed to the currently configured root authentication domain (**smp** in this example) and cannot be edited. The default policy is not bound with any resources and cannot be deleted. You can choose to edit the default policy or directly create a policy. In this example, a new policy **policy_1** is created.

If an existing gateway is edited and the authentication domain is modified, the previously configured authorization policy is cleared, and a new authorization policy needs to be configured.

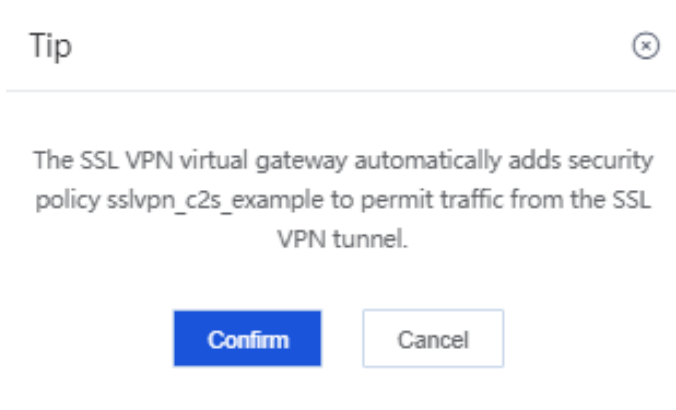
Click **Create** and create an authorization policy as follows:

- o Authorization Policy Name: **policy_1**
- o User/User Group: **group1**
- o IP Tunnel Resource: **resource_grp_1**



Click **Confirm** to save the authorization policy.

Click **Finish**. In the dialog box that is displayed, click **Confirm**.



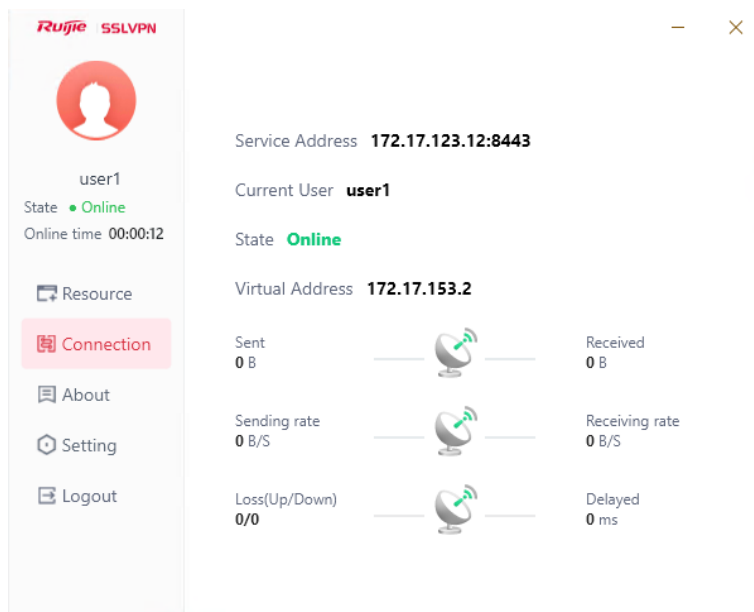
6. Verification

(1) Verifying the Result on the Client

- a Open the client, enter the configured the SSL VPN gateway address, username, and password, and click **Login**.



b After login succeeds, the client obtains the assigned virtual address.



c Open a browser, and check whether intranet resources can be accessed by the client. The following figure uses a web server address as an example.

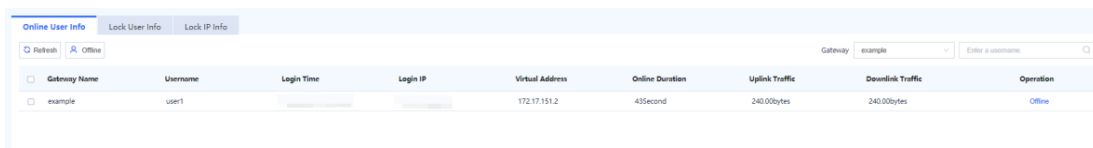


This is a web server

(2) Verifying the Result on the Device

- o Choose **Network > SSL VPN > Operation Monitoring** and check online user information. If there are multiple gateways, you can switch gateways in the upper right corner of the page to view online user

information.



- o Choose **Monitor > Log Monitoring > SSL VPN Log**. On the page that is displayed, check SSL VPN login logs.

(3) Verifying the Result on the RADIUS Server

Log in to the RG-SMP security management platform to view online user information.

8.24.8 Typical Configuration of SMS Two-Factor Authentication (Twilio)

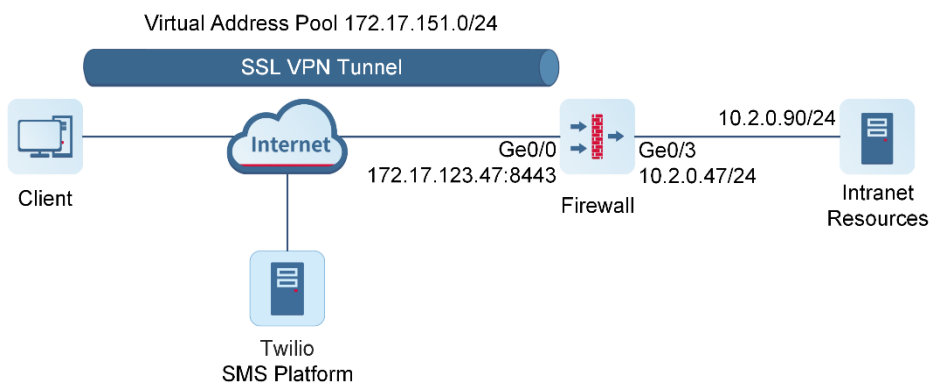
1. Applicable Products and Version

Table 8-26 Products and Versions

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS1.0R8 or later

2. Service Demands

As shown in the figure, the enterprise uses the SSL VPN function of the firewall to provide a secure access tunnel for remote office users to access intranet resources. Access users are authenticated by local authentication and SMS verification code. Only authenticated employees can access the enterprise intranet.



Item	Description	Remarks
Network interface	<ul style="list-style-type: none"> Interface: Ge0/0 (172.17.123.47), untrust Interface: Ge0/3 (10.2.0.47), trust 	
SSL VPN gateway configuration	Interface: Ge0/0 (172.17.123.47:8443)	

Item	Description	Remarks
Authentication mode	Local authentication	
SSL VPN user	<ul style="list-style-type: none"> ● User group: group1 ● Username: user1 ● Password: test@123 ● Mobile number: 187xxx9590 	In this example, the mobile number is hidden. During actual configuration, configure a valid mobile number.
SMS authentication server	Service provider: Twilio	Detailed server parameters are provided by the Twilio SMS service.
Virtual address pool	172.17.151.0/24	Upon successful login, the client obtains an IP address from the virtual address pool. In the address pool, 172.17.151.1 is a device-side virtual address and is reserved.
Intranet resource subnet	10.2.0.0/24	Intranet resource subnet that can be accessed by the client.

3. Restrictions and Guidelines

- The subnets of the virtual address pool and firewall physical interface cannot be the same.
- The mobile number must be valid.

4. Prerequisites

- 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.
- The firewall can access the Twilio SMS platform.
- Intranet resources can be accessed through the firewall.
- Remote office users have installed RG-SSLVPN_Client_2.0.2.

5. Procedure

(1) Configuring Interfaces and Security Zones

- a Log in to the firewall web UI, and choose **Network > Interface > Physical Interface**.
- b Click **Edit** in the **Operation** column of Ge0/0 to modify the configuration.

Zone: **untrust**

IP/Mask: **172.17.123.47/26**

Next-Hop Address: Enter the actual address. In this example, **172.17.123.1**.

Use the default configuration for the other parameters.

[Back](#) **Edit Physical Interface**

Basic Info

Interface Name

Description

Connection Status Enable Disable

Mode Routing Mode Transparent Mode Off-Path Mode

* Zone [Add Security Zone](#)

Interface Type WAN Interface LAN Interface

Address

IP Type IPv4 IPv6

Connection Type Static Address DHCP PPPoE

* IP/Mask

* Next-Hop Address

Default Route

Line Bandwidth

Uplink

Downlink

Line Bandwidth

Uplink

Downlink

Access Management

Permit HTTPS PING SSH

Advanced

ISP Address Library

MTU

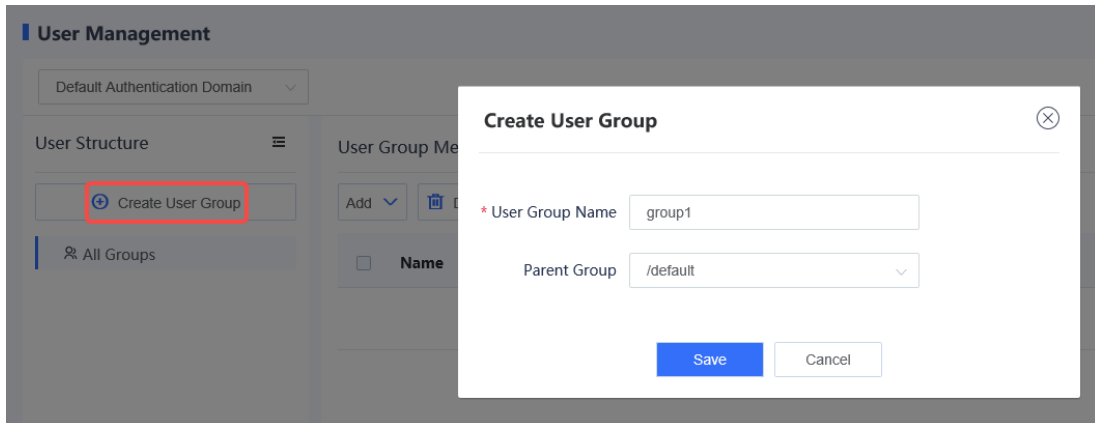
MAC

Link Detection

Reverse Path Limited

c Click **Save**.

- d Configure G0/3 in a similar way. Set **Zone** to **trust**, select **IPv4**, and set **IP/Mask** to **10.2.0.47/24**.
- (2) Configuring a User Group and Users
- a Choose **Object > User Authentication > User Management**.
 - b Click **Create User Group** to add a user group **group1**.



- c Click **Save**.
- d Configure user information as follows:
Login Username: **user1**
Parent Group: **/default/group1**
Password: **test@123**
Mobile Number: **187xxx9590**. Enter a valid mobile number for receiving an SMS verification code.

[< Back](#) **Add User**

Basic Info

* Login Username

Enabled State Enable Disable

Displayed Username

* Parent Group

Description

Mobile Number

Mobile Number

Password

* Password

* Confirm Password

[⌵ Advanced Settings](#)

- e Click **Save**.
- (3) Configuring an SMS Authentication Server
- a Choose **Object > User Authentication > Authentication Server > SMS Authentication Server**.
 - b Click **Create**.
 - c Configure parameters based on the account information provided by the Twilio SMS platform.

< Back **Create SMS Authentication Server**

SMS Provider Alibaba Cloud ⓘ Twilio ⓘ

* Server Name

* Account SID

* Authentication Token

* ⓘ Sender Mobile Number

* ⓘ SMS Template

ⓘ Test Mobile Number

i Note

You are advised to enter a test mobile number, click **Send Test Message**, and check whether the SMS server is available.

d Click **Save**.

(4) Configuring an SSL VPN Gateway

a Perform Basic Configuration

Choose **Network > SSL VPN > SSL VPN Gateway**.

Click **Create** and create an SSL VPN gateway as follows:

Set the gateway address to **Ge0/0** and use the default port number **8443**. If a port conflict occurs, change the port.

Configure **Max. Concurrent Users** as required. In this example, the value 10 is set.

Use the default configuration for the other parameters.

< Back
Add SSL VPN Gateway
Login Control Add Resource

Basic Config

Network Config

* Gateway Name

Gateway Type Exclusive Shared

* Gateway Address Port Number

[Create](#)

Domain Name

Intranet DNS

[Create](#)

Preferred DNS Intranet DNS Customer DNS

Advanced

Protocol

* Protocol Version TLS1.2 TLS1.1 TLS1.0

* Algorithm Suite TLS-ECDHE-RSA-WITH-AES128-CBC-SHA256 TLS-ECDHE-RSA-WITH-AES256-CBC-SHA384 TLS-RSA-WITH-AES256-CBC-SHA

Gateway Certificate

Concurrency Control

* Max. Concurrent Users

- Click **Next**.
- b Configure Login Control
 - Set **User Authentication Domain** to **default**.
 - Enable SMS two-factor authentication.
 - Toggle on **SMS Two-Factor Authentication** to enable this function.
 - Set **SMS Authentication Server** to the configured Twilio SMS platform.
 - Use the default configuration for the other parameters, as shown in the following figure.

[Back](#) **Add SSL VPN Gateway**

Basic Config
 Login Control
 Add Resource

Authentication

* User Authentication Domain: default [Create User Authentication Domain](#)

SMS Two-Factor Authentication:

* SMS Authentication Server: Twilio [Add SMS Authentication Server](#)

SMS-based Manual Binding:

SMS-based Manual Unbinding:

Manual Mobile Number Submission:

SMS Sending Limit: 0

Prevent Brute-Force Attack

User Lockout:

* Max. User Attempts: 5 Time * Lockout Period: 300 Second

Single IP Lockout:

* Max. Single IP Attempts: 5 Time * Lockout Period: 300 Second

Login Verification

Graphic Verification:

* Enable upon: 0 Consecutive Input Errors

Hardware Signature Verification:

* Maximum Signatures Bound to Each User: 3

Auto Hardware Signature Approval:

Auto User Unbinding:

Auto Approval of Trusted Public Terminals:

Idle Timeout

* The idle status will time out after: 30 minutes.

Client Version Control

Available Client Versions: Any Version Latest Version on Secure Cloud Custom Config (The earliest version for clients on each platform can be specified.)

Click **Next**.

c Add Resources

Set **Available IP Ranges** to **172.17.151.0/255.255.255.0**.

Use the default configuration for **Tunnel Access Keep-Alive Interval** and **Max. Disconnection Time**.

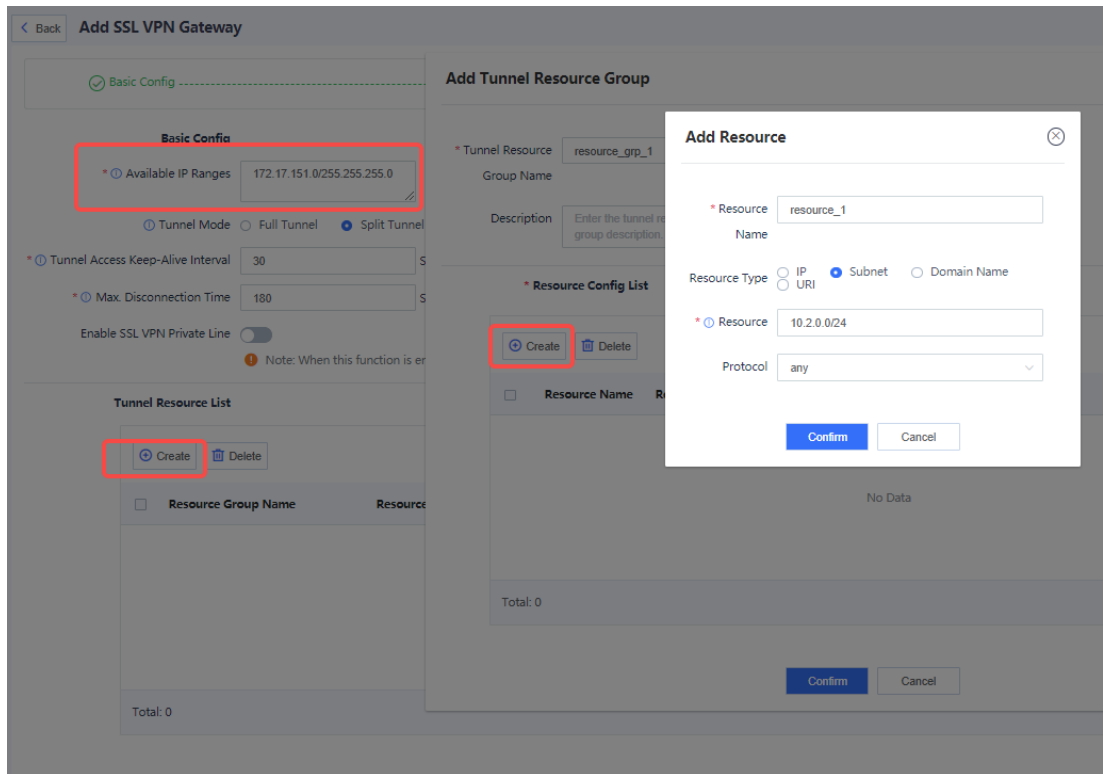
In the **Tunnel Resource List** area, click **Create** to create a tunnel resource group **resource_grp_1** and add a resource to the group:

Resource Name: **resource_1**

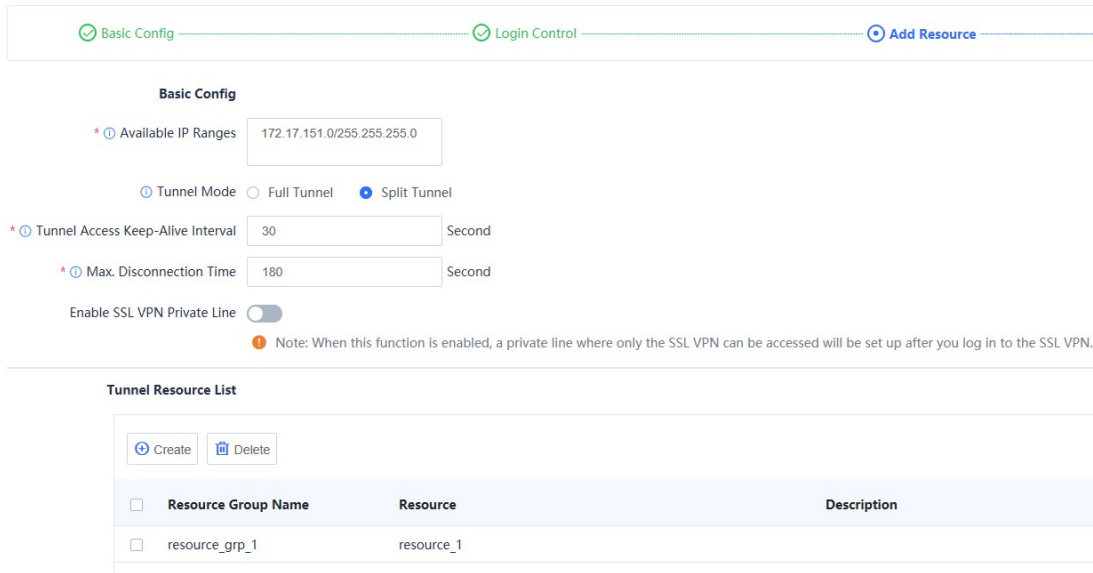
Resource Type: **Subnet**

Resource: **10.2.0.0/24**

Protocol: **any**



Click **Confirm** to create the resource. Then click **Confirm** to create the resource group, as shown in the following figure.



Click **Next**.

d Bind Resources

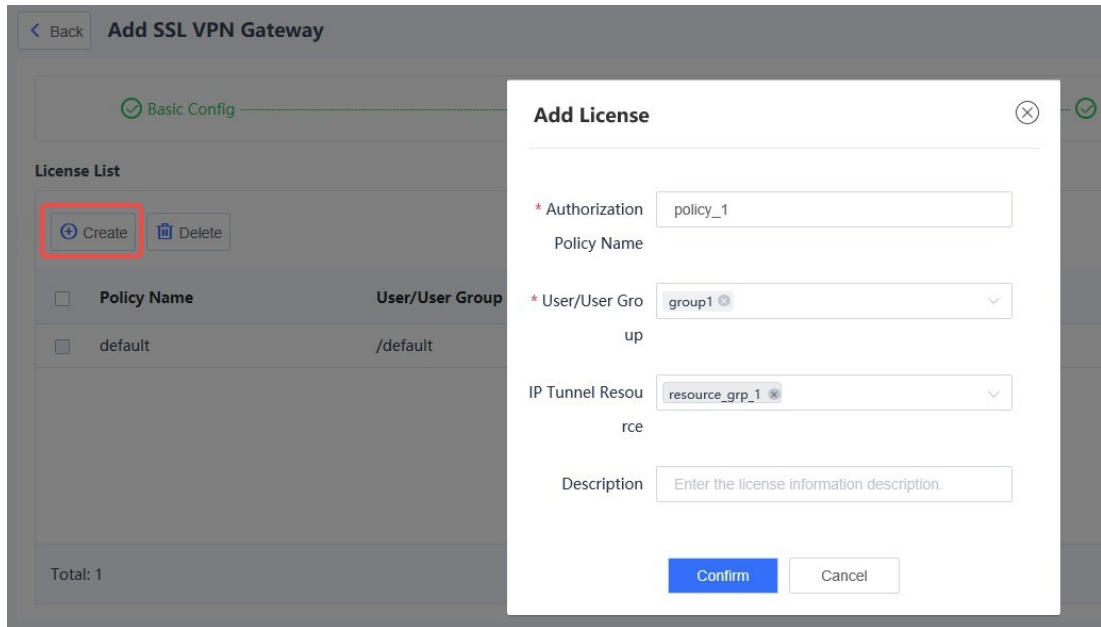
By default, the device provides a default policy. In this policy, the user/user group is fixed to the currently configured root authentication domain (**default** in this example) and cannot be edited. The default policy is not bound with any resources and cannot be deleted. You can choose to edit the default policy or directly create a policy. In this example, **policy_1** is created.

Click **Create** to create an authorization policy as follows:

Authorization Policy Name: **policy_1**

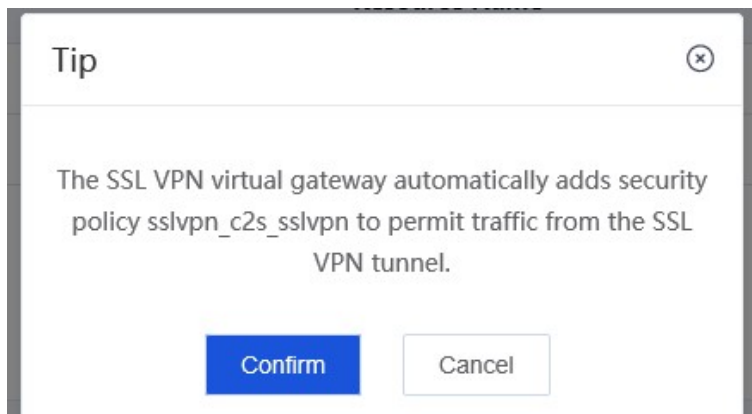
User/User Group: **group1**

IP Tunnel Resource: **resource_grp_1**



Click **Confirm** to save the authorization policy.

Click **Finish**. In the dialog box that is displayed, click **Confirm**.

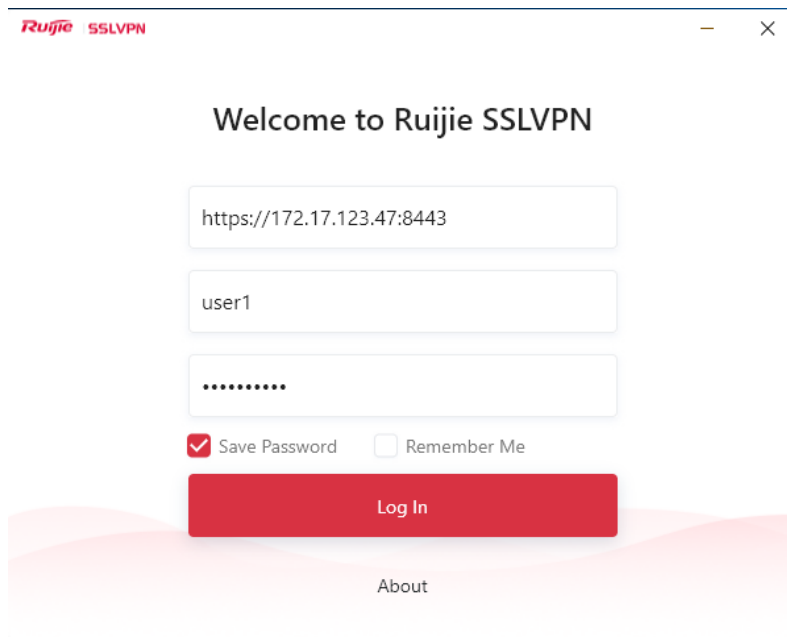


6. Verification

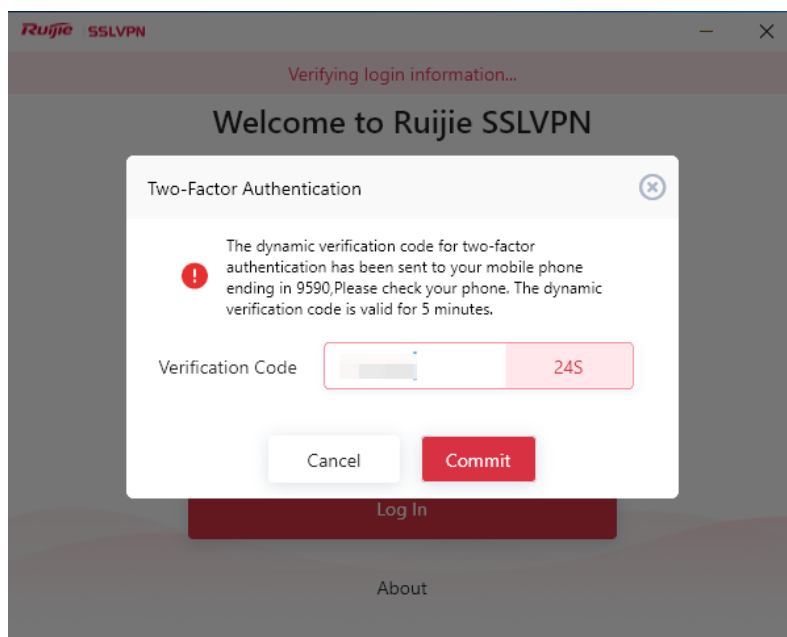
- Verifying Client Login Authentication

(1) Open the SSL VPN client and enter the gateway access information as follows:

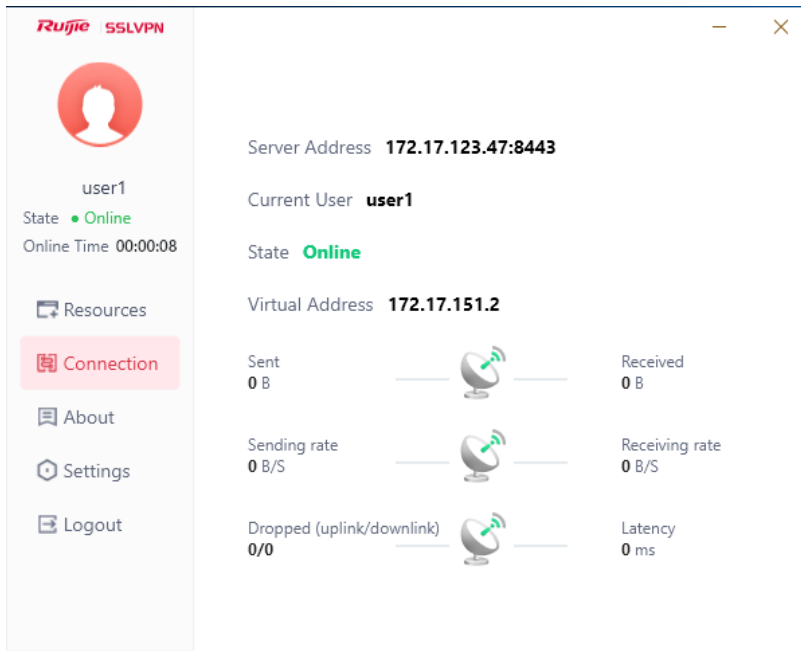
- Server Address: https://172.17.123.47:8443
- Username: **user1**
- Password: **test@123**



- (2) Click **Log In**. The system displays a message indicating that the verification code for SMS two-factor authentication has been sent.



- (3) Enter the received SMS verification code and click **Commit**.
- (4) After login, choose **Connection** and check whether the client obtains a virtual address.



- (5) Check whether the client can access intranet resources on the browser. In this example, a web server is accessed successfully.



This is a web server

- Verifying Device Authentication

- (1) Choose **Network > SSL VPN > Operation Monitoring** and view information about online users. If there are multiple gateways, select the current gateway in the upper right corner of the page to view online user information on this gateway.

Gateway Name	Username	Login Time	Login IP	Virtual Address	Online Duration	Uplink Traffic	Downlink Traffic	Operation
sslvpn	user1			172.17.151.2	2Minute1Second	0.00bytes	0.00bytes	Offline

- (2) Choose **Monitor > Log Monitoring > SSL VPN Log** and view SSL VPN login logs.

Time	Severity	Username	Gateway	IP	Details
	Tip	user1	sslvpn		User [user1] enables the tunnel access service (tunnel IP [172.17.151.2]).
	Tip	user1	sslvpn		Login succeeded.

8.24.9 Common Faults and Troubleshooting Roadmaps

1. Overview

Common SSL VPN faults include the following. Typically, troubleshooting needs to be performed on both the client and device sides.

- Client login fails.
- Client login succeeds but service access fails.

(1) Client Side

For details about troubleshooting on the client, see *RG-SSLVPN_Client_2.0.1_User Manual (V1.0)*. The typical troubleshooting roadmap is as follows:

- a Collect client logs.
- b Log in to the client and obtain packets on the client.
- c Check the client environment.
- d Check whether resources are correctly configured.

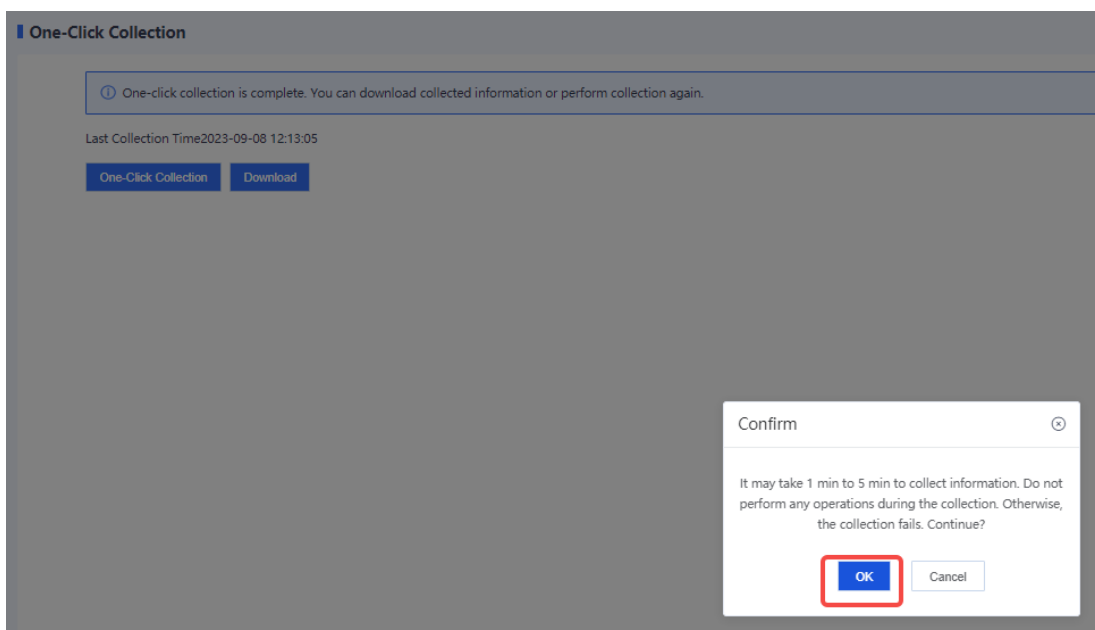
(2) Device Side

On the device side, perform troubleshooting using the one-click log collection and diagnostic center functions.

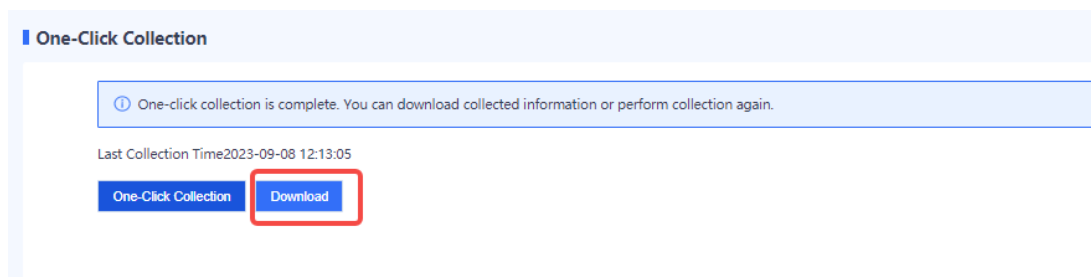
- a One-Click Log Collection

Choose **System > Fault Diagnosis > One-Click Collection**.

Click **One-Click Collection**. In the dialog box that is displayed, click **OK**. Wait 3 to 5 minutes for the information collection to complete, and download the log package.



Click **Download** and wait for the log download. After download is completed, send the log package to Ruijie technical support for analysis and processing.



b Diagnostic Center

Choose **System > Fault Diagnosis > Diagnostic Center**. Use the packet tracing function to track the packet life cycle and check whether packets are discarded by the device due to specific causes, which results in network disconnection.

2. Client Login Failure

(1) Common Causes on the Client Side and Solutions

The following table lists the causes of and solutions to SSL VPN client connection failures. For details about troubleshooting methods, see Chapter 7 of *Ruijie RG-SSLVPN Client 2.0.1 User Manual*.

Table 8-27 Description of SSL VPN Connection Failure Messages

Error Message	Description	Solution
Server certificate verification failed.	No valid certificate has been imported for the server.	You can choose to ignore the prompt and continue the login.
Hardware signature verification failed.	The hardware signature submitted by the device failed to be verified on the server.	Click Login again to submit a signature.
Login error. The server does not return the status code. Error code: 200.	The server returns an unknown error code.	Check whether the server version is supported.
Invalid server address.	The input server address is invalid.	Contact the network administrator to check whether the server address is correct. SSL VPN server address. The formats are as follows: Server IP address and port number: https://IP address:Port number Server domain name, for example, https://www.example.com
Failed to initialize the NIC.	A vNIC exception is detected during the login.	Exit the client program and uninstall the vNIC. Then, restart the client program to reinstall the vNIC.

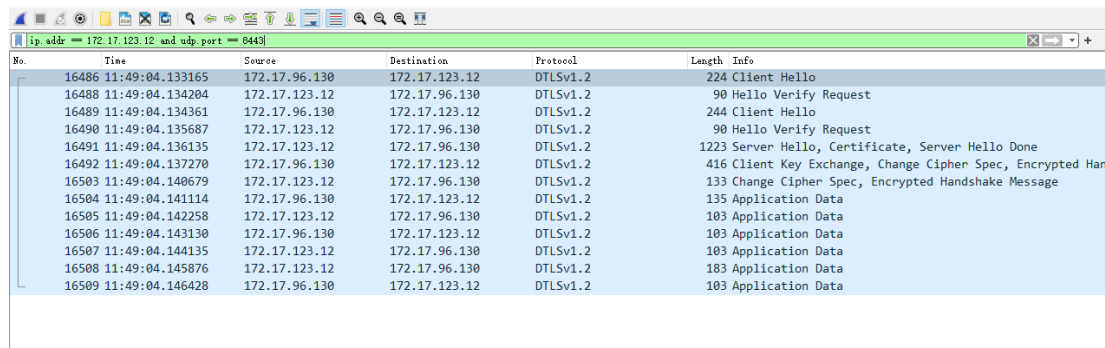
Failed to parse the server address.	The input server address cannot be resolved to an IP address.	<ul style="list-style-type: none"> ● Check the input server address and contact the network administrator to check whether the server address is correct. ● Check the network connection status of the device to ensure that the server address can be resolved properly.
Server connection timeout.	The device cannot set up a connection with the server at the input server address.	Check the network connection status to ensure that the device can set up a connection with a port on the server.
No network connection. Please check and log in again.	Network disconnection occurs on the device.	Check the local network connection status of the device to ensure that the device can set up a connection with a port on the server.
Tunnel initialization error.	The client cannot complete negotiation with the server through an SSL VPN tunnel.	Log in again, or restart the client program and log in again.
Unknown error.	The login response returned by the server has a data error.	Check whether the server version is supported by the client program.

(2) Common Causes on the Server Side and Solutions

Error Message on the Client	Description	Solution
NIC configuration failed (networking fault).	DNAT configuration may be incorrect.	Check whether networking configuration is correct

Handle the NIC configuration failure (networking fault) as follows:

Obtain packets on the client. Select the local NIC, and set the filter criteria to **ip.addr == Gateway address && udp.port == Gateway port**, as shown in the following figure.



In a normal login process, all the packets should be ciphertext packets using DTLS. If any plaintext packets using UDP are identified, a networking problem such as incorrect DNAT configuration exists.

For other issues, send the log package of one-click log collection to Ruijie technical support for analysis and processing.

3. Service Access Failure

(1) Common Causes on the Client Side and Solutions

The following uses the Windows system as an example. Run the command prompt on the client PC and enter the **route print** command.

Check whether routes to intranet resources are available:

- The values of **Network Destination** and **Netmask** are the same as the resource subnet configured on the firewall (**10.2.0.0/24** in this example).
- The value of **Gateway** is the same as the first address configured for **Available IP Ranges** (virtual address pool).
- The value of **Interface** is the same as the virtual address assigned to the client.

If the values of the preceding fields are inconsistent with those configured on the firewall, use troubleshooting methods for the client side. For details, see *Ruijie RG-SSLVPN Client 2.0.1 User Manual*.

(2) Common Causes on the Server Side and Solutions

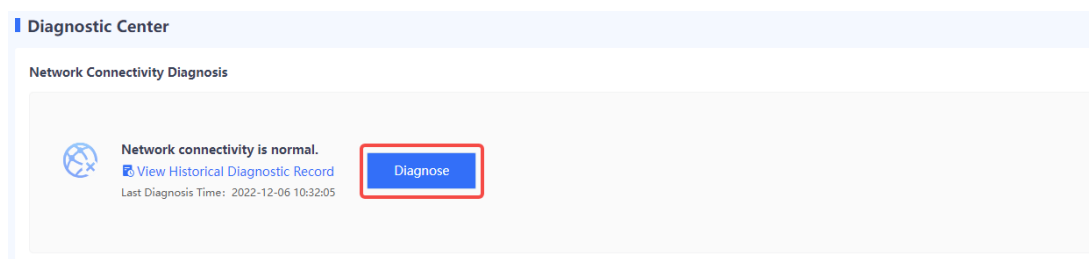
Possible Cause	Check Method	Solution
Resource configuration is incorrect or the resources are not bound with users.	Check the resource and resource binding configurations of the gateway.	Reconfigure and authorize corresponding users and their accessible resources.
The intranet host is unreachable.	Perform packet tracing.	Check the configuration to ensure that the device can access intranet resources.
Security policies do not permit traffic.	Perform packet tracing. (For details, see the following example.)	Modify security policies.

For other issues, send the log package of one-click log collection to Ruijie technical support for analysis and processing.

If security policies do not permit traffic and incur service exceptions, handle the issue as follows:

In this example, a security policy blocks the ICMP protocol and intranet resources cannot be pinged.

- a Choose **System > Fault Diagnosis > Diagnostic Center**, and click **Diagnose**.



- b On the page that is displayed, set **Src. Address** to the actual address of the client (**172.17.96.130** in this example), set the protocol to **UDP** (do not select **ICMP**), and click **Diagnose**.

Network Connectivity Diagnosis

Diagnostic Parameter Settings

The diagnostic parameters will be used throughout the diagnostic process, covering basic configuration detection, packet tracing, and traffic forwarding detection.
Note: You are advised to minimize the range to achieve a better diagnostic result. If the diagnostic range is too large, only 1000 flows will be collected.

* Src. Address: 172.17.96.130 Src. Port: Enter the Src. Port number.

Dest. Address: Enter the destination address. Dest. Port: Enter the Dest. Port number.

Inbound Interface: Select * Protocol: UDP

Src. MAC: Example: d8:9e:f3:3f:d5:64 Dest. MAC: Example: d8:9e:f3:3f:d5:64

Diagnose

- c Continuously ping intranet resources during the collection period.

Network Connectivity Diagnosis

Fault Diagnosis Tracing

Traffic Receiving Detection: ✔ Basic Config Detection: ✔ Packet Tracing: ✘ Traffic Forwarding Detection: ⚪

Diagnostic Result:

The following 6 errors have been found. Please handle them according to suggestions.

Diagnostic Content: Failed to send packets

Only packets that fail to be sent are displayed.

udp 172.17.96.130 56434 <-> 172.17.123.12 8443

Packet 1

Inbound Interface: Ge0/0 Src. Address: 172.17.96.130 Dest. Address: 172.17.123.12 Protocol: udp Src. Port: 56434 Dest. Port: 8443

Diagnostic Result: Packet is discarded.

Cause: Security Policy. Packet is discarded. Policy name: test

Legend: Pass (Green), Discard (Red), Ignore (Grey), Not checked (Blue), Pause (Yellow), Block (Black)

Flow Diagram: Packet marking on physical interfaces → Link layer packet parsing → Network layer packet parsing → Single packet attack detection → Session search → Session search → Whether a session is matched (Pass) → Security defense (Discard) → Security defense (first packet check) → Session creation → DNAT policy matching → Whether to match security policies → Security policy remaining → Whether to create → Session state check → Security policy remaining

Troubleshoot

- d Click **Troubleshoot** to access the **Security Policy** page. On the page that is displayed, check which policy was hit and caused packet discard.

Security Policy

Security Policy: Packet is discarded. Policy name: test

Policy Group: Add Policy Group

Operations: Create, Delete, Enable, Disable, Refresh, More

Priority	Name	Type	Src. Security Zone	Src. Address	User/User Group	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count	Hit Session	Operation
1	test	-	any	any	any	any	any	ping	any	any	Deny		12	Clear	View Details Edit Delete
2	skript_2...	IPv4	untrust	any	spooof_gw	any	any	res_gw	any	any	Permit		839	Clear	View Details Edit Delete
3	s1	-	any	any	any	any	any	any	any	any	Permit		43	Clear	View Details Edit Delete
4	Default Pol...	-	any	any	any	any	any	any	any	any	Deny		0	Clear	View Details Edit Delete

- e Modify the matching rule of the corresponding security policy to permit the packets.

8.25 IPsec VPN

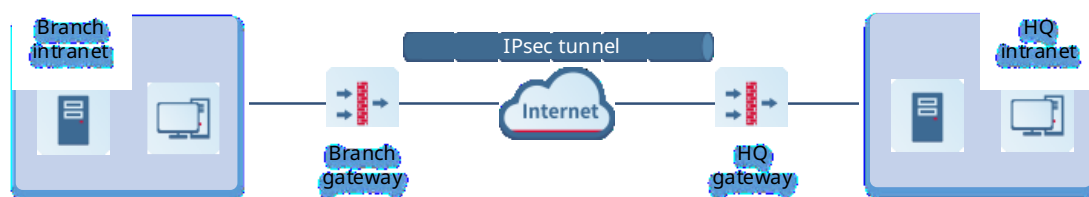
8.25.1 Overview

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

IPsec VPN is typically used to set up secure interconnection between an enterprise HQ and branch. After an IPsec tunnel is established between the HQ gateway and branch gateway, data can be securely transferred between the HQ and branch, and intranet resources can be shared.

In addition, IPsec VPN supports active/standby switchover. In an HQ-branch scenario, an active tunnel and a standby tunnel can be established between the HQ and branch. When the active tunnel fails, the standby tunnel takes over traffic, thereby ensuring stable transmission.

Figure 8-19 Typical Application Scenario of IPsec VPN



8.25.2 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.

i 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.

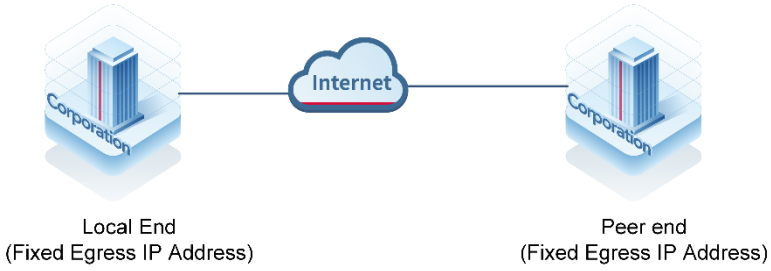
8.25.3 Application Scenario

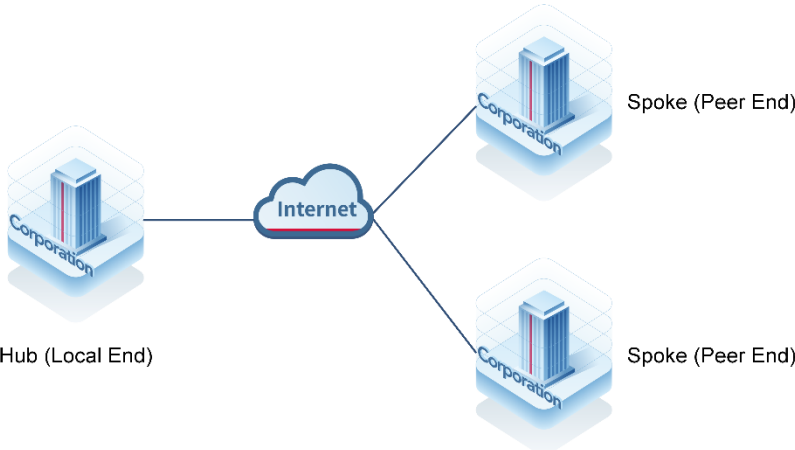
Internet Protocol Security (IPsec) is a protocol suite for establishing secure connections over public networks. The objective of IPsec is to provide security services for network layer traffic in IPv4 and IPv6 formats. Typically,

IPsec is used to provide Virtual Private Network (VPN) services between two sites or between remote users and enterprise networks.

IPsec is an open protocol suite consisting of multiple protocols, including security protocols Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE), as well as authentication and encryption algorithms. The AH and ESP protocols provide security services, and the IKE protocol enables key exchange.

IPsec VPN applies to the following scenarios.

Scenario	Description
Point-to-Point	<p>The peer device has a fixed IP address, and the local device is typically located at one end of a tunnel or a spoke site on a hub-spoke network.</p>  <p>Local End (Fixed Egress IP Address)</p> <p>Peer end (Fixed Egress IP Address)</p> <p>Key configurations:</p> <ul style="list-style-type: none"> ● Configure the address or domain name of the peer. ● Configure interesting traffic that is symmetric to that of the peer. ● Configure the same pre-shared key as that of the peer. ● Configure the same IKE and IPsec parameters as those of the peer. ● Select IKE main mode or IKE aggressive mode for negotiation.

Point-to-Multipoint	<p>The peer device does not have a fixed IP address, and the local device is typically a hub site on a hub-spoke network.</p>  <p>Key configurations:</p> <ul style="list-style-type: none"> ● Configure any-to-any interesting traffic. ● Enable IPsec Reverse Route Injection (RRI). ● Select IKE auto mode for negotiation.
---------------------	---

8.25.4 Configuration Examples of Site-to-Site IPsec VPN

1. Applicable Products and Versions

Table 8-28 Products and Versions

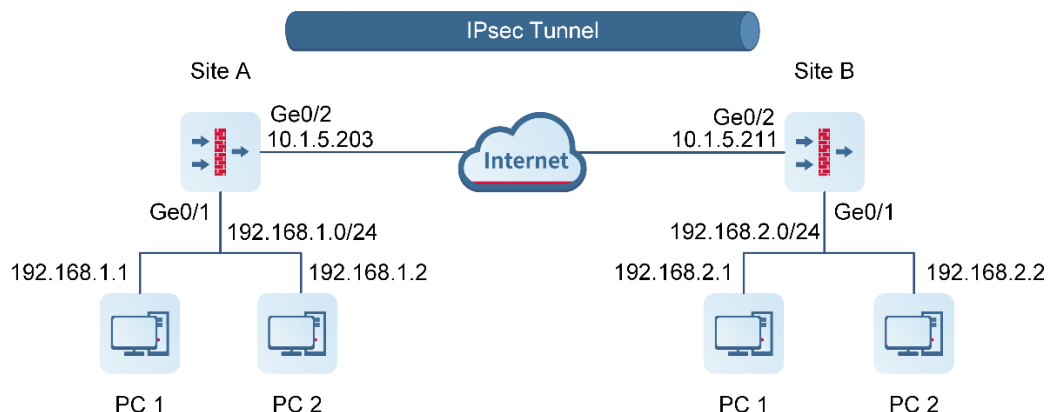
Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R6 or later

2. Service Demands

As shown in [Figure 8-20](#), Site A and Site B at both ends have fixed public IP addresses. A point-to-point IPsec VPN tunnel needs to be established between the LANs of the two sites to achieve secure mutual access.

The authentication mode should be pre-shared key, and the encapsulation mode should be the tunnel mode. In this way, both ends can initiate connections.

Figure 8-20 Point-to-Point Networking



3. Restrictions and Guidelines

- Currently, the RG-WALL 1600-Z series firewall supports only the IPsec IKEv1 protocol for pre-shared key authentication and ESP tunnel mode for encapsulation.

4. Prerequisites

You have completed basic network configurations for Site A and Site B, including interface IP addresses and default routes. Pay attention to the following point during configuration:

- Ensure that the IP addresses of Site A and Site B are fixed.

5. Using a Configuration Wizard

- Configuring Site A

(1) Perform basic configuration.

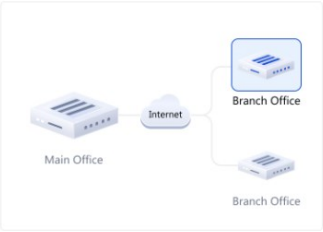
- Choose **Network > IPsec VPN > Config Wizard**. The basic configuration page of the configuration wizard is displayed.
- Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.

① Basic Config ② Authentication Config ③ Interesting Traffic Config ④ Config Verification

* ① Tunnel Interface

* Tunnel Name

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



- c After completing the configuration, click **Next**.
- (2) Configure authentication.
 - a Configure parameters according to the following figure.

① Basic Config ② Authentication Config ③ Interesting Traffic Config ④ Config Verification

* Peer Address

* Outbound Interface

* Authentication Mode Pre-shared Key

* Key

* Confirm Key

- b After completing the configuration, click **Next**.
- (3) Configure interesting traffic.
 - a Click **Create**. Configure parameters for interesting traffic according to the following figure.

Basic Config Authentication Config **Interesting Traffic Config** Config Verification ④

<input type="checkbox"/>	Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/>	Subnet-to-Sub...	192.168.1.0/24	192.168.2.0/24	Edit Delete

/ Page Total:1 Go to < 1 >

- b After completing the configuration, click **Next**.
- (4) Verify configuration.
 - a After verifying the configuration, click **Finish**.

✓ Basic Config ✓ Authentication Config ✓ Interesting Traffic Config 4 Config Verification

will be added to the custom tunnel list.

Basic Config [Edit](#)

Tunnel Interface: vti1

Tunnel Name: Site-to-Site

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

Authentication Config [Edit](#)

Peer Address: 10.15.211

Outbound Interface: Ge0/2

Authentication Mode: Pre-shared Key

Key:

Interesting Traffic Config [Edit](#)

Local Network	Peer Network
192.168.1.0/24	192.168.2.0/24

Advanced Settings [Expand](#)

- Configuring Site B

- (1) Perform basic configuration.

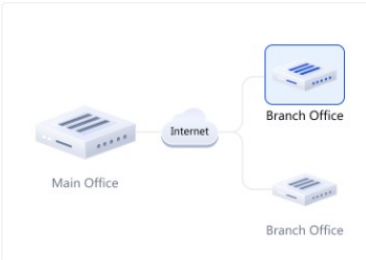
- Choose **Network > IPsec VPN > Config Wizard**. The basic configuration page of the configuration wizard is displayed.
- Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.

① **Basic Config** ② Authentication Config ③ Interesting Traffic Config ④ Config Verification

* ⓘ Tunnel Interface vti 1

* Tunnel Name Site-to-Site

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



Cancel Next

- c After completing the configuration, click **Next**.
- (2) Configure authentication.
- a Configure parameters according to the following figure.

Basic Config **Authentication Config** Interesting Traffic Config Config Verification

* Peer Address

* Outbound Interface

* Authentication Mode Pre-shared Key

* Key

* Confirm Key

- b After completing the configuration, click **Next**.
- (3) Configure interesting traffic.
 - a Click **Create**. Configure parameters for interesting traffic according to the following figure.

Basic Config Authentication Config **Interesting Traffic Config** Config Verification

<input type="checkbox"/>	Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/>	Subnet-to-Sub...	192.168.2.0/24	192.168.1.0/24	Edit Delete

10 ▾ / Page Total:1 Go to

- b After completing the configuration, click **Next**.
- (4) Verify configuration.
 - a After verifying the configuration, click **Finish**.

✓ ✓ ✓ ④
 Basic Config Authentication Config Interesting Traffic Config **Config Verification**

be added to the custom tunnel list.

Basic Config [Edit](#)

Tunnel Interface

Tunnel Name

Scenario Point-to-Point ⓘ Point-to-Multipoint ⓘ

Authentication Config [Edit](#)

Peer Address

Outbound Interface

Authentication Mode Pre-shared Key

Key

Interesting Traffic Config [Edit](#)

Local Network	Peer Network
192.168.2.0/24	192.168.1.0/24

Advanced Settings [Expand](#)

6. Manually Configuring a Tunnel

- Configuring Site A

(1) Configure a tunnel interface.

- a Choose **Network > Interface > Tunnel Interface**.
- b On the page that is displayed, click **Create**.
- c On the tunnel interface configuration page that is displayed, configure parameters as follows:
 - o Set **Interface Name** to vti1.
 - o Add security zone VPN-Zone and set **Security Zone** to **VPN-Zone** for this interface.
 - o Set **Tunnel Local Address** to the default outbound interface address of Site A: 10.1.5.203.
 - o Set **Tunnel Remote Address** to the default outbound interface address of Site B: 10.1.5.211.

< Back **Create Tunnel Interface Details**

* Interface Name

Security Zone [+ Add Security Zone](#)

* Tunnel Local Address

Tunnel Remote Address IP Dynamic

Description

(2) Configure an IPsec tunnel.

a Perform basic configuration.

Choose **Network > IPsec VPN > Custom Tunnel**. Click **Create**. On the basic configuration page of the custom tunnel, configure parameters as follows:

- o Set **Tunnel Name** to **Site-to-Site**.
- o Set **Enabled State** to **Enable**.
- o Set **Tunnel Interface** to **vti1**. Set **Local Address** to interface Ge0/2, and **Peer Address** to 10.1.5.211.
- o For **Authentication Mode**, use the default value **Pre-shared Key**. Set both **Key** and **Confirm Key** to **ruijie123**.

① ————— ② ————— ③

Basic Config Interesting Traffic Config Security Parameter Config

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

* Tunnel Name

Description

* Enabled State Enable Disable

* Tunnel Interface ⓘ Add Tunnel Interface

* Authentication Mode

* Key

* Confirm Key

* Local Address Interface ⓘ IP ⓘ

* Peer Address

* Local ID Type

Verify Peer ID

☰ **Advanced**

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

b Configure interesting traffic.

On the interesting traffic configuration page, click **Create**. Then configure parameters as follows:

- o Set **Proxy Mode** to **Subnet-to-Subnet**.
- o Set **Local Network** to 192.168.1.0/24 and **Peer Network** to 192.168.2.0/24.

✓ ————— ② ————— ③

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

ⓘ

<input type="checkbox"/>	Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/>	Subnet-to-Sub...	192.168.1.0/24	192.168.2.0/24	Edit Delete

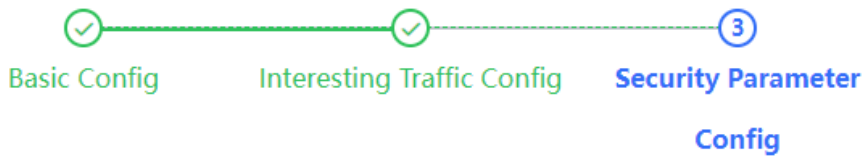
10 ▾ / Page Total:1 Go to < >

After completing the configuration for interesting traffic, click **Next**.

c. Configure security parameters.

On the security parameter configuration page, configure IKE and IPsec parameters and ensure that the configuration matches that on the peer device.

- o IKE parameters: Set **Negotiation Mode** to **IKEv1 Main Mode**, **Encryption Algorithm** to **AES-128**, **Verification Algorithm** to **SHA**, **DH Group** to **GROUP5**, and **SA Lifetime** to 86400 (in seconds).
- o IPsec parameters: Set **Protocol** to **ESP**, **Encapsulation Mode** to **Tunnel**, **Encryption Algorithm** to **AES-128**, and **Verification Algorithm** to **SHA**. Do not toggle on **Perfect Forward Secrecy**. Set **SA Lifetime** to 3600 (in seconds) and **Tunnel MTU** to 1400.



IKE Parameter

* Negotiation Mode

* Encryption Algorithm

* Verification Algorithm

* DH Group

* SA Lifetime Second

IPsec Parameter

* Protocol

* Encapsulation Mode

* Encryption Algorithm

* Verification Algorithm

Perfect Forward Secrecy

* SA Lifetime Second

Previous
Cancel
Finish

Click **Finish** to complete the configuration for the IPsec tunnel.

(3) Create security policies.

- a Choose **Object > Address > IPv4 Address**. On the page that is displayed, click **Create** and create two address objects for local network 192.168.1.0/24 and peer network 192.168.2.0/24 of the interesting traffic separately.

IPv4 Address			
	IPv6 Address	IPv4 Address Group	IPv6 Address Group
<input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/>			
<input type="checkbox"/>	Name	IP Address/Range	Address Group
<input type="checkbox"/>	VPN-remotesubnet	192.168.2.0/24	-
<input type="checkbox"/>	VPN-localsubnet	192.168.1.0/24	-

- b Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, click **Create** and create outbound security policy **VPN-outbound** and inbound security policy **VPN-inbound** separately.

< Back

Edit Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group ⊕ Add Group

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

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

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

(4) Configure a static route.

- a Choose **Network > Routing > Static Routing > IPv4**.
- b Click **Create** and create a static route to the peer protected subnet of the VPN.

< Back

Edit Static Routing

IP Type IPv4

* Dest. IP Range/Mask

Next-Hop Address

Interface

* ❗ Priority

Link Detection

Description

- Configuring Site B

- (1) Configure a tunnel interface.

- a Choose **Network > Interface > Tunnel Interface**.
- b On the page that is displayed, click **Create**.
- c On the tunnel interface configuration page that is displayed, configure parameters as follows:
 - Set **Interface Name** to **vti1**.
 - Add security zone VPN-Zone and set **Security Zone** to **VPN-Zone** for this interface.
 - Set **Tunnel Local Address** to the default outbound interface address of Site B: 10.1.5.211.
 - Set **Tunnel Remote Address** to the default outbound interface address of Site A: 10.1.5.203.

< Back

Edit Tunnel Interface Details

* Interface Name

Security Zone ⊕ Add Security Zone

* Tunnel Local Address

Tunnel Remote Address IP Dynamic

Description

- (2) Configure an IPsec tunnel.

- a Perform basic configuration.

Choose **Network > IPsec VPN > Custom Tunnel**. Click **Create**. On the basic configuration page of the custom tunnel, configure parameters as follows:

- Set **Tunnel Name** to **Site-to-Site**.
- Set **Enabled State** to **Enable**.
- Set **Tunnel Interface** to **vti1**. Set **Local Address** to interface Ge0/2, and **Peer Address** to 10.1.5.203.
- For **Authentication Mode**, use the default value **Pre-shared Key**. Set both **Key** and **Confirm Key** to **ruijie123**.

① Basic Config ② Interesting Traffic Config ③ Security Parameter Config

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

* Tunnel Name

Description

* Enabled State Enable Disable

* Tunnel Interface ⓘ Add Tunnel Interface

* Authentication Mode

* Key

* Confirm Key

* Local Address Interface ⓘ IP ⓘ

* Peer Address ⓘ

* Local ID Type

Verify Peer ID

☰ Advanced

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

b Configure interesting traffic.

On the interesting traffic configuration page, click **Create**. Then configure parameters as follows:

- Set **Proxy Mode** to **Subnet-to-Subnet**.
- Set **Local Network** to 192.168.2.0/24 and **Peer Network** to 192.168.1.0/24.

The screenshot shows a configuration wizard with three steps: **Basic Config** (marked with a green checkmark), **Interesting Traffic Config** (marked with a blue '2'), and **Security Parameter Config** (marked with a grey '3'). Below the steps are two buttons: **Create** (with a plus icon) and **Delete** (with a trash icon). To the right is a search bar with the placeholder text "Enter the keyword." and a magnifying glass icon. Below these elements is a table with the following data:

<input type="checkbox"/>	Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/>	Subnet-to-Subnet	192.168.2.0/24	192.168.1.0/24	Edit Delete

After completing the configuration for interesting traffic, click **Next**.

c Configure security parameters.

On the security parameter configuration page, configure IKE and IPsec parameters and ensure that the configuration matches that on the peer device.

- o IKE parameters: Set **Negotiation Mode** to **IKEv1 Main Mode**, **Encryption Algorithm** to **AES-128**, **Verification Algorithm** to **SHA**, **DH Group** to **GROUP5**, and **SA Lifetime** to 86400 (in seconds).
- o IPsec parameters: Set **Protocol** to **ESP**, **Encapsulation Mode** to **Tunnel**, **Encryption Algorithm** to **AES-128**, and **Verification Algorithm** to **SHA**. Do not toggle on **Perfect Forward Secrecy**. Set **SA Lifetime** to 3600 (in seconds) and **Tunnel MTU** to 1400.

IKE Parameter

* Negotiation Mode: IKEv1 Main Mode

* Encryption Algorithm: AES-128

* Verification Algorithm: SHA

* DH Group: GROUP5

* SA Lifetime: 86400 Second

IPsec Parameter

* Protocol: ESP

* Encapsulation Mode: Tunnel

* Encryption Algorithm: AES-128

* Verification Algorithm: SHA

Perfect Forward Secrecy:

* SA Lifetime: 3600 Second

Previous
Cancel
Finish

Click **Finish** to complete the configuration for the IPsec tunnel.

(3) Create security policies.

- a Choose **Object > Address > IPv4 Address**. On the page that is displayed, click **Create** and create two address objects for local network 192.168.2.0/24 and peer network 192.168.1.0/24 of the interesting traffic separately.

	IPv4 Address	IPv6 Address	IPv4 Address Group	IPv6 Address Group
	<div style="display: flex; justify-content: center; gap: 10px;"> + Create 🗑️ Delete 🔄 Refresh </div>			
	Name	IP Address/Range	Address Group	Address Group
<input type="checkbox"/>	VPN-remotesubnet	192.168.1.0/24		-
<input type="checkbox"/>	VPN-localsubnet	192.168.2.0/24		-

- b Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, click **Create** and create outbound security policy **VPN-outbound** and inbound security policy **VPN-inbound** separately.

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

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

[Back](#) **Edit Security Policy**

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [+ Add Group](#)

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

(4) Configure a static route.

- a Choose **Network > Routing > Static Routing > IPv4**.
- b Click **Create** and create a static route to the peer protected subnet of the VPN.

< Back

Edit Static Routing

IP Type IPv4

* Dest. IP Range/Mask

Next-Hop Address

Interface

* ⓘ Priority

Link Detection

Description

7. Verification

- Verifying Configuration of Site A

Choose **Network > IPsec VPN > Tunnel Monitoring**. On the page that is displayed, check tunnel establishment and status information.

Tunnel Monitoring

Start
Stop
Refresh
Custom Field

Enter a tunnel name. Q

Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent	Operation
Site-to-Site	● Not established	Point-to-Point	10.1.5.211	192.168.1.0/24->192.168.2.0/24	0		Start

- Verifying Configuration of Site B

Choose **Network > IPsec VPN > Tunnel Monitoring**. On the page that is displayed, check tunnel establishment and status information.

Tunnel Monitoring

Start
Stop
Refresh
Custom Field

Enter a tunnel name. Q

Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets	Operation
Site-to-Site	● Established	Point-to-Point	10.1.5.203	192.168.2.0/24->192.168.1.0/24	2346	0	Stop

8.25.5 Configuration Examples of Site-to-Site IPsec VPN (Interconnection with Fortinet Firewall)

1. Applicable Products and Versions

Table 8-29 Products and Versions

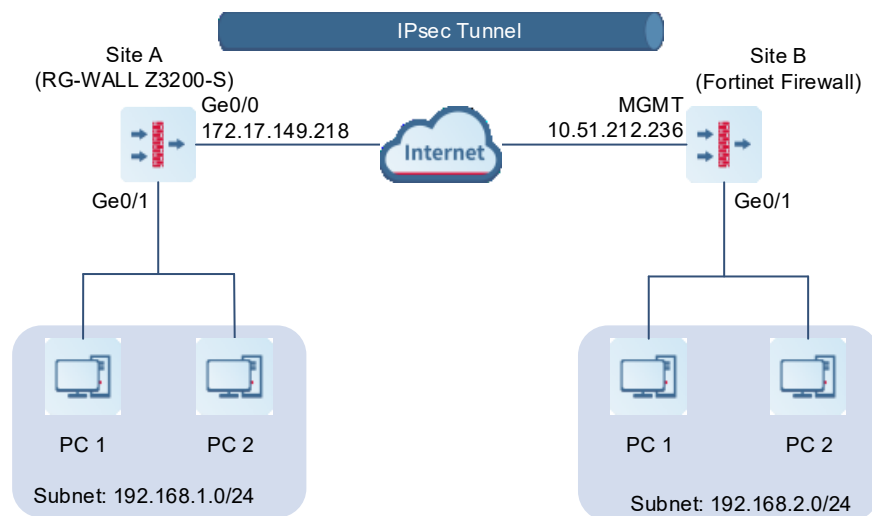
Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R8 or later
Firewall	FortiGate 100F	FortiOS 7.2.4 Build 1396 (Feature)

2. Service Demands

As shown in [Figure 8-21](#), Site A (RG-WALL Z3200-S) and Site B (Fortinet firewall) at both ends have fixed public IP addresses. A site-to-site IPsec VPN tunnel needs to be established between the LANs of the two sites to achieve secure mutual access.

The authentication mode should be pre-shared key, and the encapsulation mode should be the tunnel mode. In this way, both ends can initiate connections.

Figure 8-21 Site-to-Site Networking



3. Restrictions and Guidelines

Currently, the IPsec VPN function of the RG-WALL 1600-Z series firewall supports only the IKEv1 protocol for pre-shared key authentication and ESP tunnel mode for encapsulation.

4. Prerequisites

You have completed basic network configurations for Site A and Site B, including interface IP addresses and default routes. Pay attention to the following points during configuration:

- Ensure that the IP addresses of Site A and Site B are fixed.

5. Procedure

Configuring Site A (RG-WALL 1600-Z3200-S)

(1) Basic Configuration

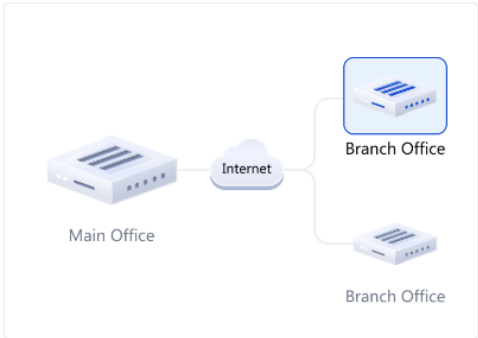
- a Log in to the RG-WALL 1600-Z3200-S firewall and choose **Network > IPsec VPN > Config Wizard**. The basic configuration page of the configuration wizard is displayed.
- b Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.

① Basic Config ② Authentication Config ③ Interesting Traffic Config ④ Config Verification

* ① Tunnel Interface

* Tunnel Name

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



Cancel Next

- c After completing the configuration, click **Next**.

(2) Authentication Configuration

- a Configure parameters as follows:
 - o Set the peer address to the IP address of the Fortinet firewall's WAN interface (10.51.212.236).
 - o Set the outbound interface to that of the local device (Ge0/0).
 - o Set the authentication mode to pre-shared key, and set the key to 123123. The pre-shared keys on both ends of an IPsec VPN tunnel must be the same. Otherwise, the tunnel cannot be established.

Basic Config **Authentication Config** Interesting Traffic Config Config Verification

* Peer Address

* Outbound Interface

* Authentication Mode Pre-shared Key

*

*

(3)

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

(4) Interesting Traffic Configuration

a Click **Create**. Configure parameters for interesting traffic as follows:

- o Set **Proxy Mode** to **Subnet-to-Subnet**.
- o Set the local network to the subnet 192.168.1.0/24 of the RG-WALL Z3200-S.
- o Set the peer network to the subnet 192.168.2.0/24 of the Fortinet firewall.

Basic Config Authentication Config **Interesting Traffic Config** Config Verification

<input type="checkbox"/>	Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/>	Subnet-to-Su...	192.168.1.0/24	192.168.2.0/24	Edit Delete

/ Page Total:1 Go to

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

(5) Verification

a Verify that the basic configuration, authentication configuration, and interesting traffic configuration are correct.

✓ Basic Config
 ✓ Authentication Config
 ✓ Interesting Traffic Config
 4 Config Verification

Basic Config [Edit](#)

Tunnel Interface

Tunnel Name

Scenario Point-to-Point [?](#) Point-to-Multipoint [?](#)

Authentication Config [Edit](#)

Peer Address

Outbound Interface

Authentication Mode Pre-shared Key

[?](#) Key

Interesting Traffic Config [Edit](#)

Local Network	Peer Network
192.168.1.0/24	192.168.2.0/24

- b Click **Advanced Settings** and modify the following IKE and IPsec parameters. Use the default configuration for the other parameters.

IKE parameters:

- o Set **IKE Version** to **IKEv1**.
- o Set **Negotiation Mode** to **IKEv1 Main Mode**.
- o Set **Encryption Algorithm** to **AES-128**.
- o Set **Verification Algorithm** to **SHA**.
- o Set **DH Group** to **GROUP5**.

Advanced Settings [Fold](#)

* Local ID Type

Peer ID Authentication

DPD Type

DPD Detection Interval Second

DPD Retry Interval Second

IKE Parameter

* IKE Version IKEv1 IKEv2

* Negotiation Mode

* Encryption Algorithm

* Verification Algorithm

* DH Group

* SA Lifetime Second

IPsec parameters:

- o Set **Encryption Algorithm** to **AES-128**.
- o Set **Verification Algorithm** to **SHA**.
- o Enable **Perfect Forward Secrecy**.
- o Set **DH Group** to **GROUP5**.

IPsec Parameter

* Protocol

* Encapsulation Mode

* Encryption Algorithm

* Verification Algorithm

Perfect Forward Secrecy

* DH Group

* SA Lifetime Second

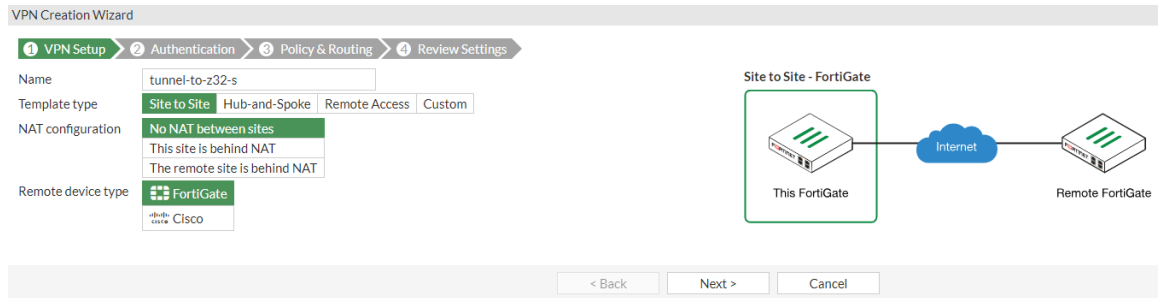
Tunnel MTU

- c After verifying the configuration, click **Finish**.

Configuring Site B (Fortinet Firewall)

(1) VPN Setup

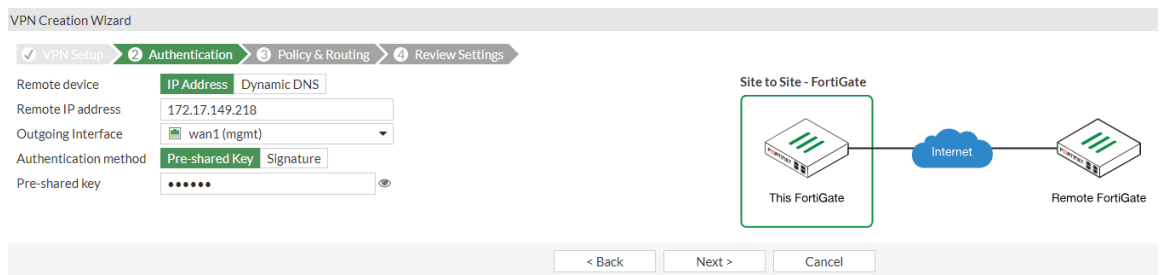
- a Log in to the Fortinet firewall and choose **VPN > IPsec Wizard**. The configuration wizard page is displayed.
- b Configure parameters as follows:
 - o Set **Template type** to **Site to Site**.
 - o Set **NAT configuration** to **No NAT between sites**.
 - o For the device type, use the default configuration.



- c After completing the configuration, click **Next**.

(2) Authentication Configuration

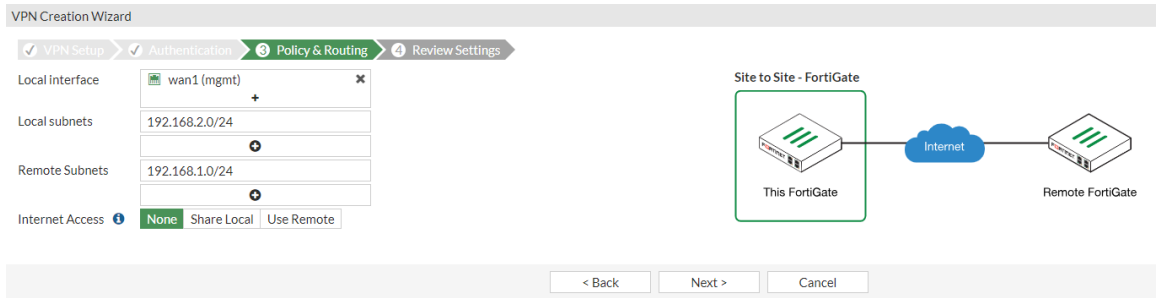
- a Configure parameters as follows:
 - o Set **Remote device** to **IP Address**.
 - o Set **Remote IP address** to the IP address of the RG-WALL Z3200-S (172.17.149.218).
 - o Set **Outgoing interface** to that of the local device: **wan1(mgmt)**.
 - o Set **Authentication method** to **Pre-shared Key**, and set the key to 123123. The pre-shared keys on both ends of an IPsec VPN tunnel must be the same. Otherwise, the tunnel cannot be established.



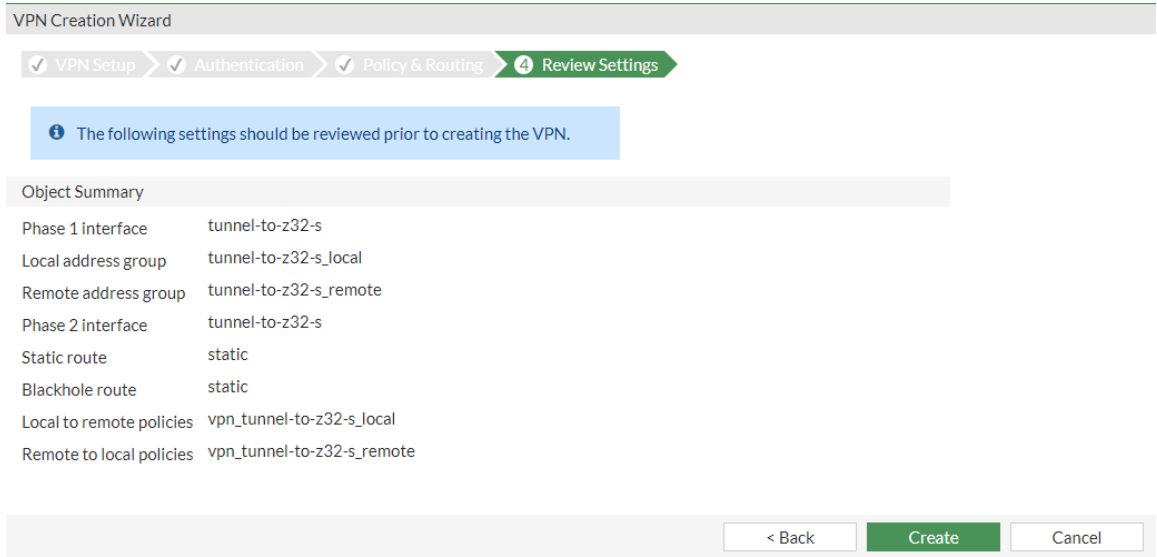
- b After completing the configuration, click **Next**.

(3) Policy and Route Configuration

- a Configure policy and route parameters as follows:
 - o Set **Local interface** to the outbound interface **wan1(mgmt)** of the local device.
 - o Set **Local subnets** to the subnet 192.168.2.0/24 of the Fortinet firewall.
 - o Set **Remote subnets** to the subnet 192.168.1.0/24 of the RG-WALL Z3200-S.



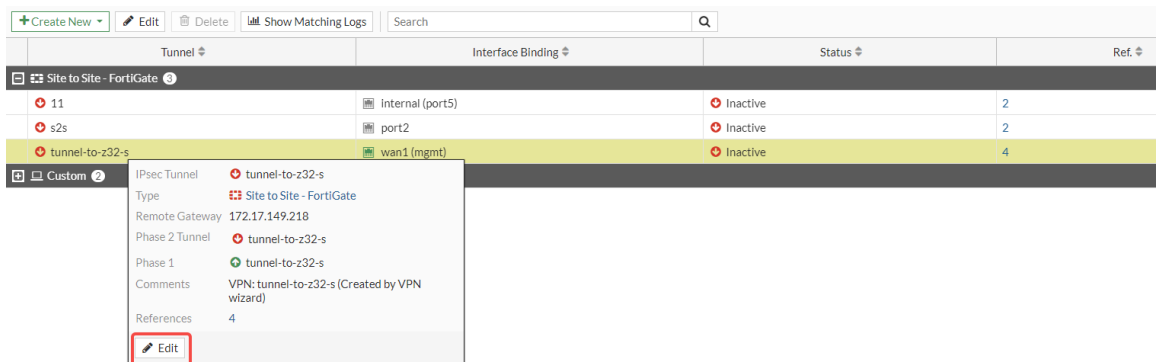
b After completing the configuration, click **Next**. The **Review Settings** page is displayed.



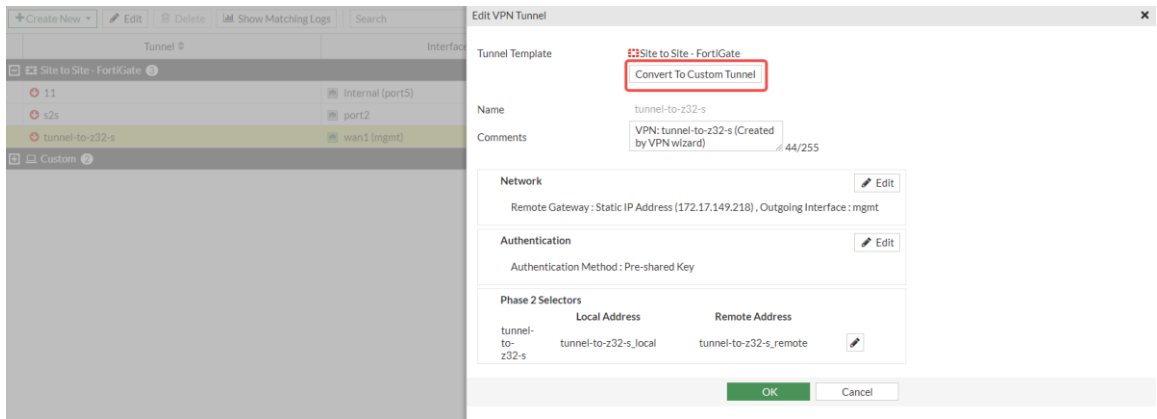
c After verifying the configuration, click **Create**.

(4) VPN Authentication Configuration

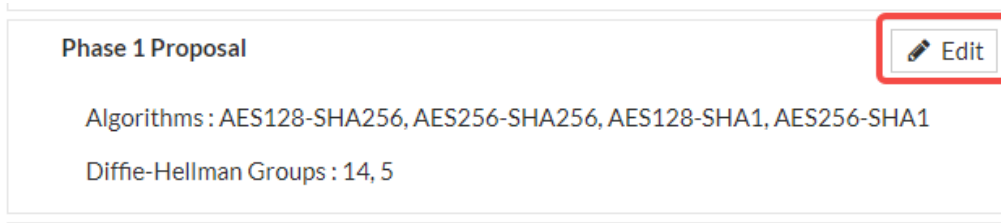
a Choose **VPN > IPsec Tunnels**. The IPsec tunnel page is displayed.



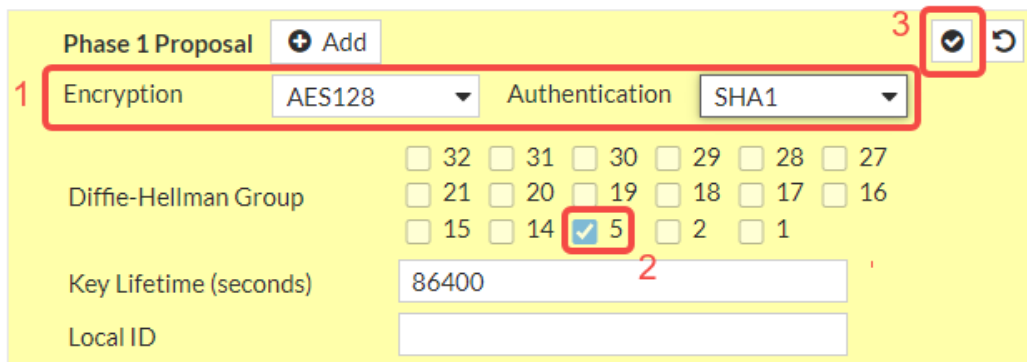
b Select the tunnel created in the previous step, and click **Edit**. In the dialog box that is displayed, click **Convert To Custom Tunnel**.



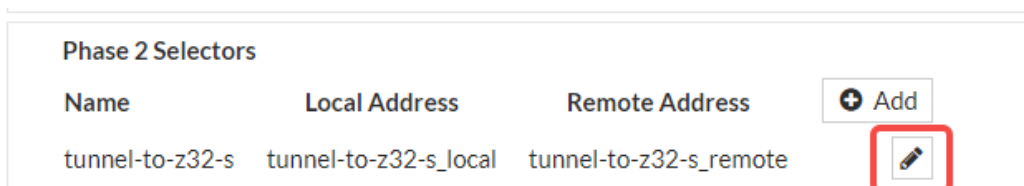
- c Click **Edit** in the **Phase 1 Proposal** area and modify the authentication parameters according to the following figure.



- o Set **Encryption** to **AES128**.
- o Set **Authentication** to **SHA1**.
- o Set **Diffie-Hellman Group** to **5**.
- o Use the default configuration for the other parameters.



- d Click the edit icon in the **Phase 2 Proposal** area and modify the authentication parameters according to the following figure.



- o Set **Local Address** to the subnet 192.168.2.0/24 of the Fortinet firewall.
- o Set **Remote Address** to the subnet 192.168.1.0/24 of the RG-WALL Z3200-S.
- o Set **Encryption** to **AES128**.
- o Set **Authentication** to **SHA1**.
- o Set **Diffie-Hellman Group** to **5**.
- o Use the default configuration for the other parameters.

Edit Phase 2 4 🔒 ↺

Name: tunnel-to-z32-s

Comments: VPN: tunnel-to-z32-s (Created by VPN wizard)

Local Address: Subnet ▼ 192.168.2.0/24

Remote Address: Subnet ▼ 192.168.1.0/24 1

Advanced...

Phase 2 Proposal ➕ Add

Encryption: AES128 ▼ Authentication: SHA1 ▼ 2

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group: 32 31 30 29 28 27
 21 20 19 18 17 16
 15 14 5 2 1 3

Local Port: All

Remote Port: All

Protocol: All

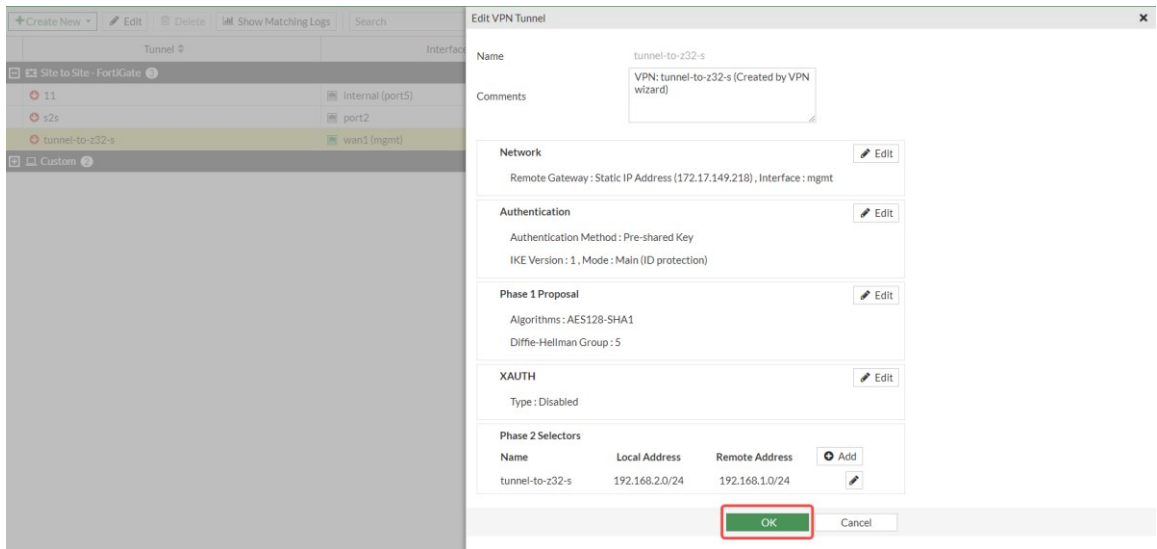
Auto-negotiate:

Autokey Keep Alive:

Key Lifetime: Seconds ▼

Seconds: 43200

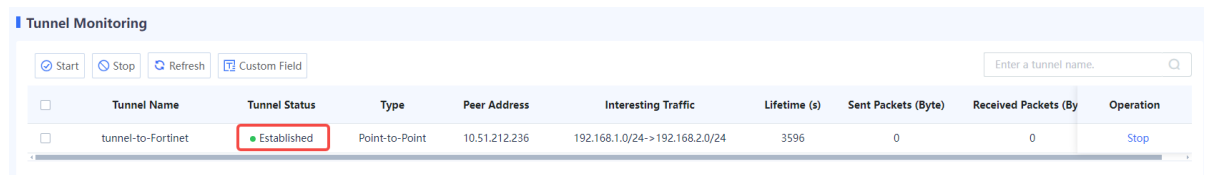
- e After completing the modification, click **OK**.



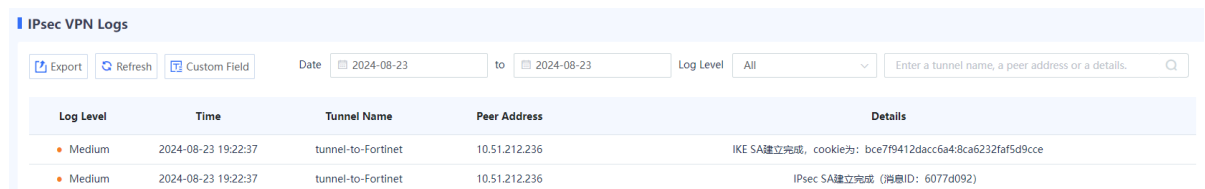
6. Verification

Verifying Configuration of Site A (RG-WALL Z3200-S)

- Choose **Network > IPsec VPN > Tunnel Monitoring**. Verify that the tunnel status is **Established**.

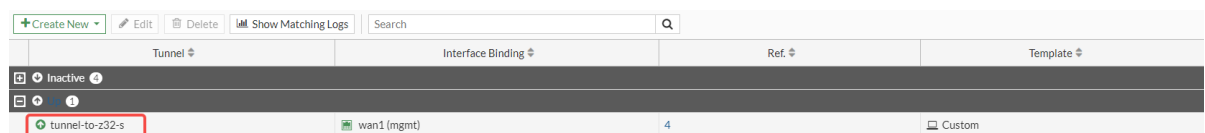


- Choose **Monitor > Log Monitoring > IPsec VPN Log**. Check IPsec tunnel negotiation logs.



Verifying Configuration of Site B (Fortinet Firewall)

- Choose **VPN > IPsec Tunnels**. Verify that the tunnel status is established.



- Select the IPsec tunnel and click **Show Matching Logs** to view IPsec tunnel negotiation logs.

The screenshot shows a network management interface with a 'Show Matching Logs' button highlighted in red. Below the interface is a table of logs for a VPN tunnel named 'tunnel-to-z32-s'.

Date/Time	Level	Action	Status	Message	VPN Tunnel
2024/08/23 19:18:45	Info	tunnel-stats		IPsec tunnel statistics	tunnel-to-z32-s
2024/08/23 19:16:30	Info	negotiate	success	negotiate IPsec phase 2	tunnel-to-z32-s
2024/08/23 19:16:30	Info	negotiate	success	progress IPsec phase 2	tunnel-to-z32-s
2024/08/23 19:16:30	Info	negotiate	success	progress IPsec phase 2	tunnel-to-z32-s
2024/08/23 19:16:30	Info	tunnel-up		IPsec connection status change	tunnel-to-z32-s
2024/08/23 19:16:30	Info	phase2-up		IPsec phase 2 status change	tunnel-to-z32-s
2024/08/23 19:16:30	Info	install_sa		install IPsec SA	tunnel-to-z32-s
2024/08/23 19:16:30	Info	negotiate	success	progress IPsec phase 1	tunnel-to-z32-s
2024/08/23 19:16:30	Info	negotiate	success	progress IPsec phase 1	tunnel-to-z32-s
2024/08/23 19:16:30	Info	negotiate	success	progress IPsec phase 1	tunnel-to-z32-s
2024/08/23 19:16:30	Info	negotiate	success	progress IPsec phase 1	tunnel-to-z32-s

8.25.6 Configuration Examples of Site-to-Multisite IPsec VPN

1. Applicable Products and Versions

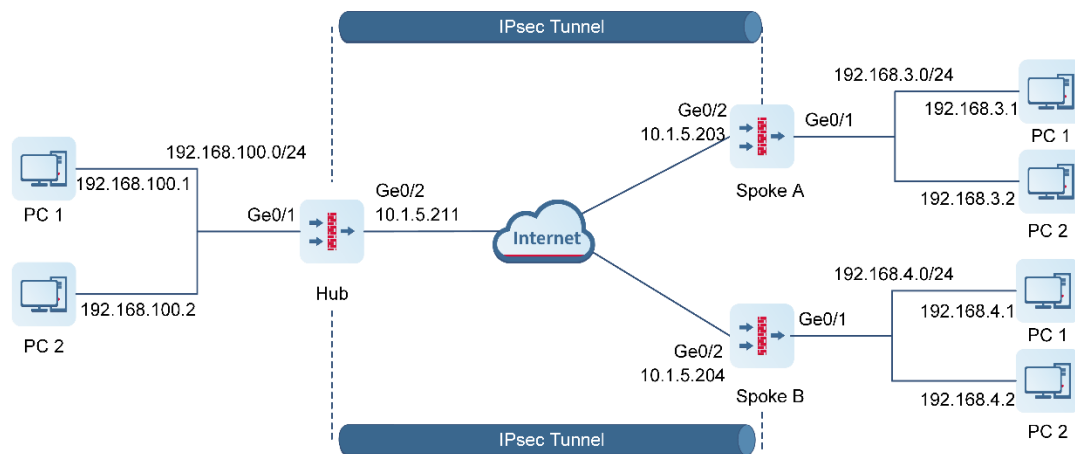
Table 8-30 Products and Versions

Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R6 or later

2. Service Demands

In a point-to-point scenario, a pre-shared key needs to be specified for each peer. When defining an IPsec policy, you also need to specify the IP address or domain name of the peer. As the number of peers increases, duplicate configurations also increase, making maintenance difficult. In addition, if a peer does not have a fixed IP address, the IPsec tunnel cannot be established.

To solve the preceding problems, a point-to-multipoint solution is proposed, as shown in [Figure 8-22](#). In a point-to-multipoint scenario, the hub site needs to establish tunnels with multiple spoke sites. All the spoke sites use the same pre-shared key as the hub site. The hub site does not initiate connections. Instead, the spoke sites initiate connections to establish IPsec tunnels.

Figure 8-22 Point-to-Multipoint Networking

3. Restrictions and Guidelines

- Currently, if the RG-WALL 1600-Z series firewall acts as a hub site on an IPsec VPN, all spoke sites must use the same pre-shared key to negotiate with the hub site.
- The following describes how to configure Spoke A. The configuration for Spoke B is similar.

4. Prerequisites

You have completed basic network configurations for Site A and Site B, including interface IP addresses and default routes. Pay attention to the following points during configuration:

- Ensure that the IP address of the hub site is fixed.
- All spoke sites obtain the pre-shared key configured on the hub site in out-of-band (OOB) mode.

5. Using a Configuration Wizard

- Configuring the Hub Site

(1) Perform basic configuration.

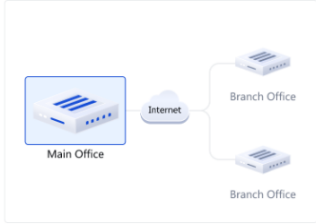
- Choose **Network > IPsec VPN > Config Wizard**. The basic configuration page of the configuration wizard is displayed.
- Set **Scenario** to **Point-to-Multipoint**, and set the other parameters according to the following figure.

① Basic Config ② Authentication Config ③ Interesting Traffic Config ④ Config Verification

* Tunnel Interface

* Tunnel Name

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



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

(2) Configure authentication.

a Configure parameters according to the following figure.

① Basic Config ② Authentication Config ③ Interesting Traffic Config ④ Config Verification

* Outbound Interface

* Authentication Mode Pre-shared Key

* Key

* Confirm Key

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

(3) Configure interesting traffic.

a Click **Create**. Configure parameters for interesting traffic according to the following figure.

Basic Config Authentication Config **Interesting Traffic Config** Config Verification

<input type="checkbox"/>	Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/>	Auto	any	any	Edit Delete

10 / Page Total:1 Go to

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

(4) Verify configuration.

a After verifying the configuration, click **Finish**.

✓ ✓ ✓ ④
 Basic Config Authentication Config Interesting Traffic Config Config Verification

① The tunnel configured on the wizard will be added to the custom tunnel list.

Basic Config [Edit](#)

Tunnel Interface: vti100

Tunnel Name: Hub-Spoke

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

Authentication Config [Edit](#)

Outbound Interface: Ge0/2

Authentication Mode: Pre-shared Key

Key:

Interesting Traffic Config [Edit](#)

Local Network	Peer Network
any	any

Advanced Settings [Expand](#)

Previous Cancel Finish

● Configuring Spoke A

(1) Perform basic configuration.

- a Choose **Network > IPsec VPN > Config Wizard**. The basic configuration page of the configuration wizard is displayed.
- b Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.

① ② ③ ④
 Basic Config Authentication Config Interesting Traffic Config Config Verification

* ① Tunnel Interface: vti 100

* Tunnel Name: Site-to-Site

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

Cancel Next

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

(2) Configure authentication.

a Configure parameters according to the following figure.

Basic Config **Authentication Config** Interesting Traffic Config Config Verification

* Peer Address

* Outbound Interface

* Authentication Mode Pre-shared Key

* Key

* Confirm Key

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

(3) Configure interesting traffic.

a Click **Create**. Configure parameters for interesting traffic according to the following figure.

Basic Config Authentication Config **Interesting Traffic Config** Config Verification

<input type="checkbox"/>	Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/>	Subnet-to-Subnet	192.168.3.0/24	192.168.100.0/24	Edit Delete

/ Page Total:1 Go to

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

(4) Verify configuration.

a After verifying the configuration, click **Finish**.

Basic Config Authentication Config Interesting Traffic Config **Config Verification**

... will be added to the custom tunnel list.

Basic Config Edit

Tunnel Interface vti100

Tunnel Name Site-to-Site

Scenario Point-to-Point Point-to-Multipoint

Authentication Config Edit

Peer Address 10.1.5.211

Outbound Interface Ge0/2

Authentication Mode Pre-shared Key

Key *****

Interesting Traffic Config Edit

Local Network	Peer Network
192.168.3.0/24	192.168.100.0/24

Advanced Settings Expand

Previous Cancel Finish

6. Manually Configuring a Tunnel

- Configuring the Hub Site
- (1) Configure a tunnel interface.
 - a Choose **Network > Interface > Tunnel Interface**.
 - b On the page that is displayed, click **Create**.
 - c On the tunnel interface configuration page that is displayed, configure parameters as follows:
 - Set **Interface Name** to **vti100**.
 - Add security zone VPN-Zone and set **Security Zone** to **VPN-Zone** for this interface.
 - Set **Tunnel Local Address** to the default outbound interface address of the hub site: 10.1.5.211.
 - Set **Tunnel Remote Address** to **Dynamic**.

[Back](#) **Create Tunnel Interface Details**

* Interface Name vti100

Security Zone VPN-Zone [+ Add Security Zone](#)

* Tunnel Local Address 10.1.5.211

Tunnel Remote Address IP Dynamic

Description Enter Description

(2) Configure an IPsec tunnel.

a Perform basic configuration.

Choose **Network > IPsec VPN > Custom Tunnel**. Click **Create**. On the basic configuration page of the custom tunnel, configure parameters as follows:

- o Set **Tunnel Name** to **Hub-Spoke**.
- o Set **Enabled State** to **Enable**.
- o Set **Tunnel Interface** to **vti100**.
- o Set **Local Address** to **interface Ge0/2**.
- o For **Authentication Mode**, use the default value **Pre-shared Key**. Set both **Key** and **Confirm Key** to **ruijie123**.
- o Toggle on **Reverse Route Injection** for the hub site. For **Priority**, use the default value 5. Do not configure **Next-Hop Address**.

1 Basic Config 2 Interesting Traffic Config 3 Security Parameter Config

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

* Tunnel Name

Description

* Enabled State Enable Disable

* Tunnel Interface [⊕ Add Tunnel Interface](#)

* Authentication Mode

* Key

* Confirm Key

* Local Address Interface IP

* Local ID Type

Verify Peer ID

☰ **Advanced**

Reverse Route Injection

Next-Hop Address

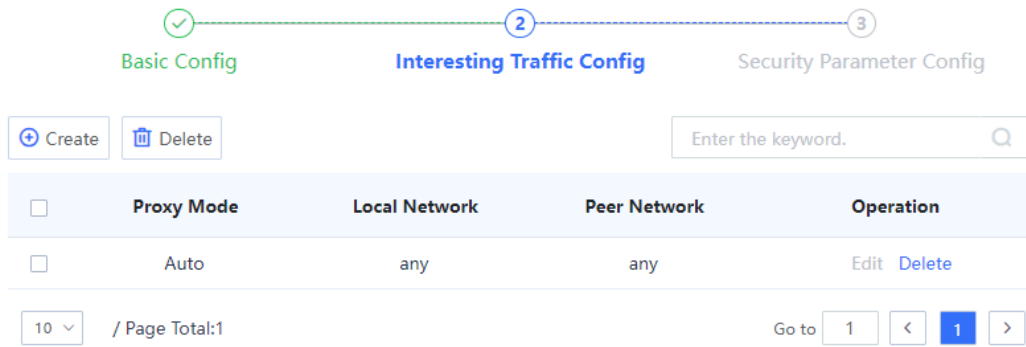
* Priority

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

b Configure interesting traffic.

On the interesting traffic configuration page, click **Create**. Then configure parameters as follows:

o Set **Proxy Mode** to **Auto**.



After completing the configuration for interesting traffic, click **Next**.

c Configure security parameters.

On the security parameter configuration page, configure IKE and IPsec parameters and ensure that the configuration matches that on the peer device.

- o IKE parameters: Set **Negotiation Mode** to **IKEv1 Main Mode**, **Encryption Algorithm** to **AES-128**, **Verification Algorithm** to **SHA**, **DH Group** to **GROUP5**, and **SA Lifetime** to 86400 (in seconds).
- o IPsec parameters: Set **Protocol** to **ESP**, **Encapsulation Mode** to **Tunnel**, **Encryption Algorithm** to **AES-128**, and **Verification Algorithm** to **SHA**. Do not toggle on **Perfect Forward Secrecy**. Set **SA Lifetime** to 3600 (in seconds) and **Tunnel MTU** to 1400.

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

IKE Parameter

* Negotiation Mode

* Encryption Algorithm

* Verification Algorithm

* DH Group

* SA Lifetime Second

IPsec Parameter

* Protocol

* Encapsulation Mode

* Encryption Algorithm

* Verification Algorithm

Perfect Forward Secrecy

* SA Lifetime Second

Tunnel MTU

Click **Finish** to complete the IPsec tunnel configuration for the hub site.

(3) Create security policies.

- a Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, click **Create** and create outbound security policy **VPN-hub-outbound** and inbound security policy **VPN-hub-inbound** separately.

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

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

< Back

Create Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

- **Configuring Spoke A**

(1) Configure a tunnel interface.

- a Choose **Network > Interface > Tunnel Interface**.
- b On the page that is displayed, click **Create**.
- c On the tunnel interface configuration page that is displayed, configure parameters as follows:
 - Set **Interface Name** to **vti1**.
 - Add security zone VPN-Zone and set **Security Zone** to **VPN-Zone** for this interface.
 - Set **Tunnel Local Address** to the default outbound interface address of Site A: 10.1.5.203.
 - Set **Tunnel Remote Address** to the default outbound interface address of the hub site: 10.1.5.211.

[Back](#) **Edit Tunnel Interface Details**

* Interface Name

Security Zone [+ Add Security Zone](#)

* Tunnel Local Address

Tunnel Remote Address IP Dynamic

Description

(2) Configure an IPsec tunnel.

- a Perform basic configuration.

Choose **Network > IPsec VPN > Custom Tunnel**. Click **Create**. On the basic configuration page of the custom tunnel, configure parameters as follows:

- o Set **Tunnel Name** to **Site-to-Site**.
- o Set **Enabled State** to **Enable**.
- o Set **Tunnel Interface** to **vti1**. Set **Local Address** to **interface Ge0/2**, and **Peer Address** to 10.1.5.211.
- o For **Authentication Mode**, use the default value **Pre-shared Key**. Set both **Key** and **Confirm Key** to **ruijie123**.

1 Basic Config 2 Interesting Traffic Config 3 Security Parameter Config

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

* Tunnel Name

Description

* Enabled State Enable Disable

* Tunnel Interface [Add Tunnel Interface](#)

* Authentication Mode

* Key

* Confirm Key

* Local Address Interface IP

* Peer Address [Ping](#)

* Local ID Type

Verify Peer ID

[Advanced](#)

[Cancel](#) [Next](#)

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

b Configure interesting traffic.

On the interesting traffic configuration page, click **Create**. Then configure parameters as follows:

- o Set **Proxy Mode** to **Subnet-to-Subnet**.
- o Set **Local Network** to 192.168.3.0/24 and **Peer Network** to 192.168.100.0/24.

Basic Config 2 Interesting Traffic Config 3 Security Parameter Config

[Create](#) [Delete](#)

<input type="checkbox"/>	Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/>	Subnet-to-Subnet	192.168.3.0/24	192.168.100.0/24	Edit Delete

After completing the configuration for interesting traffic, click **Next**.

- c Configure security parameters.

On the security parameter configuration page, configure IKE and IPsec parameters and ensure that the configuration matches that on the peer device.

- o IKE parameters: Set **Negotiation Mode** to **IKEv1 Main Mode**, **Encryption Algorithm** to **AES-128**, **Verification Algorithm** to **SHA**, **DH Group** to **GROUP5**, and **SA Lifetime** to 86400 (in seconds).
- o IPsec parameters: Set **Protocol** to **ESP**, **Encapsulation Mode** to **Tunnel**, **Encryption Algorithm** to **AES-128**, and **Verification Algorithm** to **SHA**. Do not toggle on **Perfect Forward Secrecy**. Set **SA Lifetime** to 3600 (in seconds) and **Tunnel MTU** to 1400.

IKE Parameter

* Negotiation Mode	<input type="text" value="IKEv1 Main Mode"/>	▼
* Encryption Algorithm	<input type="text" value="AES-128"/>	▼
* Verification Algorithm	<input type="text" value="SHA"/>	▼
* DH Group	<input type="text" value="GROUP5"/>	▼
* SA Lifetime	<input type="text" value="86400"/>	Second

IPsec Parameter

* Protocol	<input type="text" value="ESP"/>	▼
* Encapsulation Mode	<input type="text" value="Tunnel"/>	▼
* Encryption Algorithm	<input type="text" value="AES-128"/>	▼
* Verification Algorithm	<input type="text" value="SHA"/>	▼
Perfect Forward Secrecy	<input type="checkbox"/>	
* SA Lifetime	<input type="text" value="3600"/>	Second

Click **Finish** to complete the configuration for the IPsec tunnel.

- (3) Create security policies.

- a Choose **Object > Address > IPv4 Address**. On the page that is displayed, click **Create** and create two address objects for local network 192.168.3.0/24 and peer network 192.168.100.0/24 of the interesting traffic separately.

IPv4 Address	IPv6 Address	IPv4 Address Group	IPv6 Address Group
<div style="display: flex; gap: 10px;"> Create Delete Refresh </div>			
<input type="checkbox"/>	Name	IP Address/Range	Address Group
<input type="checkbox"/>	VPN-remotesubnet	192.168.100.0/24	-
<input type="checkbox"/>	VPN-localsubnet	192.168.3.0/24	-

- b Choose **Policy > Security Policy > Security Policy**. On the page that is displayed, click **Create** and create outbound security policy **VPN-outbound** and inbound security policy **VPN-inbound** separately.

Back

Edit Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group + Add Group

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

[Back](#) **Edit Security Policy**

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [+ Add Group](#)

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

(4) Configure a static route.

- a Choose **Network > Routing > Static Routing > IPv4**.
- b Click **Create** and create a static route to the peer protected subnet of the VPN.

< Back
Edit Static Routing

IP Type IPv4

* Dest. IP Range/Mask

Next-Hop Address

Interface

* i Priority

Link Detection

Description

7. Verification

- Verifying Configuration of the Hub Site

Choose **Network > IPsec VPN > Tunnel Monitoring**. On the page that is displayed, check tunnel establishment and status information.

Tunnel Monitoring

Start
Stop
Refresh
Custom Field

Enter a tunnel name. Q

Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent	Operation
Hub-Spoke	-	Point-to-Multipoint	0.0.0.0	-	-		
Hub-Spoke	● Established	Instance Link	10.1.5.203	192.168.100.0/24->192.168.3.0/24	3586		Stop

- Verifying Configuration of Spoke A

Choose **Network > IPsec VPN > Tunnel Monitoring**. On the page that is displayed, check tunnel establishment and status information.

Tunnel Monitoring

Start
Stop
Refresh
Custom Field

Enter a tunnel name. Q

Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent	Operation
Site-to-Site	● Established	Point-to-Point	10.1.5.211	192.168.3.0/24->192.168.100.0/24	3509		Stop

8.25.7 Configuration Examples of Site-to-Multisite IPsec VPN (Interconnection with Fortinet Firewall)

1. Applicable Products and Versions

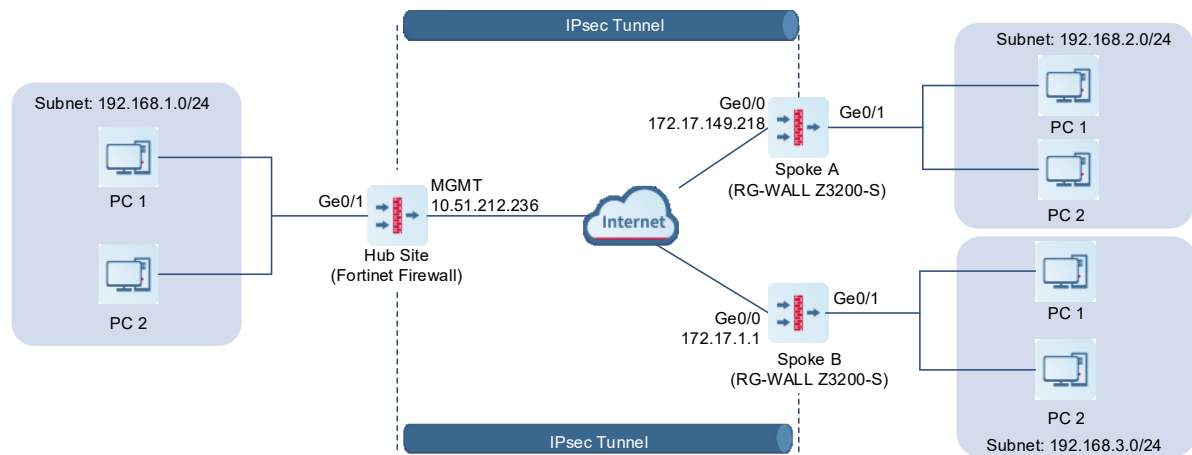
Table 8-31 Products and Versions

Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R8 or later
Firewall	FortiGate 100F	FortiOS 7.2.4 Build 1396 (Feature)

2. Service Demands

As shown in [Figure 8-23](#), in a site-to-multisite scenario, the Fortinet firewall acts as the hub site, and multiple RG-WALL Z3200-S firewalls act as spoke sites. In a site-to-multisite scenario, the hub site needs to establish tunnels with multiple spoke sites. All the spoke sites use the same pre-shared key as the hub site. The hub site does not initiate connections. Instead, the spoke sites initiate connections to establish IPsec tunnels.

Figure 8-23 Site-to-Multisite Networking



3. Restrictions and Guidelines

- If the Fortinet FortiGate 100F series firewall acts as a hub site on an IPsec VPN, all spoke sites must use the same pre-shared key to negotiate with the hub site.
- The following describes how to configure Spoke A. The configuration for Spoke B is similar.

4. Prerequisites

You have completed basic network configurations for the hub site, Site A, and Site B, including interface IP addresses and default routes. Pay attention to the following points during configuration:

- Ensure that the IP address of the hub site is fixed.
- All spoke sites obtain the pre-shared key configured on the hub site in OOB mode.

5. Procedure

Configuring Spoke A (RG-WALL Z3200-S)

(1) Basic Configuration

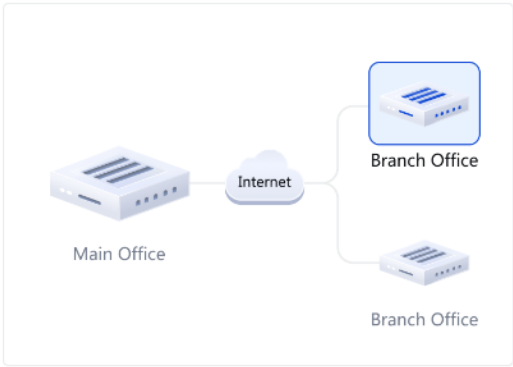
- a Log in to the RG-WALL Z3200-S firewall and choose **Network > IPsec VPN > Config Wizard**. The basic configuration page of the configuration wizard is displayed.
- b Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.

① **Basic Config** ② Authentication Config ③ Interesting Traffic Config ④ Config Verification

* ① Tunnel Interface

* Tunnel Name

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



Cancel Next

- c After completing the configuration, click **Next**.

(2) Authentication Configuration

- a Configure parameters as follows:
 - o Set the peer address to the IP address of the Fortinet firewall's WAN interface (10.51.212.236).
 - o Set the outbound interface to that of the local device (Ge0/0).
 - o Set the authentication mode to pre-shared key, and set the key to 123123. The pre-shared keys on both ends of an IPsec VPN tunnel must be the same. Otherwise, the tunnel cannot be established.

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

(3) Interesting Traffic Configuration

- a Click **Create**. Configure parameters for interesting traffic according to the following figure.
 - o Set **Proxy Mode** to **Subnet-to-Subnet**.
 - o Set the local network to the subnet 192.168.2.0/24 of the RG-WALL Z3200-S.
 - o Set the peer network to the subnet 192.168.1.0/24 of the Fortinet firewall.

<input type="checkbox"/>	Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/>	Subnet-to-Su...	192.168.2.0/24	192.168.1.0/24	Edit Delete

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

(4) Verification

- a Verify that the basic configuration, authentication configuration, and interesting traffic configuration are correct.

✓ Basic Config
 ✓ Authentication Config
 ✓ Interesting Traffic Config
 4 Config Verification

Basic Config [Edit](#)

Tunnel Interface

Tunnel Name

Scenario Point-to-Point [?](#) Point-to-Multipoint [?](#)

Authentication Config [Edit](#)

Peer Address

Outbound Interface

Authentication Mode Pre-shared Key

[?](#) Key

Interesting Traffic Config [Edit](#)

Local Network	Peer Network
192.168.2.0/24	192.168.1.0/24

- b Click **Advanced Settings** and modify the following IKE and IPsec parameters. Use the default configuration for the other parameters.

IKE parameters:

- o Set **IKE Version** to **IKEv1**.
- o Set **Negotiation Mode** to **IKEv1 Main Mode**.
- o Set **Encryption Algorithm** to **AES-128**.
- o Set **Verification Algorithm** to **SHA**.
- o Set **DH Group** to **GROUP5**.

Advanced Settings [Fold](#)

* Local ID Type

Peer ID Authentication

DPD Type

DPD Detection Interval Second

DPD Retry Interval Second

IKE Parameter

* IKE Version IKEv1 IKEv2

* Negotiation Mode

* Encryption Algorithm

* Verification Algorithm

* DH Group

* SA Lifetime Second

IPsec parameters:

- o Set **Encryption Algorithm** to **AES-128**.
- o Set **Verification Algorithm** to **SHA**.
- o Enable **Perfect Forward Secrecy**.
- o Set **DH Group** to **GROUP5**.

IPsec Parameter

* Protocol

* Encapsulation Mode

* Encryption Algorithm

* Verification Algorithm

Perfect Forward Secrecy

* DH Group

* SA Lifetime Second

Tunnel MTU

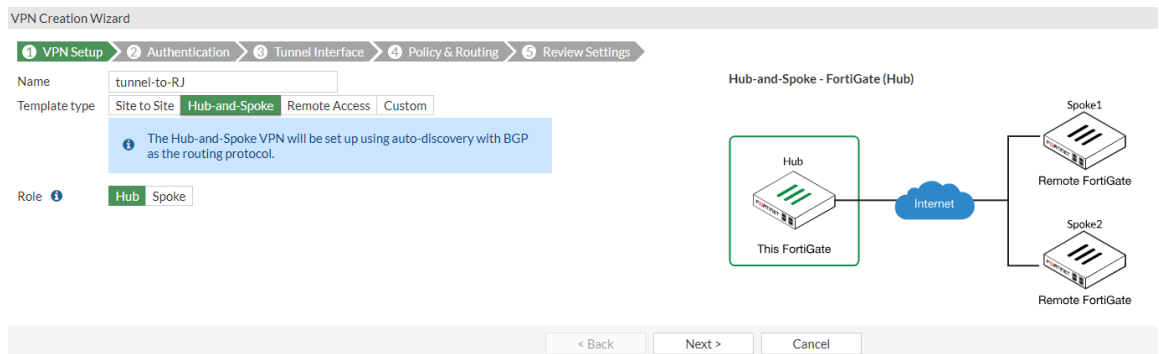
Configuring Spoke B (RG-WALL Z3200-S)

The configuration steps are the same as those of Spoke A and are not described here.

Configuring the Hub Site (Fortinet Firewall)

(1) VPN Setup

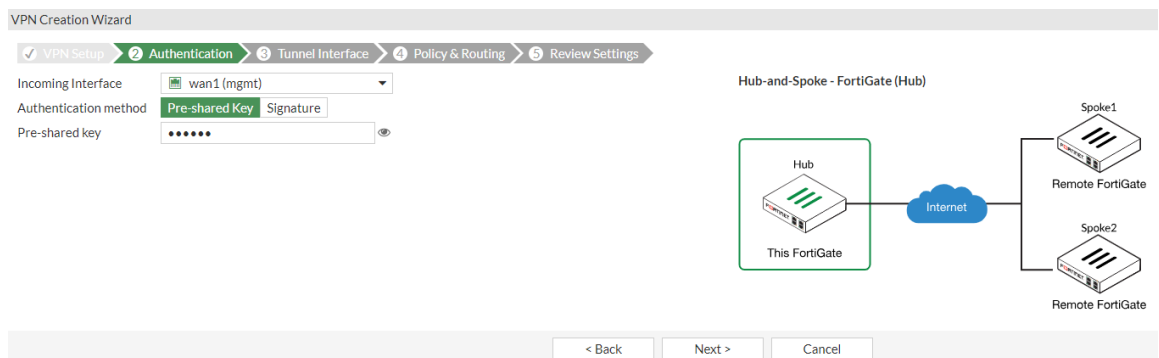
- a Log in to the Fortinet firewall and choose **VPN > IPsec Wizard**. The configuration wizard page is displayed.
- b Configure parameters as follows:
 - o Set **Template type** to **Hub-and-Spoke**.
 - o Select **Role** to **Hub**.



- c After completing the configuration, click **Next**.

(2) Authentication Configuration

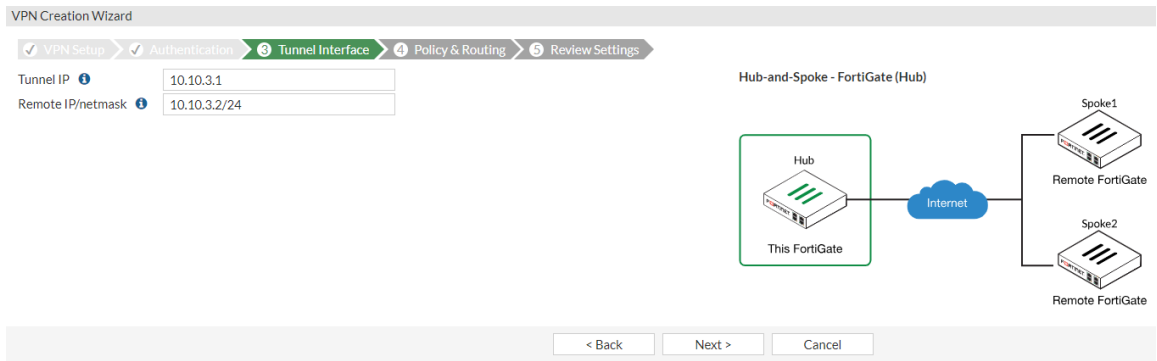
- a Configure parameters as follows:
 - o Set **Incoming interface** to the WAN interface of the local device: **wan1(mgmt)**.
 - o Set **Authentication method** to **Pre-shared Key**, and set the key to 123123. The pre-shared keys on both ends of an IPsec VPN tunnel must be the same. Otherwise, the tunnel cannot be established.



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

(3) Tunnel Interface Configuration

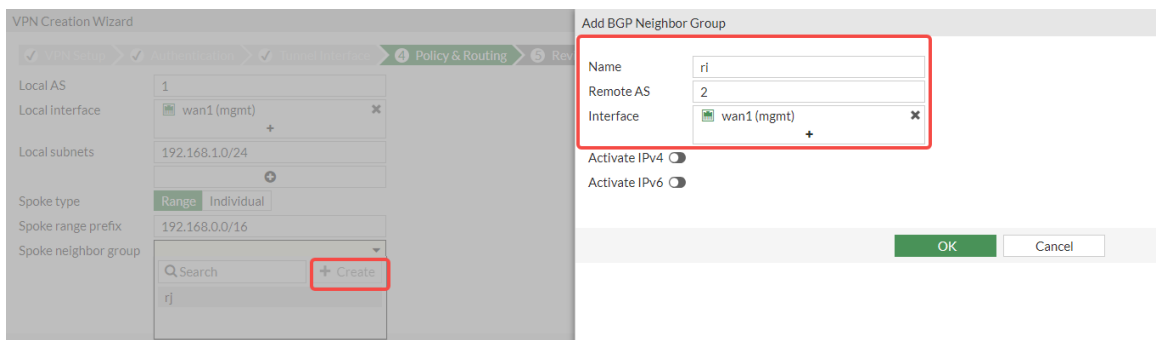
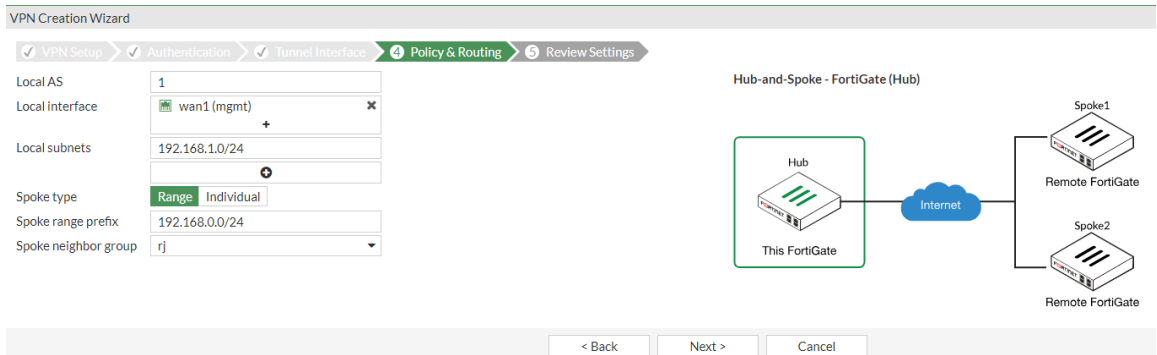
Use the default configuration for parameters on this page and click **Next**.



(4) Policy and Route Configuration

a Configure policy and route parameters as follows:

- o Set **Local AS** to 1.
- o Set **Local interface** to **wan1(mgmt)** of the local device.
- o Set **Local subnets** to the subnet 192.168.1.0/24 of the Fortinet firewall.
- o Set **Spoke type** to **Range**.
- o Set the **Spoke range prefix** to the subnet range 192.168.0.0/16 of the spoke sites.
- o For **Spoke neighbor group**, click **Create**. Set **Name** and **Remote AS** as required, and select the local WAN interface **wan1(mgmt)** as the interface.



b After completing the configuration, click **Next**. The **Review Settings** page is displayed.

VPN Creation Wizard

✓ VPN Setup >
 ✓ Authentication >
 ✓ Tunnel Interface >
 ✓ Policy & Routing >
 5 Review Settings

i The following settings should be reviewed prior to creating the VPN.

Object Summary

Phase 1 interface	tunnel-to-RJ
Local address group	tunnel-to-RJ_local
Phase 2 interface	tunnel-to-RJ
Tunnel interface	tunnel-to-RJ
Remote to local policies	vpn_tunnel-to-RJ_spoke2hub
Local to remote policies	vpn_tunnel-to-RJ_spoke2spoke
BGP route	bgp

c After verifying the configuration, click **Create**.

6. Verification

Verifying Configuration of Spoke Sites (Spoke A as an Example)

- Choose **Network > IPsec VPN > Tunnel Monitoring**. Verify that the tunnel status is **Established**.

Tunnel Monitoring

Enter a tunnel name.

<input type="checkbox"/>	Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Received Packets (By)	Operation
<input type="checkbox"/>	tunnel-to-Fortinet	Established	Point-to-Point	10.51.212.236	192.168.2.0/24->192.168.1.0/24	3596	0	0	Stop

- Choose **Monitor > Log Monitoring > IPsec VPN Log**. Check IPsec tunnel negotiation logs.

IPsec VPN Logs

Date: to
Log Level:
Enter a tunnel name, a peer address or a details.

Log Level	Time	Tunnel Name	Peer Address	Details
Medium	2024-08-23 19:22:37	tunnel-to-Fortinet	10.51.212.236	IKE SA建立完成, cookie为: bce7f9412dacc6a4:8ca6232faf5d9cce
Medium	2024-08-23 19:22:37	tunnel-to-Fortinet	10.51.212.236	IPsec SA建立完成 (消息ID: 6077d092)

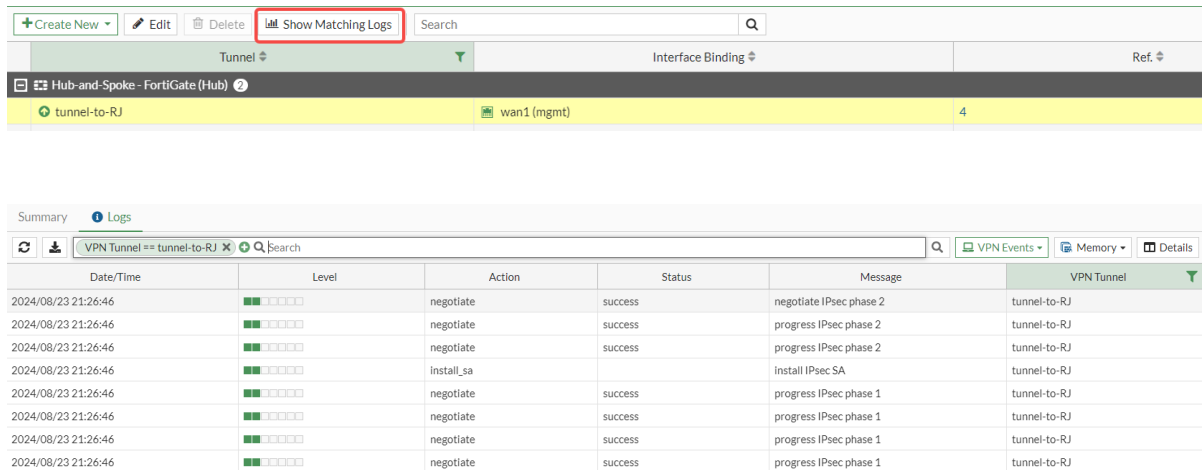
Verifying Configuration of the Hub Site (Fortinet Firewall)

- Choose **VPN > IPsec Tunnels**. Verify that the tunnel status is established.

Search

Tunnel	Interface Binding	Ref.
Hub-and-Spoke - FortiGate (Hub)		
tunnel-to-RJ	wan1 (mgmt)	4

- Select the IPsec tunnel and click **Show Matching Logs** to view IPsec tunnel negotiation logs.



8.25.8 Configuration Examples of IPsec VPN with NAT Traversal

1. Applicable Products and Versions

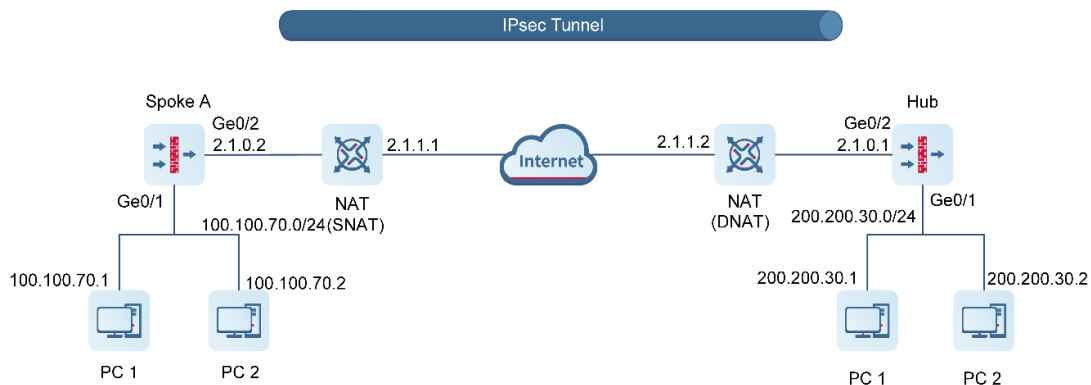
Table 8-32 Products and Versions

Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R6 or later

2. Service Demands

In a scenario of IPsec VPN with NAT traversal, static NAT (SNAT) needs to be deployed for Spoke A to initiate a connection with the hub site, and dynamic NAT (DNAT) needs to be deployed for the hub site. [Figure 8-24](#) shows the typical networking diagram.

Figure 8-24 Networking of IPsec VPN with NAT Traversal



3. Restrictions and Guidelines

- In IPsec, the default port that supports NAT traversal is UDP port 4500. A custom port is not supported.

4. Prerequisites

You have completed basic network configurations, including interface IP address and routing information on routers and servers.

5. Using a Configuration Wizard

- Configuring the Hub Site

(1) Perform basic configuration.

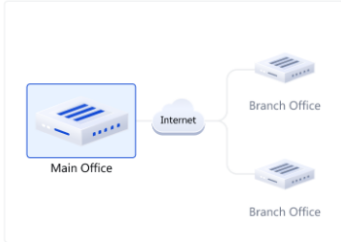
- Choose **Network > IPsec VPN > Config Wizard**. The basic configuration page of the configuration wizard is displayed.
- Set **Scenario** to **Point-to-Multipoint**, and set the other parameters according to the following figure.

① Basic Config ② Authentication Config ③ Interesting Traffic Config ④ Config Verification

* Tunnel Interface

* Tunnel Name

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



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

(2) Configure authentication.

- Configure parameters according to the following figure.

Basic Config **Authentication Config** Interesting Traffic Config Config Verification

* Outbound Interface

* Authentication Mode Pre-shared Key

* Key

* Confirm Key

- b After completing the configuration, click **Next**.
- (3) Configure interesting traffic.
- a Click **Create**. Configure parameters for interesting traffic according to the following figure.

Progress indicator: Basic Config (✓), Authentication Config (✓), Interesting Traffic Config (3), Config Verification (4)

Buttons: Create, Delete, Search (Enter the keyword. Q)

<input type="checkbox"/>	Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/>	Auto	any	any	Edit Delete

Page controls: 10 / Page Total:1, Go to 1 < 1 >

Buttons: Previous, Cancel, Next

- b After completing the configuration, click **Next**.
- (4) Verify configuration.
 - a After verifying the configuration, click **Finish**.

be added to the custom tunnel list.

Basic Config [Edit](#)

Tunnel Interface

Tunnel Name

Scenario Point-to-Point Point-to-Multipoint

Authentication Config [Edit](#)

Outbound Interface

Authentication Mode Pre-shared Key

Key

Interesting Traffic Config [Edit](#)

Local Network	Peer Network
any	any

Advanced Settings [Expand](#)

[Previous](#) [Cancel](#) [Finish](#)

- Configuring Spoke A

(1) Perform basic configuration.

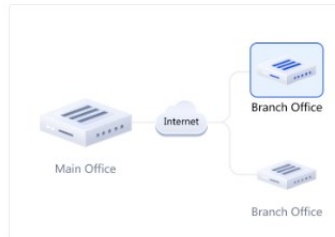
- Choose **Network > IPsec VPN > Config Wizard**. The basic configuration page of the configuration wizard is displayed.
- Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.



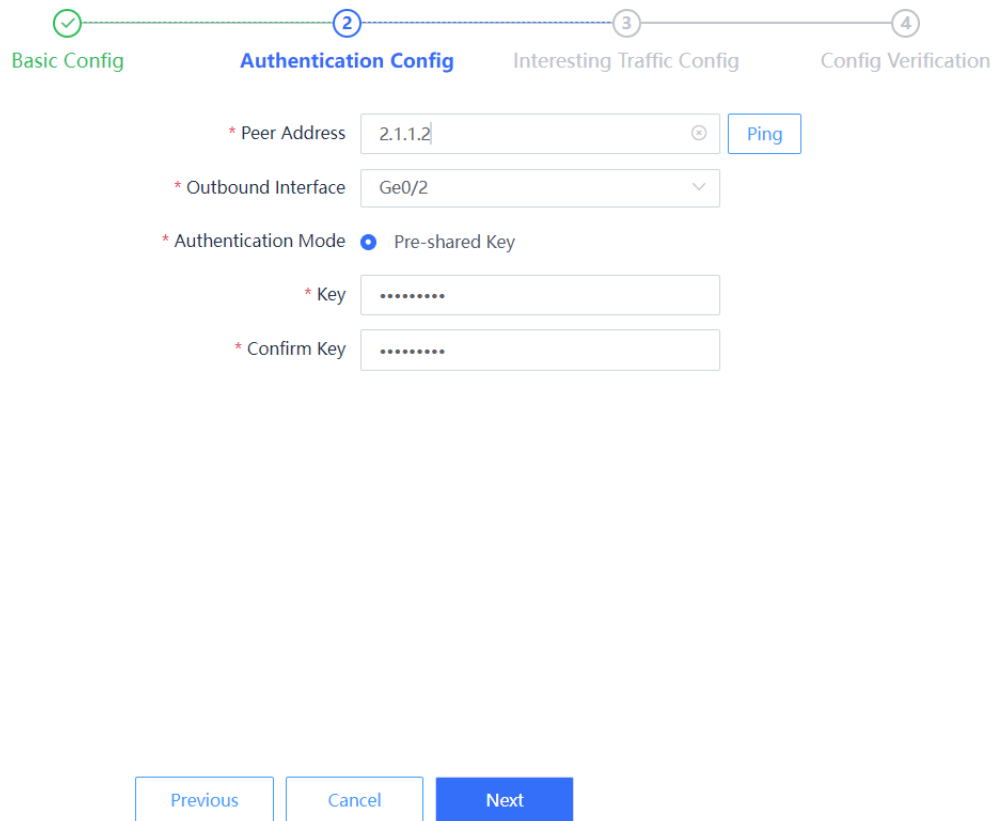
* ① Tunnel Interface

* Tunnel Name

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



- c After completing the configuration, click **Next**.
- (2) Configure authentication.
 - a Configure parameters according to the following figure.



The image shows a configuration wizard with four steps: 1. Basic Config (checked), 2. Authentication Config (active), 3. Interesting Traffic Config, and 4. Config Verification. The Authentication Config step includes the following fields:

- * Peer Address: 2.1.1.2 (with a clear button) and a Ping button.
- * Outbound Interface: Ge0/2 (dropdown menu).
- * Authentication Mode: Pre-shared Key (selected with a radio button).
- * Key: [Redacted]
- * Confirm Key: [Redacted]

At the bottom of the form are three buttons: Previous, Cancel, and Next (highlighted in blue).

- b After completing the configuration, click **Next**.
- (3) Configure interesting traffic.
 - a Click **Create**. Configure parameters for interesting traffic according to the following figure.

Basic Config Authentication Config **Interesting Traffic Config** Config Verification

<input type="checkbox"/>	Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/>	Subnet-to-Sub...	100.100.70.0/24	200.200.30.0/24	Edit Delete

/ Page Total:1
 Go to

- b After completing the configuration, click **Next**.
- (4) Verify configuration.
 - a After verifying the configuration, click **Finish**.

✓ ✓ ✓ 4
 Basic Config Authentication Config Interesting Traffic Config **Config Verification**

I will be added to the custom tunnel list.

Basic Config [Edit](#)

Tunnel Interface

Tunnel Name

Scenario Point-to-Point ⓘ Point-to-Multipoint ⓘ

Authentication Config [Edit](#)

Peer Address

Outbound Interface

Authentication Mode Pre-shared Key

Key

Interesting Traffic Config [Edit](#)

Local Network	Peer Network
100.100.70.0/24	200.200.30.0/24

Advanced Settings [Expand](#)

6. Manually Configuring a Tunnel

- Configuring the Hub Site

(1) Configure a tunnel interface.

- a Choose **Network > Interface > Tunnel Interface**.
- b On the page that is displayed, click **Create**.
- c On the tunnel interface configuration page that is displayed, configure parameters as follows:
 - Set **Interface Name** to **test1**.
 - Add security zone **VTI** and set **Security Zone** to **VTI** for this interface.
 - Set **Tunnel Local Address** to the default outbound interface address of the hub site: 2.1.0.1. Set **Tunnel Remote Address** to **Dynamic**.

< Back **Create Tunnel Interface Details**

* Interface Name

Security Zone [+ Add Security Zone](#)

* Tunnel Local Address

Tunnel Remote Address IP Dynamic

Description

(2) Configure an IPsec tunnel.

- a Perform basic configuration.

Choose **Network > IPsec VPN > Custom Tunnel**. Click **Create**. On the basic configuration page of the custom tunnel, configure parameters as follows:

- o Set **Tunnel Name** to **test1**.
- o Set **Enabled State** to **Enable**.
- o Set **Tunnel Interface** to **test1**.
- o Set **Local Address** to **interface Ge0/2**.
- o For **Authentication Mode**, use the default value **Pre-shared Key**. Set both **Key** and **Confirm Key** to **ruijie123**.
- o Toggle on **Reverse Route Injection** for the hub site. For **Priority**, use the default value 5. Do not configure **Next-Hop Address**.

① ————— ② ————— ③

Basic Config Interesting Traffic Config Security Parameter Config

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

* Tunnel Name

Description

* Enabled State Enable Disable

* Tunnel Interface [⊕ Add Tunnel Interface](#)

* Authentication Mode

* Key

* Confirm Key

* Local Address Interface IP

* Local ID Type

* Local Identity

☰ Advanced

Reverse Route Injection

Next-Hop Address

* Priority

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

b Configure interesting traffic.

On the interesting traffic configuration page, click **Create**. Then configure parameters as follows:

- o Set **Proxy Mode** to **Auto**.

Basic Config Interesting Traffic Config Security Parameter Config

Enter the keyword.

<input type="checkbox"/>	Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/>	Auto	any	any	Edit Delete

After completing the configuration for interesting traffic, click **Next**.

c Configure security parameters.

On the security parameter configuration page, configure IKE and IPsec parameters and ensure that the configuration matches that on the peer device.

- o IKE parameters: Set **Negotiation Mode** to **IKEv1 Aggressive Mode**, **Encryption Algorithm** to **AES-128**, **Verification Algorithm** to **SHA**, **DH Group** to **GROUP5**, and **SA Lifetime** to 604800 (in seconds).
- o IPsec parameters: Set **Protocol** to **ESP**, **Encapsulation Mode** to **Tunnel**, **Encryption Algorithm** to **AES-128**, and **Verification Algorithm** to **SHA**. Do not toggle on **Perfect Forward Secrecy**. Set **SA Lifetime** to 604800 (in seconds) and **Tunnel MTU** to 1400.

Basic Config Interesting Traffic Config Security Parameter Config

IKE Parameter

* Negotiation Mode ▾

* Encryption Algorithm ▾

* Verification Algorithm ▾

* DH Group ▾

* SA Lifetime Second

IPsec Parameter

* Protocol ▾

* Encapsulation Mode ▾

* Encryption Algorithm ▾

* Verification Algorithm ▾

Perfect Forward Secrecy

* SA Lifetime Second

Tunnel MTU

Click **Finish** to complete the IPsec tunnel configuration for the hub site.

(3) Configure advanced IPsec settings.

On a network with NAT, enable NAT traversal for IPsec, and configure the NAT keep-alive interval.

Choose **Network > IPsec VPN > Advanced Settings Details**. On the advanced IPsec settings page, verify that NAT traversal is enabled, configure a proper NAT keep-alive interval, and click **Save**.

Advanced Settings Details

NAT traversal

* ⓘ NAT Keep-Alive Interval Second

ⓘ Anti-Replay Attack

Anti-Replay Window ▾

Action Specified by DF Bit ▾

(4) Create security policies.

- a Choose **Policy > Security Policy > Security Policy**.
- b On the page that is displayed, click **Create** and create outbound security policy **VPN-hub-outbound** and inbound security policy **VPN-hub-inbound** separately.

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

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

< Back

Create Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group ⊕ Add Group

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

- Configuring Spoke A
 - (1) Configure a tunnel interface.
 - a Choose **Network > Interface > Tunnel Interface**.
 - b On the page that is displayed, click **Create**.
 - c On the tunnel interface configuration page that is displayed, configure parameters as follows:
 - Set **Interface Name** to **out**.
 - Add security zone VTI and set **Security Zone** to **VTI** for this interface.
 - Set **Tunnel Local Address** to the default outbound interface address of Site A: 2.1.0.2.
 - Set **Tunnel Remote Address** to the default outbound interface address of the hub site: 2.1.1.2.

[Back](#) **Create Tunnel Interface Details**

* Interface Name

Security Zone [Add Security Zone](#)

* Tunnel Local Address

Tunnel Remote Address IP Dynamic

Description

(2) Configure an IPsec tunnel.

- a Perform basic configuration.

Choose **Network > IPsec VPN > Custom Tunnel**. Click **Create**. On the basic configuration page of the custom tunnel, configure parameters as follows:

- o Set **Tunnel Name** to **to_71**.
- o Set **Enabled State** to **Enable**.
- o Set **Tunnel Interface** to **out**.
- o Set **Local Address** to 2.1.0.2, and **Peer Address** to 2.1.1.2.
- o For **Authentication Mode**, use the default value **Pre-shared Key**. Set both **Key** and **Confirm Key** to **ruijie123**.

1 ————— 2 ————— 3
Basic Config Interesting Traffic Config Security Parameter Config

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

* Tunnel Name

Description

* Enabled State Enable Disable

* Tunnel Interface ⓘ Add Tunnel Interface

* Authentication Mode

* Key

* Confirm Key

* Local Address Interface ⓘ IP ⓘ

* Peer Address

* Local ID Type

* Local Identity

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

b Configure interesting traffic.

On the interesting traffic configuration page, click **Create**. Then configure parameters as follows:

- o Set **Proxy Mode** to **Subnet-to-Subnet**.
- o Set **Local Network** to 100.100.70.0/24 and **Peer Network** to 200.200.30.0/24.

✓ ————— 2 ————— 3
Basic Config **Interesting Traffic Config** Security Parameter Config

ⓘ

<input type="checkbox"/>	Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/>	Subnet-to-Subnet	100.100.70.0/24	200.200.30.0/24	Edit Delete

After completing the configuration for interesting traffic, click **Next**.

c. Configure security parameters.

On the security parameter configuration page, configure IKE and IPsec parameters and ensure that the configuration matches that on the peer device.

- o IKE parameters: Set **Negotiation Mode** to **IKEv1 Aggressive Mode**, **Encryption Algorithm** to **AES-128**, **Verification Algorithm** to **SHA**, **DH Group** to **GROUP5**, and **SA Lifetime** to 604800 (in seconds).
- o IPsec parameters: Set **Protocol** to **ESP**, **Encapsulation Mode** to **Tunnel**, **Encryption Algorithm** to **AES-128**, and **Verification Algorithm** to **SHA**. Do not toggle on **Perfect Forward Secrecy**. Set **SA Lifetime** to 604800 (in seconds) and **Tunnel MTU** to 1400.

IKE Parameter

- * Negotiation Mode: IKEv1 Aggressive Mode
- * Encryption Algorithm: AES-128
- * Verification Algorithm: SHA
- * DH Group: GROUP5
- * SA Lifetime: 604800 Second

IPsec Parameter

- * Protocol: ESP
- * Encapsulation Mode: Tunnel
- * Encryption Algorithm: AES-128
- * Verification Algorithm: SHA
- Perfect Forward Secrecy:
- * SA Lifetime: 604800 Second

Click **Finish** to complete the configuration for the IPsec tunnel.

(3) Configure advanced IPsec settings.

On a network with NAT, enable NAT traversal for IPsec, and configure the NAT keep-alive interval.

Choose **Network > IPsec VPN > Advanced Settings Details**. On the advanced IPsec settings page, verify that NAT traversal is enabled, configure a proper NAT keep-alive interval, and click **Save**.

Advanced Settings Details

NAT traversal

* NAT Keep-Alive Interval Second

Anti-Replay Attack

Anti-Replay Window

Action Specified by DF Bit

(4) Create security policies.

- a Choose **Object > Address > IPv4 Address**.
- b On the page that is displayed, click **Create** to create two address objects **test1_local** and **test1_remote** separately. Set **IP Address/Range** to local network address 100.100.70.0/24 and peer network address 200.200.30.0/24 in the interesting traffic for the two address objects, respectively.

IPv4 Address				
IPv6 Address				
IPv4 Address Group				
IPv6 Address Group				
<input type="button" value="Create"/>	<input type="button" value="Delete"/>	<input type="button" value="Refresh"/>		
<input type="checkbox"/>	Name	IP Address/Range	Address Group	Descr
<input type="checkbox"/>	test1_remote	200.200.30.0/24	-	by tunnel
<input type="checkbox"/>	test1_local	100.100.70.0/24	-	by tunnel

- c Choose **Policy > Security Policy > Security Policy**.
- d On the page that is displayed, click **Create** and create outbound security policy **test1_out** and inbound security policy **test1_in** separately.

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

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

< Back **Edit Security Policy**

Basic Info
* Name
Enabled State Enable Disable
* Policy Group ⊕ Add Group
Description

Src. and Dest.
* Src. Security Zone
* Src. Address
User/User Group
* Dest. Security Zone
* Dest. Address

Service
Service

(5) Configure a static route.

- a Choose **Network > Routing > Static Routing > IPv4**.
- b Click **Create** and create a static route to the peer protected subnet of the VPN.

< Back
Edit Static Routing

IP Type IPv4

* Dest. IP Range/Mask

Next-Hop Address

Interface

* ⓘ Priority

Link Detection

Description

7. Verification

- Verifying Configuration of the Hub Site

Choose **Network > IPsec VPN > Tunnel Monitoring**. On the page that is displayed, check tunnel establishment and status information.

Tunnel Monitoring

Start
 Stop
 Refresh
 Custom Field

Enter a tunnel name. Q

Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Operation
test1	-	Point-to-Multipoint	0.0.0.0	-	-	
test1	● Established	Instance Link	2.1.1.1	200.200.30.0/24->100.100.70.0/24	1493	Stop

- Verifying Configuration of Spoke A

Choose **Network > IPsec VPN > Tunnel Monitoring**. On the page that is displayed, check tunnel establishment and status information.

Tunnel Monitoring

Start
 Stop
 Refresh
 Custom Field

Enter a tunnel name. Q

Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Operation
to_71	● Established	Point-to-Point	2.1.1.2	100.100.70.0/24->200.200.30.0/24		Stop

8.25.9 Configuration Examples of IPsec VPN Networking with Link Redundancy

1. Applicable Products and Versions

Table 8-33 Products and Versions

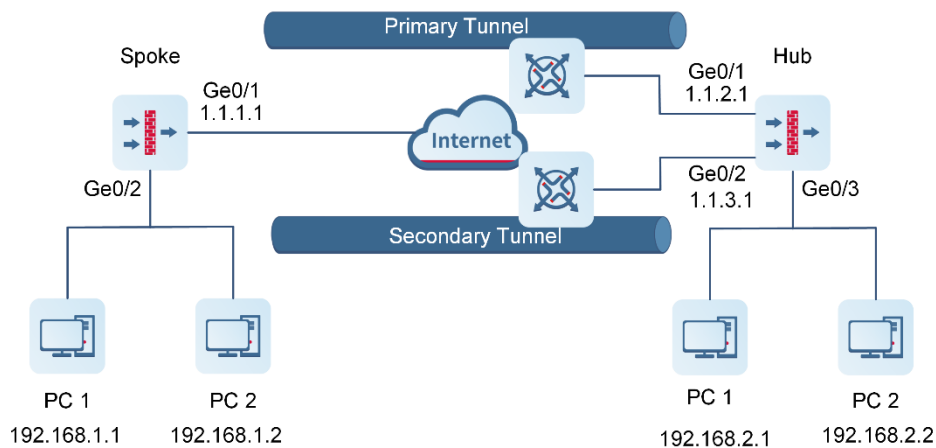
Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R6P2 or later

2. Service Demands

Typically, multiple physical links need to be deployed to ensure high reliability of IPsec VPN tunnels and prevent service interruption caused by single point of failures (SPOFs) of links. In this case, if a link is disconnected, the IPsec VPN tunnel can automatically switch to another link through Dead Peer Detection (DPD).

As shown in the following figure, the hub site accesses the Internet through two links in active/standby mode, and both the active and standby outbound interfaces are configured with fixed public IP addresses. The spoke site accesses the Internet through one link, and the outbound interface is configured with a fixed public IP address.

Figure 8-25 IPsec VPN Networking with Link Redundancy



3. Restrictions and Guidelines

- When RG-WALL 1600 serves as the IPsec VPN hub site, all spoke sites must use the same pre-shared key to negotiate with the hub site.

4. Prerequisites

You have completed basic network configurations for the two sites, including interface IP addresses and default routes. Pay attention to the following points during configuration:

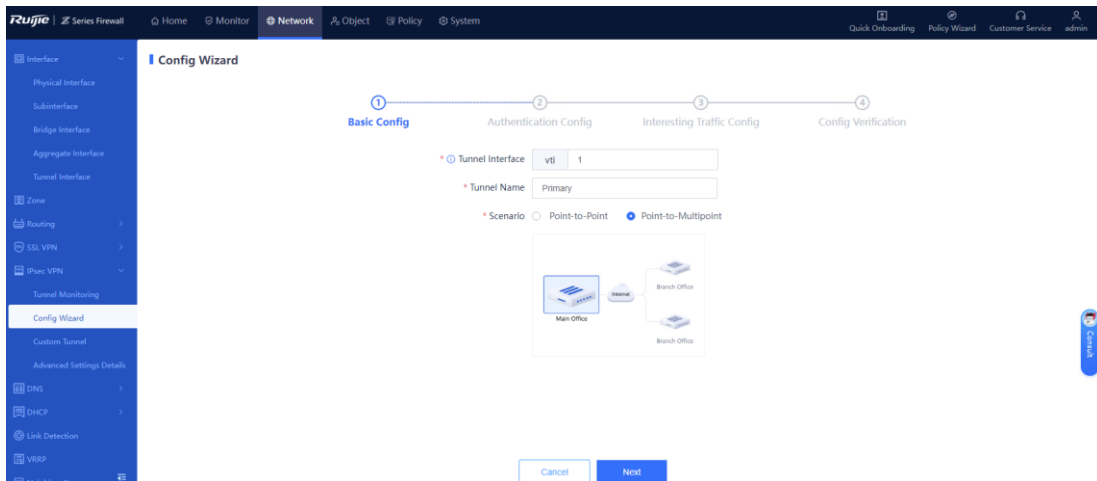
- The IP address of the hub site is fixed.
- All spoke sites can obtain the pre-shared key configured on the hub site in OOB mode.

5. Using a Configuration Wizard

- Configuring the Primary Tunnel for the Hub Site

(1) Performing Basic Configuration

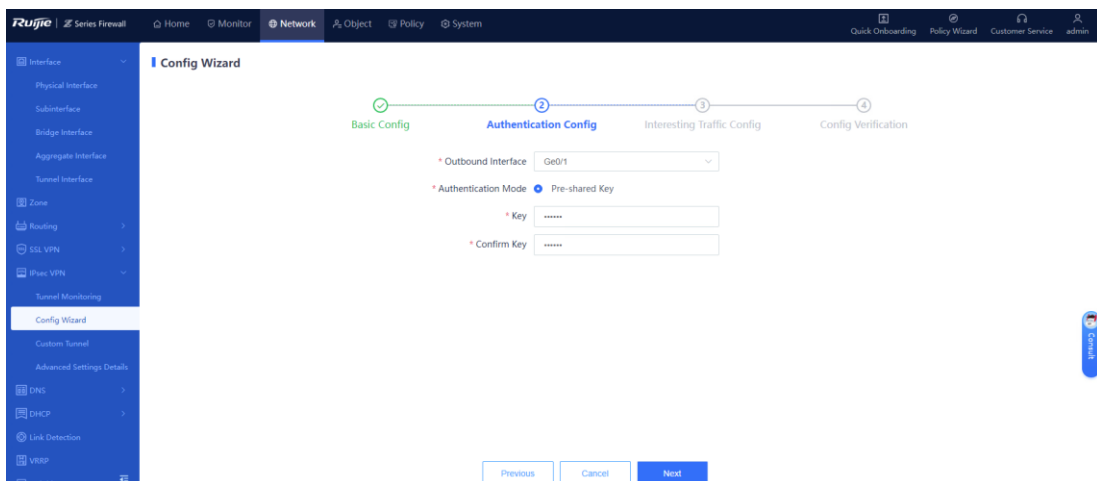
- Choose **Network > IPsec VPN > Config Wizard**. The basic configuration page of the configuration wizard is displayed.
- Set **Scenario** to **Point-to-Multipoint**, and set the other parameters according to the following figure.



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

(2) Configuring Authentication

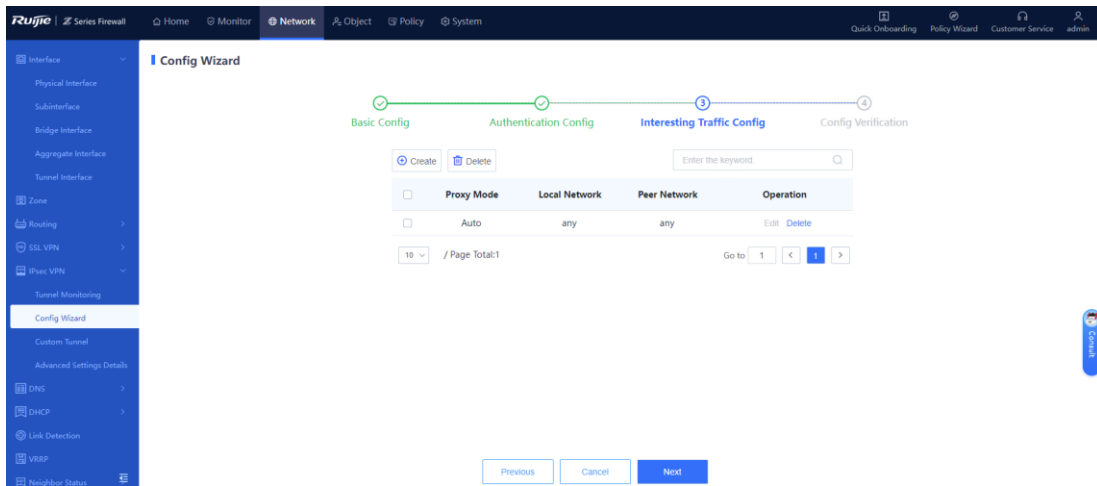
- Configure parameters according to the following figure.



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

(3) Configuring Interesting Traffic

- Click **Create**. Configure parameters for interesting traffic according to the following figure.



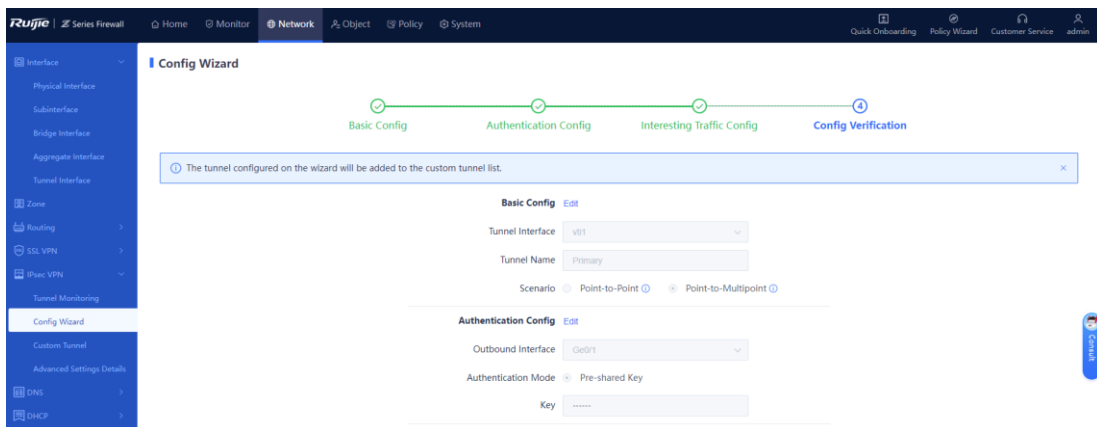
b After completing the configuration, click **Next**.

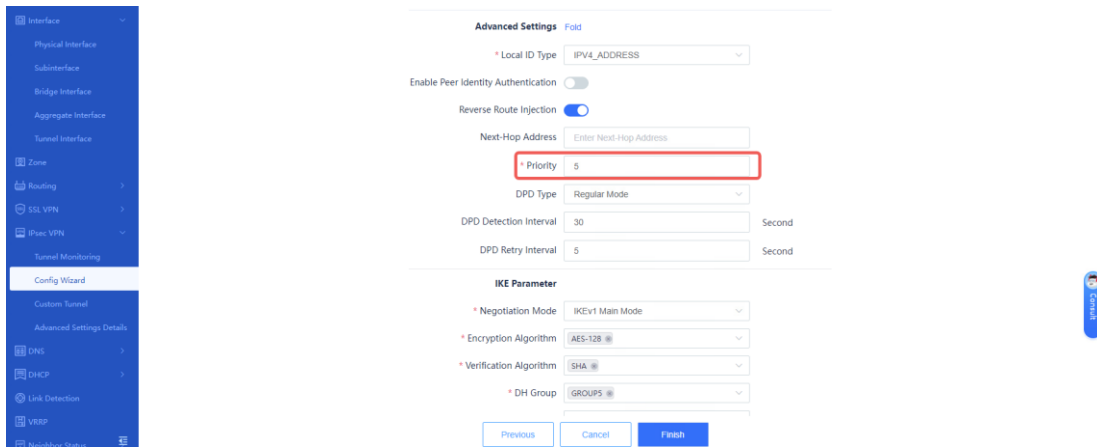
(4) Verifying Configuration

a Verify that the priority of the reverse route of the primary IPsec VPN tunnel is higher than that of the secondary tunnel. In this example, the reverse route priority value of the primary tunnel is set to 5. (A larger value indicates a lower priority.)

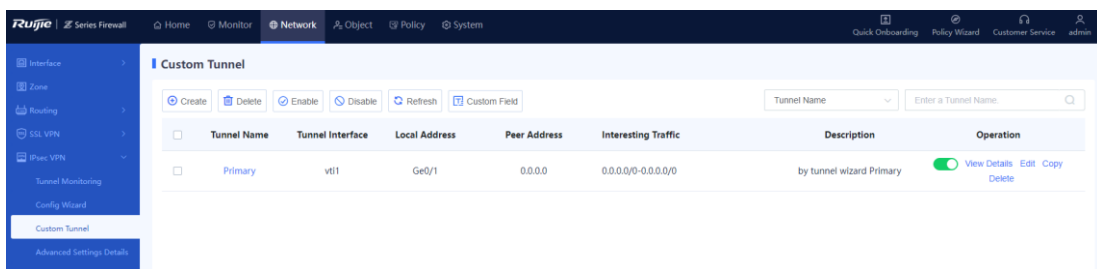
Caution

NTOS IPsec VPN is implemented based on routing. The primary and secondary tunnels are determined by the route priority of the interesting traffic. Therefore, you need to modify the priority of the reverse route of the secondary tunnel to ensure that it is lower than that of the primary tunnel.





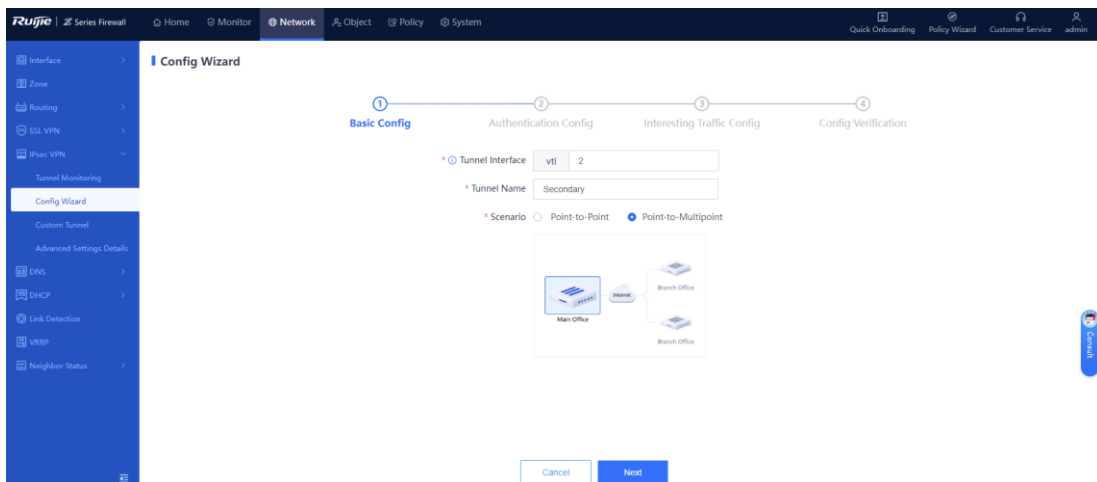
b After verifying the configuration, click **Finish**.



- Configuring the Secondary Tunnel for the Hub Site

(1) Performing Basic Configuration

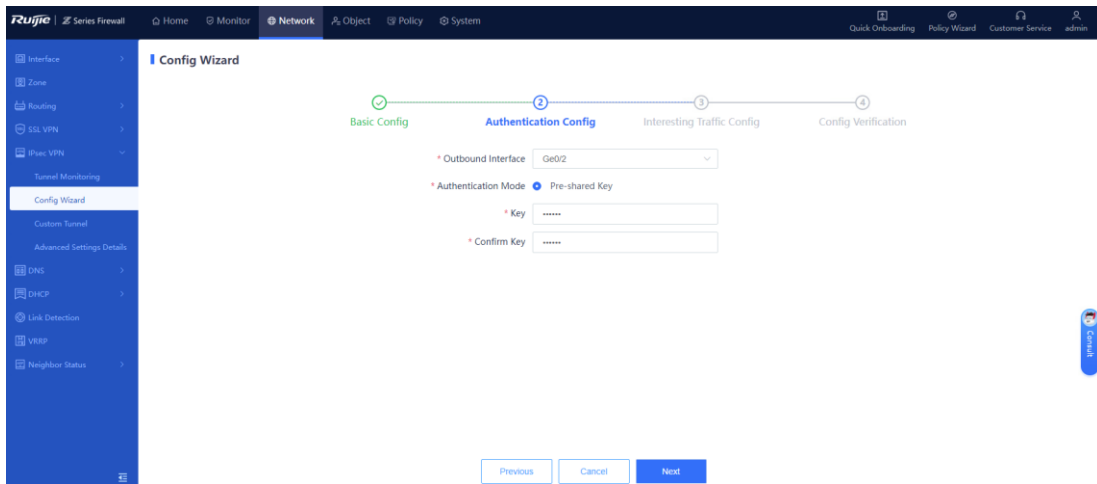
- a Choose **Network > IPsec VPN > Config Wizard**. The basic configuration page of the configuration wizard is displayed.
- b Set **Scenario** to **Point-to-Multipoint**, and set the other parameters according to the following figure.



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

(2) Configuring Authentication

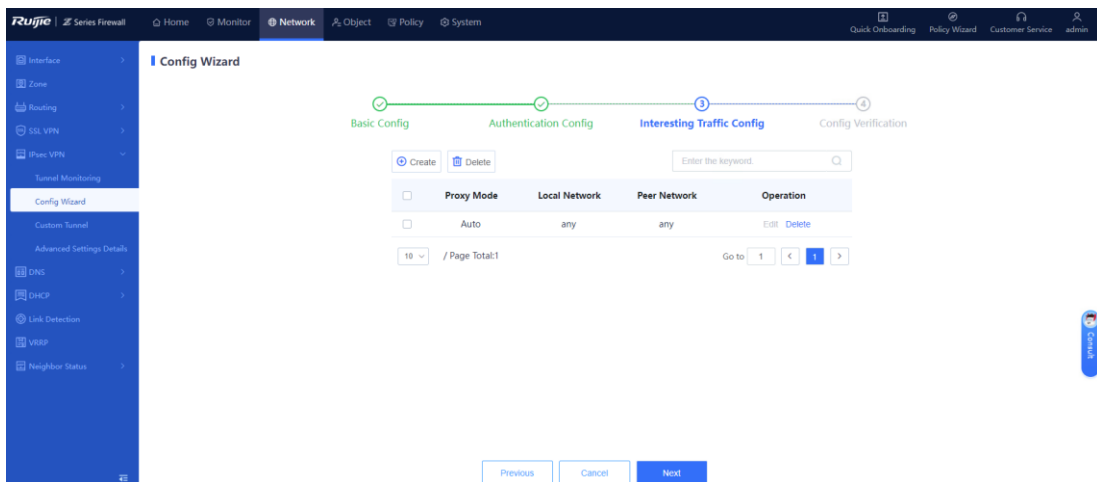
- a Configure parameters according to the following figure.



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

(3) Configuring Interesting Traffic

a Click **Create**. Configure parameters for interesting traffic according to the following figure.



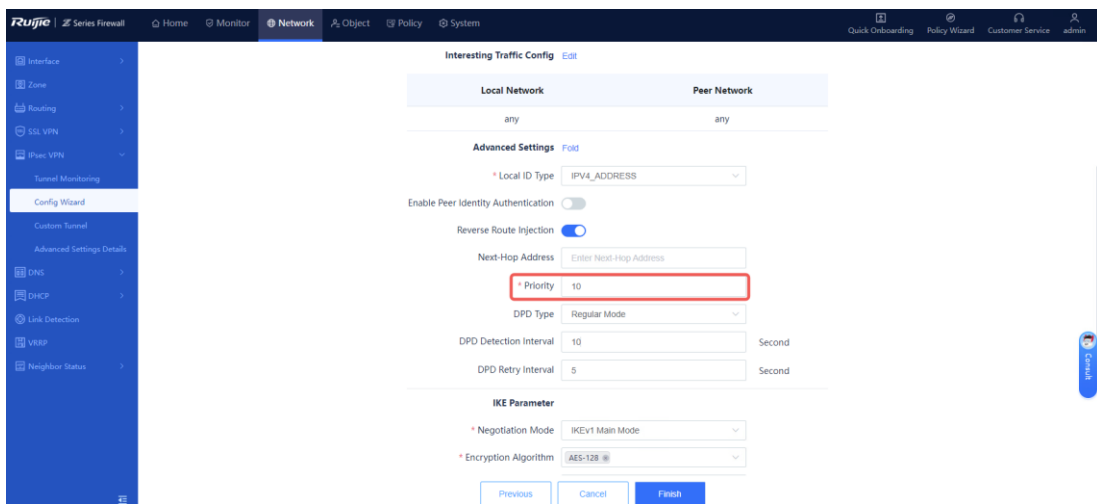
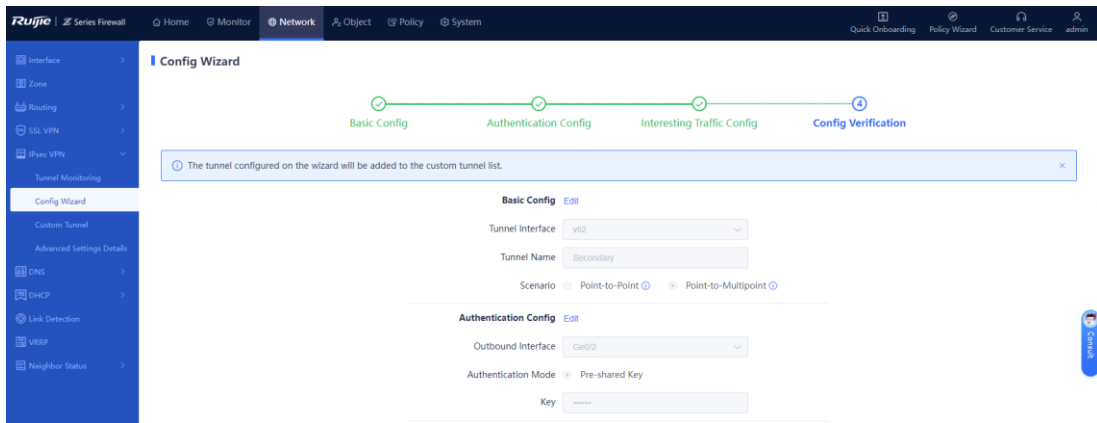
b After completing the configuration, click **Next**.

(4) Verifying Configuration

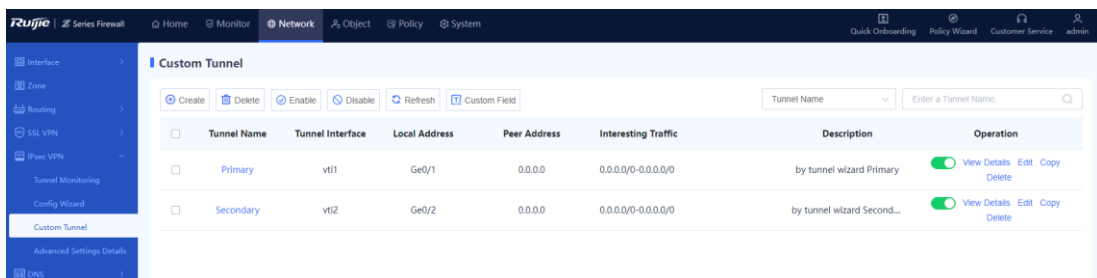
a Verify that the priority of the reverse route of the secondary IPsec VPN tunnel is lower than that of the primary tunnel. In this example, the reverse route priority value of the secondary tunnel is set to 10. (A larger value indicates a lower priority.)

Caution

NTOS IPsec VPN is implemented based on routing. The primary and secondary tunnels are determined by the route priority of the interesting traffic. Therefore, you need to modify the priority of the reverse route of the secondary tunnel to ensure that it is lower than that of the primary tunnel.



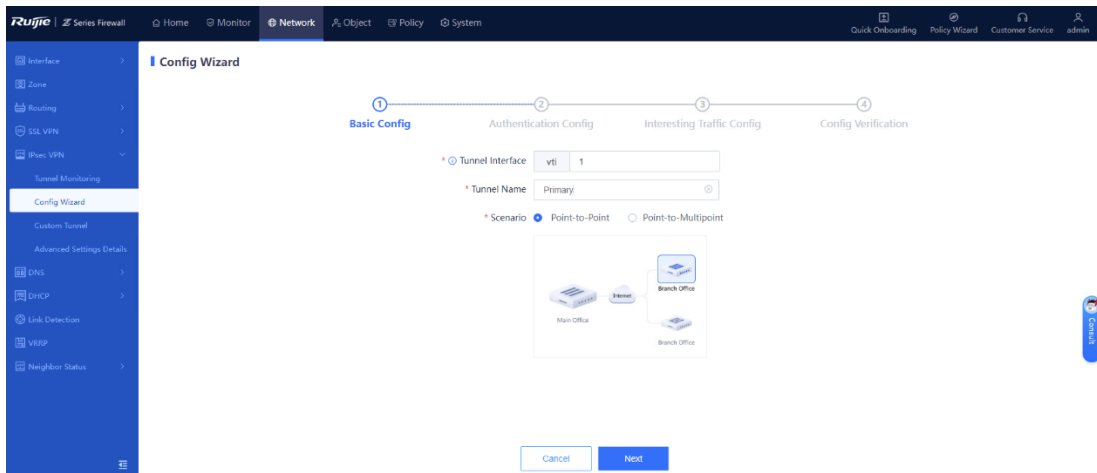
b After verifying the configuration, click **Finish**.



- Configuring the Primary Tunnel for the Spoke Site

- (1) Performing Basic Configuration

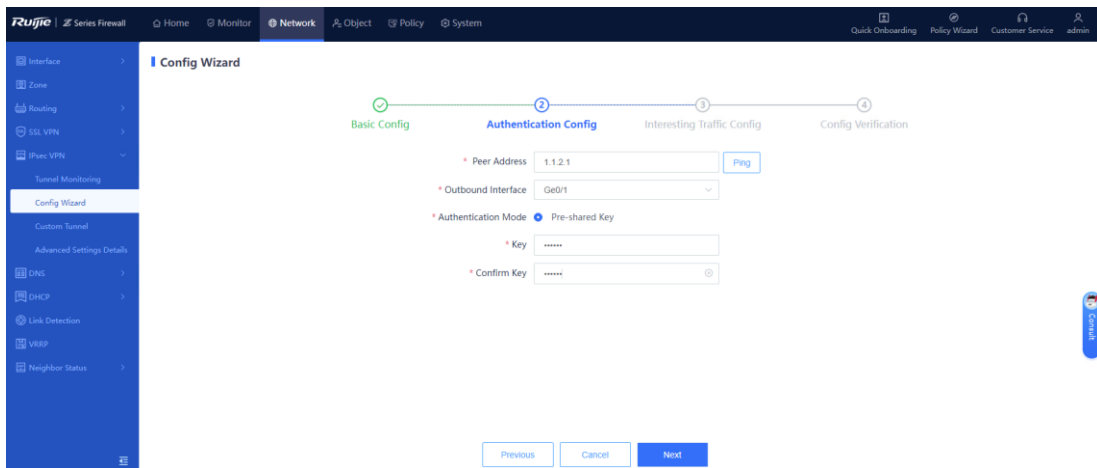
- a Choose **Network > IPsec VPN > Config Wizard**. The basic configuration page of the configuration wizard is displayed.
- b Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.



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

(2) Configuring Authentication

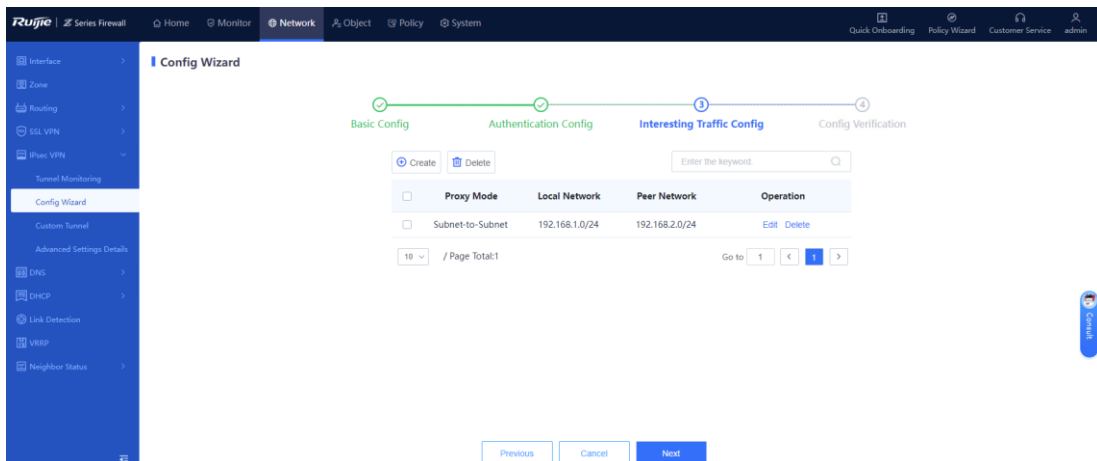
a Configure parameters according to the following figure.



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

(3) Configuring Interesting Traffic

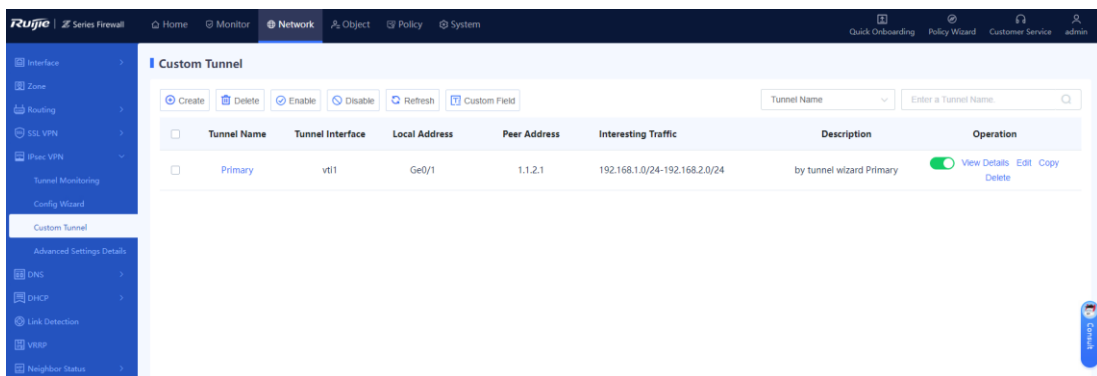
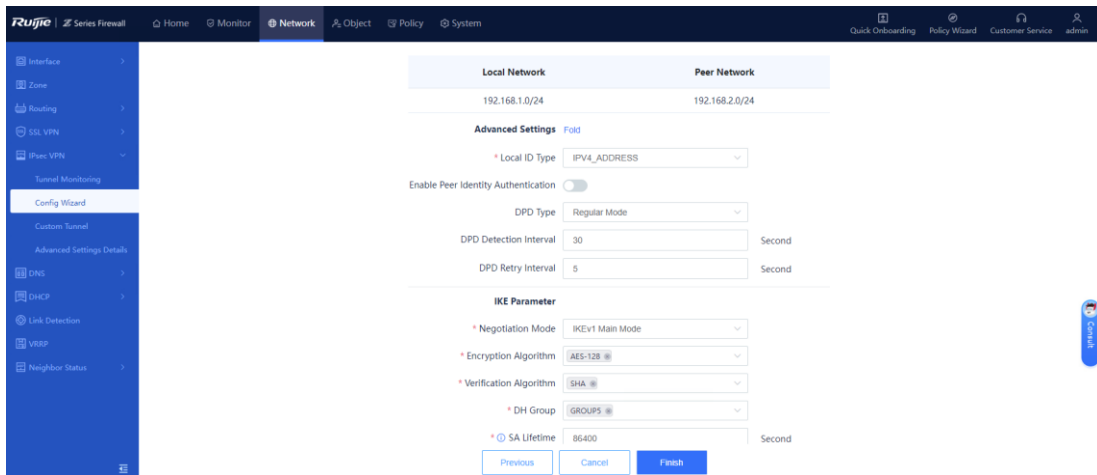
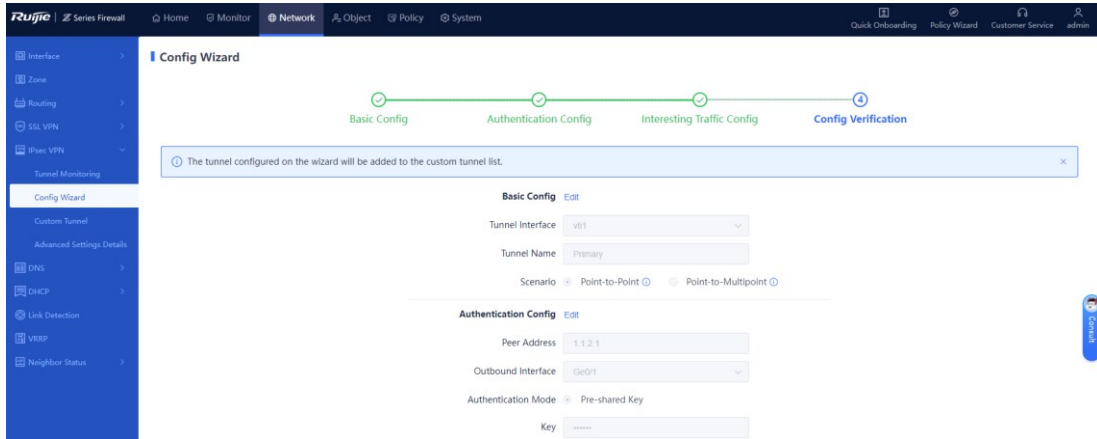
a Click **Create**. Configure parameters for interesting traffic according to the following figure.



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

(4) Verifying Configuration

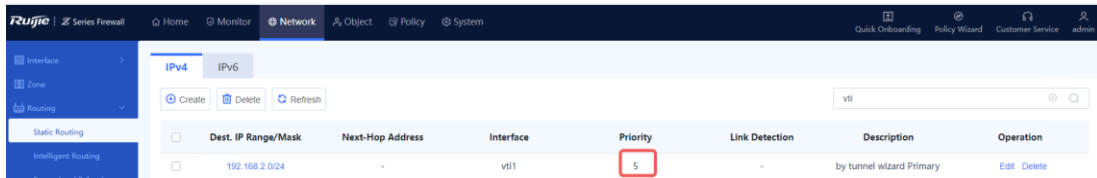
a After verifying the configuration, click **Finish**.



b When you create a primary tunnel using the wizard, a static route is automatically created based on the destination subnet of the interesting traffic. The outbound interface is **vt1** and the priority value is 5 by default.

⚠ Caution

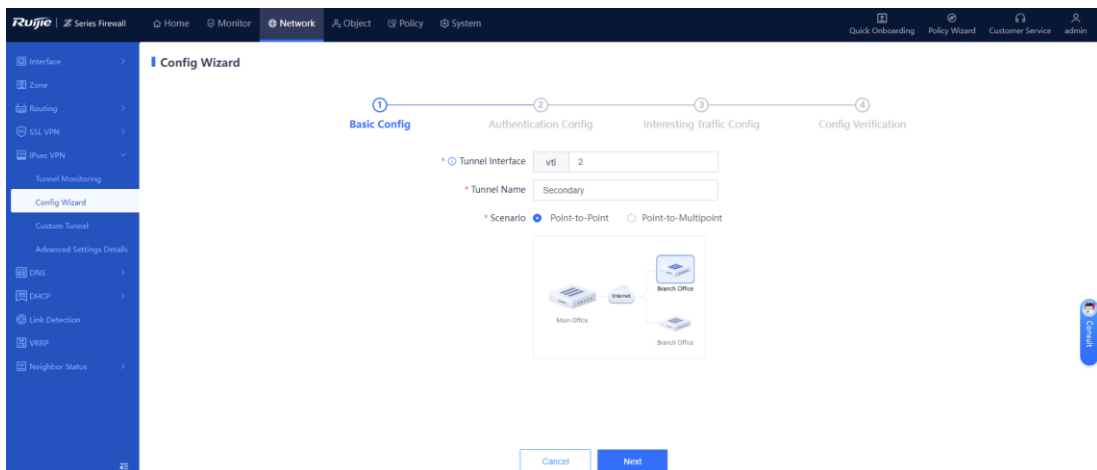
NTOS IPsec VPN is implemented based on routing. The primary and secondary tunnels are determined by the route priority of the interesting traffic. Therefore, you need to modify the priority of the route of the secondary tunnel to ensure that it is lower than that of the primary tunnel.



- Configuring the Secondary Tunnel for the Spoke Site

(1) Performing Basic Configuration

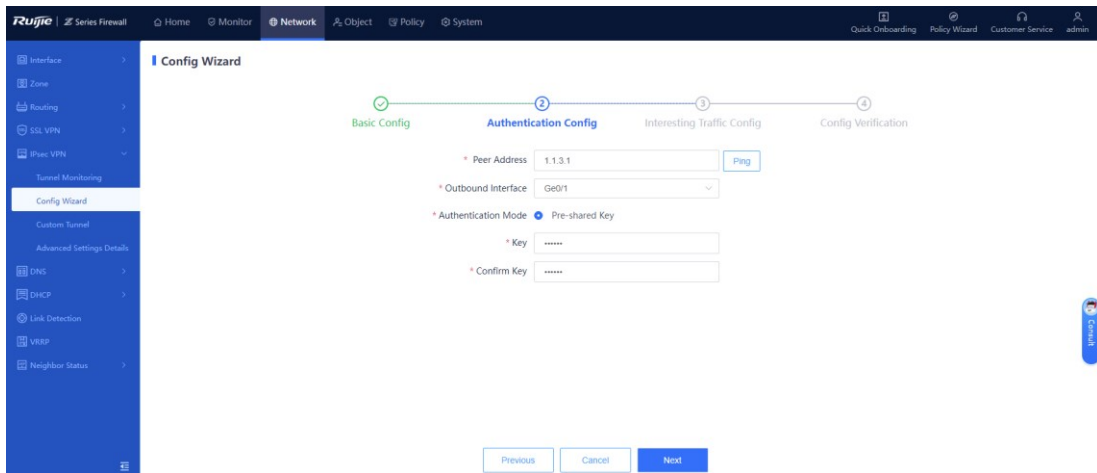
- Choose **Network > IPsec VPN > Config Wizard**. The basic configuration page of the configuration wizard is displayed.
- Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.



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

(2) Configuring Authentication

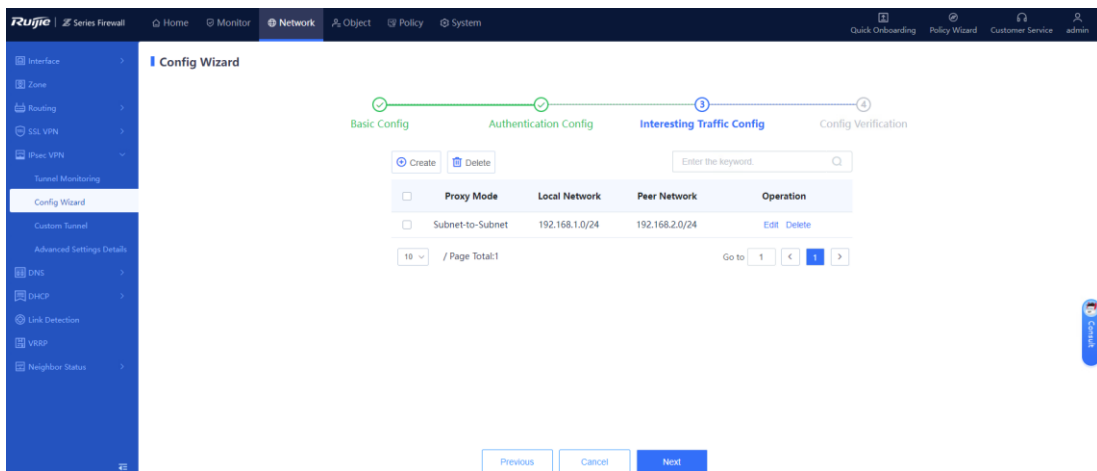
- Configure parameters according to the following figure.



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

(3) Configuring Interesting Traffic

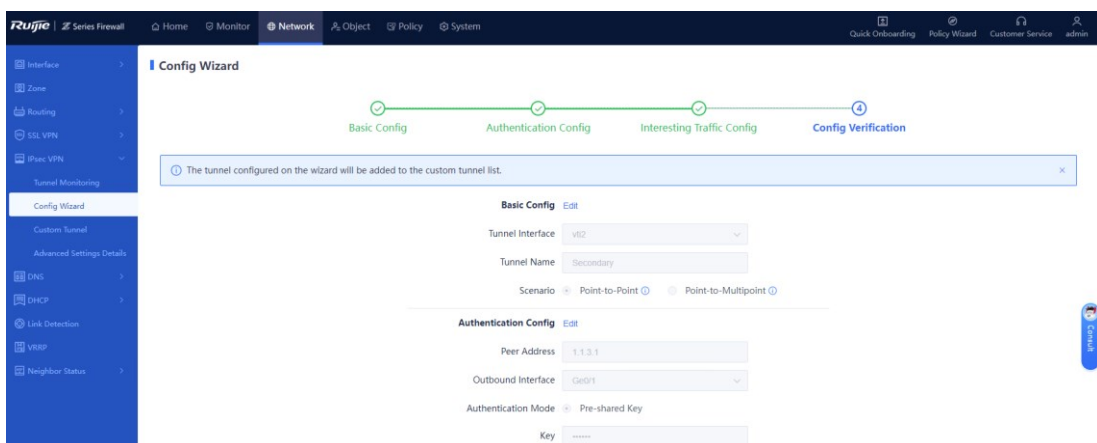
a Click **Create**. Configure parameters for interesting traffic according to the following figure.

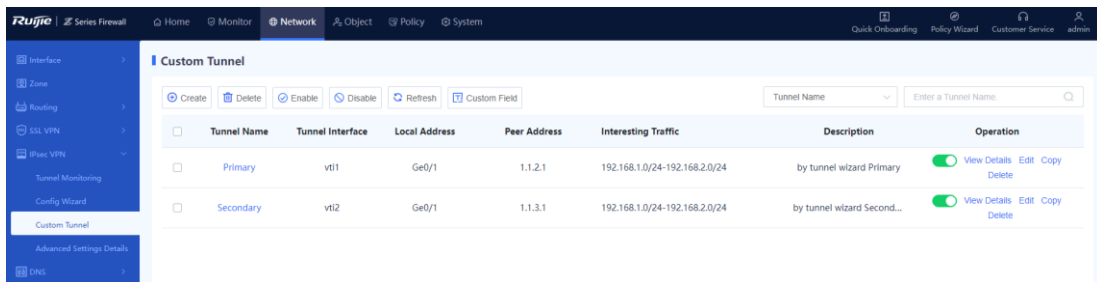
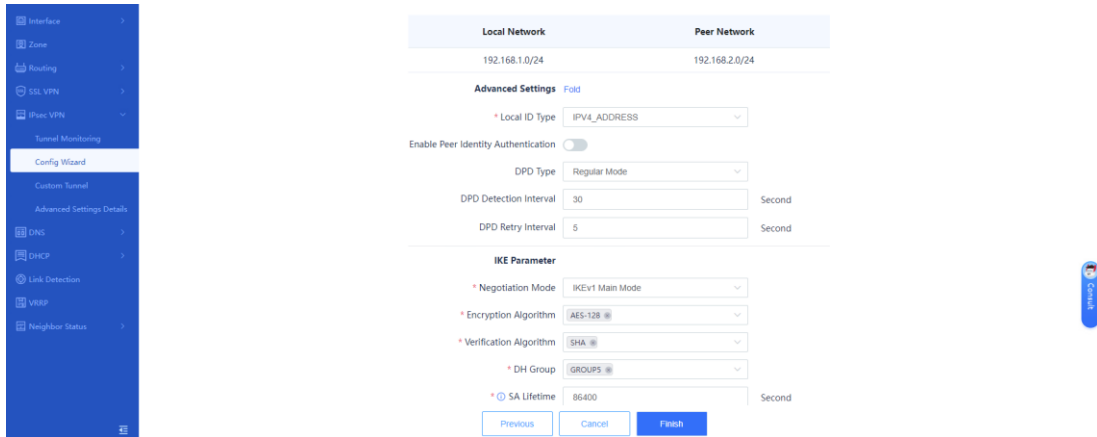


b After completing the configuration, click **Next**.

(4) Verifying Configuration

a After verifying the configuration, click **Finish**.

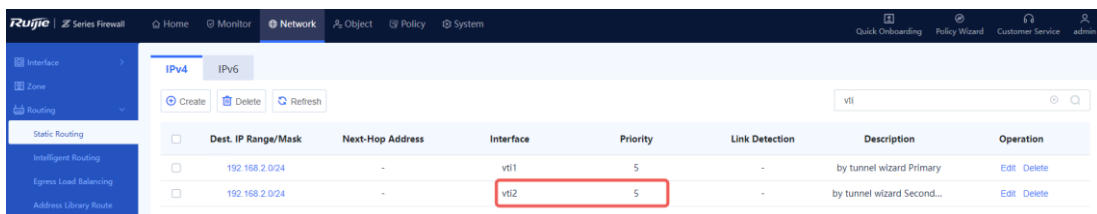


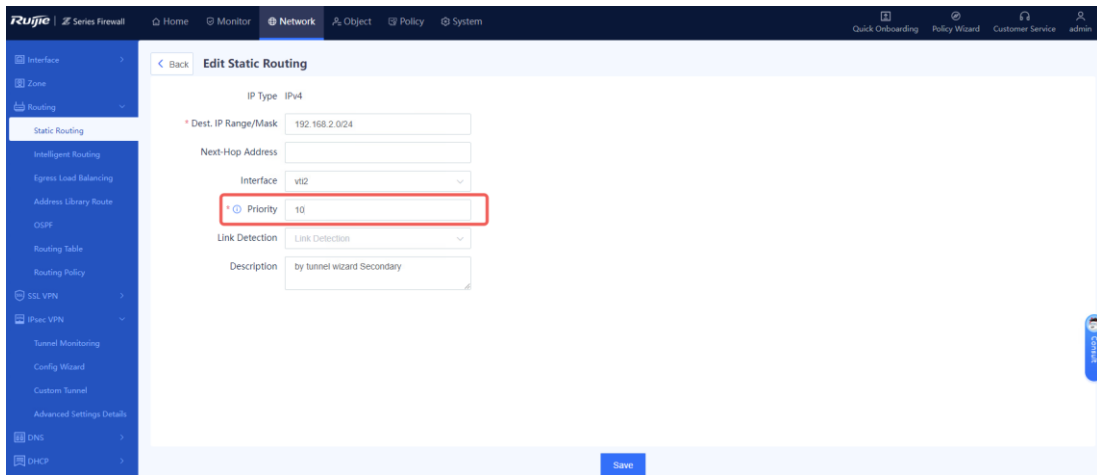


b When you create a secondary tunnel using the wizard, a static route is automatically created based on the destination subnet of the interesting traffic. The outbound interface is **vti2** and the priority value is 5 by default. Therefore, you need to lower the priority of this route by changing the value to 10. (A larger value indicates a lower priority.)

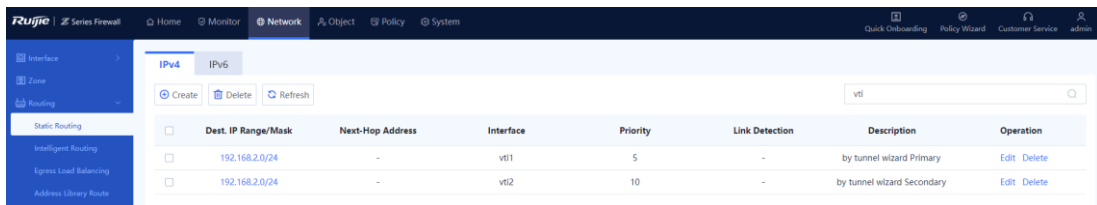
Caution

NTOS IPsec VPN is implemented based on routing. The primary and secondary tunnels are determined by the route priority of the interesting traffic. Therefore, you need to modify the priority of the route of the secondary tunnel to ensure that it is lower than that of the primary tunnel.





After the modification, the following static route configuration is displayed.

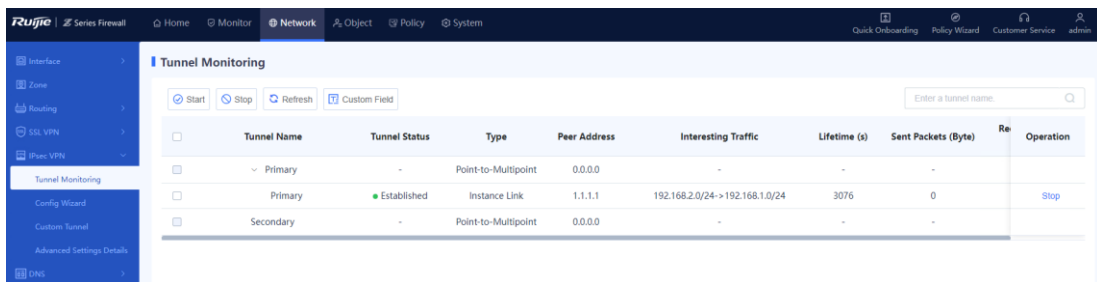


6. Verification

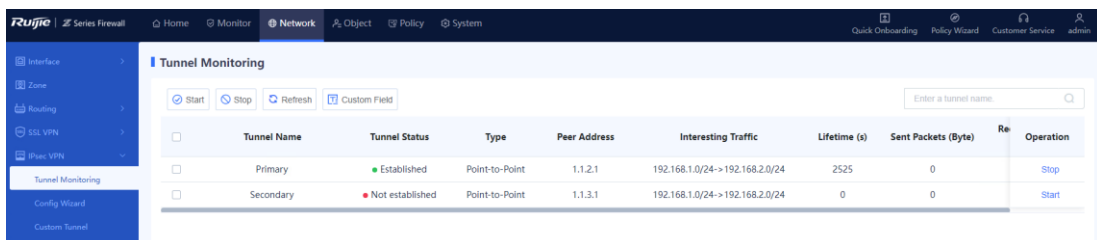
- Verifying Tunnel Establishment When the Primary Link Is Normal

After the configuration is successful, the spoke site first establishes a tunnel with the primary link address of the hub site. Check the following tunnel status.

- Checking the Tunnel Status of the Hub Site



- Checking the Tunnel Status of the Spoke Site



- Verifying Tunnel Switching When the Primary Link Is Faulty

Shut down the interface of the primary link on the hub site, and check the tunnel switching result. The primary tunnel is disconnected and the secondary tunnel is established successfully.

- Checking the Tunnel Status of the Hub Site

Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re	Operation
Primary	-	Point-to-Multipoint	0.0.0.0	-	-	-		
Secondary	-	Point-to-Multipoint	0.0.0.0	-	-	-		
Secondary	Established	Instance Link	1.1.1.1	192.168.2.0/24->192.168.1.0/24	3524	0		Stop

- Checking the Tunnel Status of the Spoke Site

Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re	Operation
Primary	Not established	Point-to-Point	1.1.2.1	192.168.1.0/24->192.168.2.0/24	0	0		Start
Secondary	Established	Point-to-Point	1.1.3.1	192.168.1.0/24->192.168.2.0/24	3476	0		Stop

- Verifying Tunnel Switchback After the Primary Link Recovers

- Checking the Tunnel Status of the Hub Site

Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re	Operation
Primary	-	Point-to-Multipoint	0.0.0.0	-	-	-		
Primary	Established	Instance Link	1.1.1.1	192.168.2.0/24->192.168.1.0/24	3076	0		Stop
Secondary	-	Point-to-Multipoint	0.0.0.0	-	-	-		

- Checking the Tunnel Status of the Spoke Site

Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re	Operation
Primary	Established	Point-to-Point	1.1.2.1	192.168.1.0/24->192.168.2.0/24	2525	0		Stop
Secondary	Not established	Point-to-Point	1.1.3.1	192.168.1.0/24->192.168.2.0/24	0	0		Start

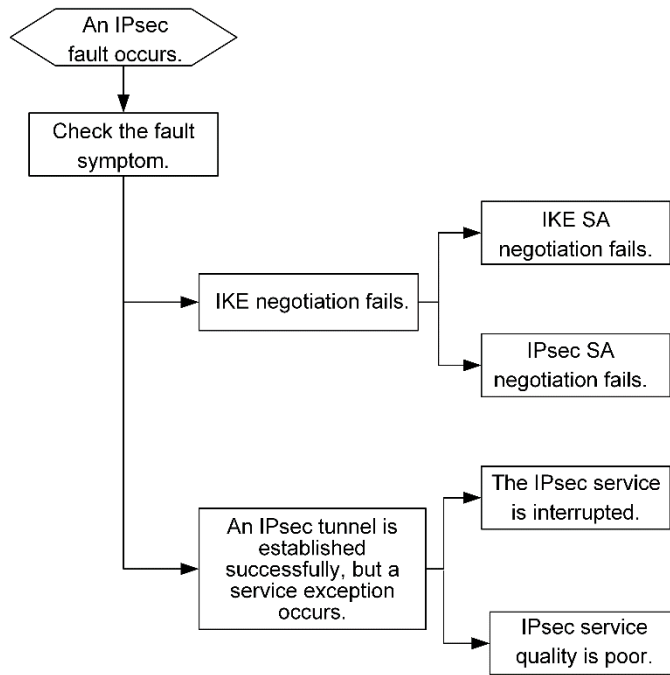
8.25.10 Common Faults and Troubleshooting Roadmaps

Common IPsec faults are as follows:

- An IPsec tunnel cannot be established. That is, IKE negotiation failed.
- An IPsec tunnel is established successfully, but a service exception occurs.

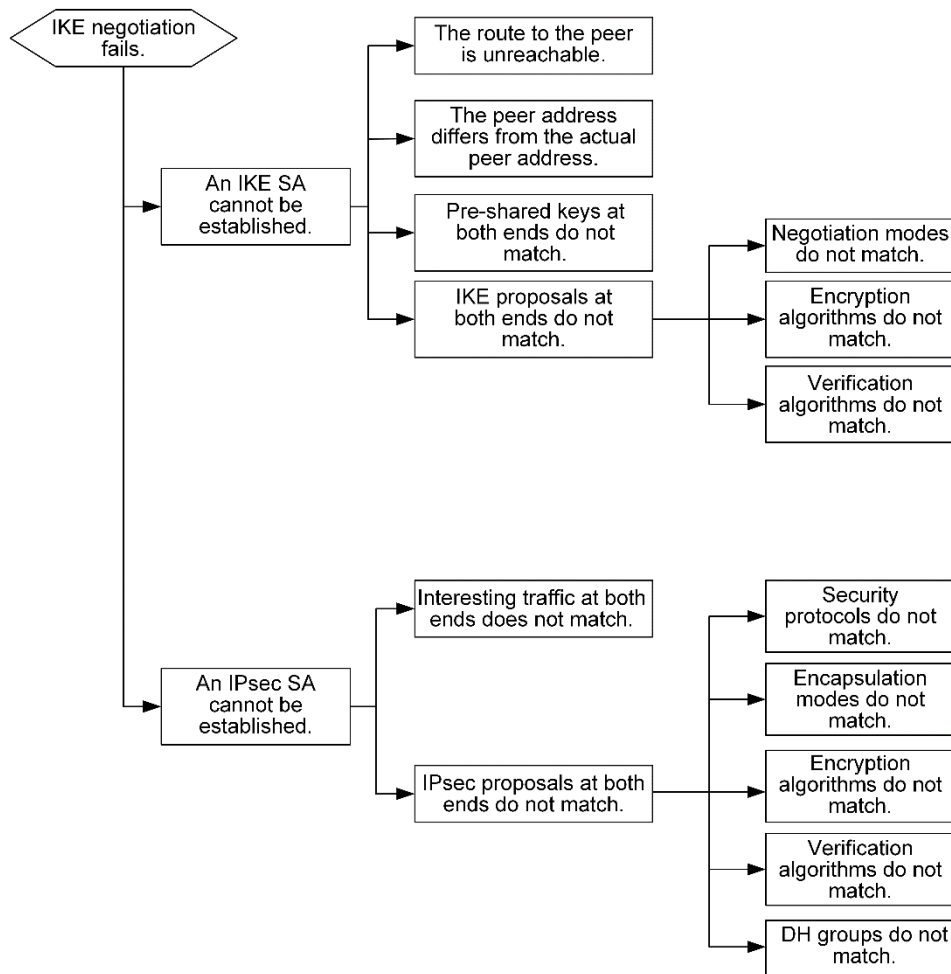
[Figure 8-26](#) shows the typical troubleshooting roadmap for IPsec faults.

Figure 8-26 Troubleshooting Roadmap for IPsec Faults



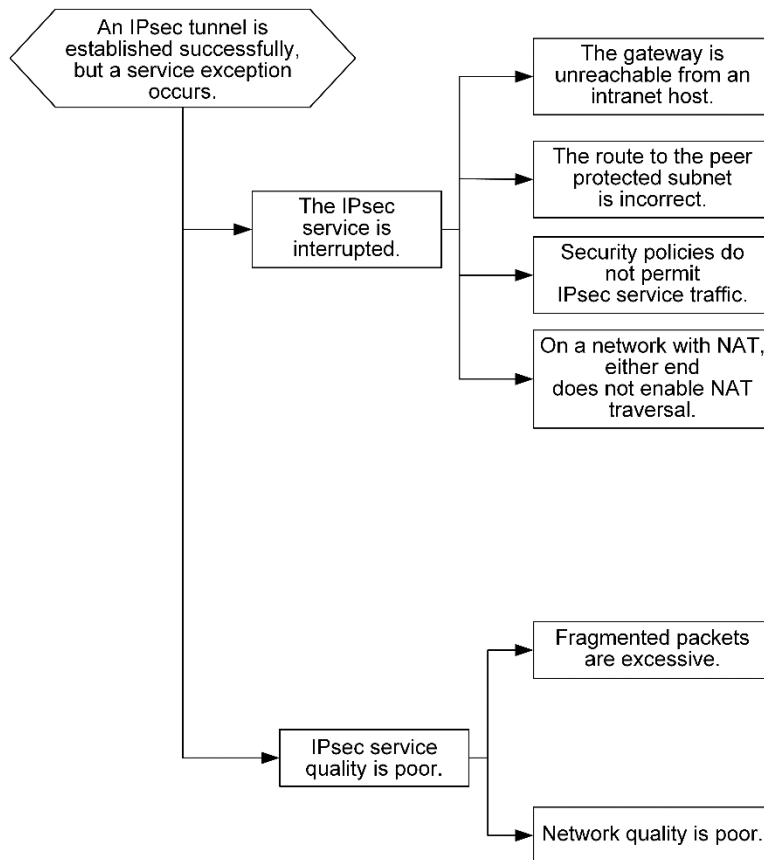
1. IKE Negotiation Failure

Figure 8-27 Troubleshooting Roadmap for IKE Negotiation Failures



2. IPsec Service Exception

Figure 8-28 Troubleshooting Roadmap for IPsec Service Exceptions



8.26 GRE VPN

8.26.1 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.

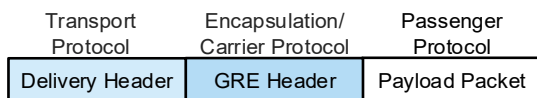
GRE tunnels transmit data in plaintext. If the data transmitted between the two ends of a tunnel needs to be encrypted, GRE over IPsec can be used.

8.26.2 Working Principle

The tunneling function includes the following three components:

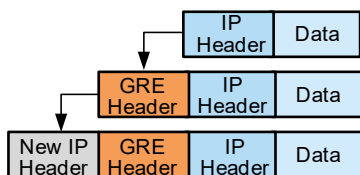
- Load protocol: Packet protocol before encapsulation, that is, the innermost tunnel protocol. IPv4 and IPv6 protocols are generally used as load protocols. For a GRE tunnel, the load protocol can be IPv4, IPv6, or MPLS.
- Carrier protocol: Encapsulation protocol, which is used for secondary encapsulation 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 8-29 GRE Packet Format



GRE encapsulates packets layer by layer based on the protocol stack. As shown in [Figure 8-30](#), 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 8-30 GRE Packet Encapsulation



8.26.3 Application Scenario

Scenario	Description
IPv4 over IPv4 GRE tunnel	Cross-region IPv4 communication over IPv4 GRE tunnels Key configurations: <ul style="list-style-type: none"> ● Configure tunnel encapsulation addresses and set other attributes based on the encapsulation security requirements. ● Configure a routing policy for IPv4 data flows to be encapsulated.
IPv6 over IPv4 GRE tunnel	Cross-region IPv6 communication over IPv4 GRE tunnels Key configurations: <ul style="list-style-type: none"> ● Configure tunnel encapsulation addresses and set other attributes based on the encapsulation security requirements. ● Enable IPv6 forwarding on GRE interfaces. ● Configure a routing policy for IPv6 data flows to be encapsulated.

Scenario	Description
GRE over IPsec	<p>Meeting both GRE networking and tunnel security requirements</p> <p>Key configurations:</p> <ul style="list-style-type: none"> ● Set the IP address of the virtual tunnel interface (VTI) of the IPsec tunnel to the local address for GRE encapsulation. ● Set the tunnel encapsulation address to the VTI address and set other attributes based on the encapsulation security requirements. ● Configure a routing policy for service data flows to be encapsulated. ● Configure the tunnel addresses of GRE encapsulation for IPsec interesting traffic.

8.26.4 Configuring an IPv4 over IPv4 GRE Tunnel

1. Applicable Products and Versions

Table 8-34 Products and Versions

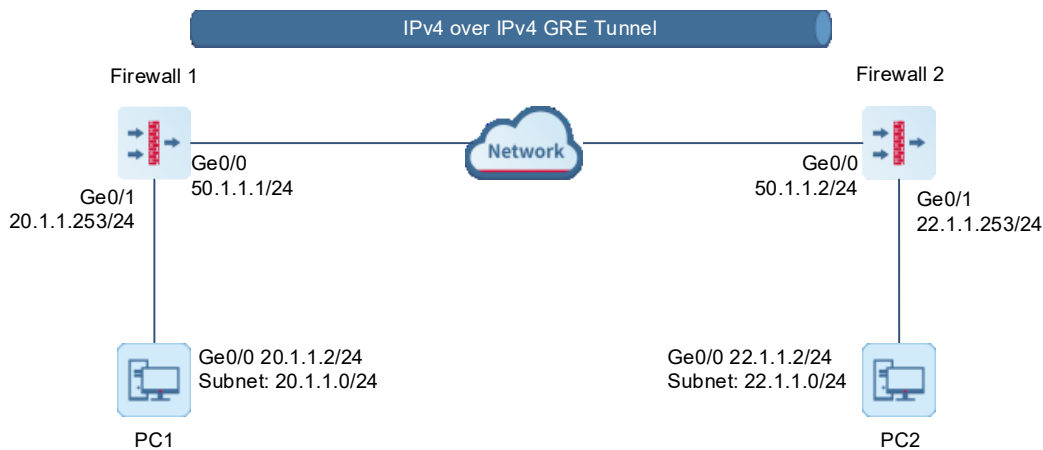
Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R7 or later

2. Service Demands

As shown in [Figure 8-31](#), both Firewall 1 and Firewall 2 have fixed public IP addresses. A GRE VPN tunnel needs to be established between the LANs where Firewall 1 and Firewall 2 reside to enable IPv4 network communication.

- Configure tunnel key values for both ends to authenticate the remote end of the GRE tunnel.
- Enable the checksum function to prevent data tampering.
- Enable the keepalive mechanism to detect whether the remote end is available. If the remote end is unavailable, the corresponding GRE interface is switched to Down to prevent data black holes.

Figure 8-31 Topology of an IPv4 over IPv4 GRE Tunnel



3. Restrictions and Guidelines

- Currently, GRE supports IPv4 tunnel encapsulation but not IPv6 tunnel encapsulation.

4. Prerequisites

You have completed basic network configurations for Firewall 1 and Firewall 2, including interface IP addresses and default routes. Pay attention to the following point during configuration:

- Ensure that Firewall 1 and Firewall 2 can communicate with each other through tunnel encapsulation IP addresses.

5. Procedure

- Configuring Firewall 1

(1) Configure a GRE interface.

- a Choose **Network > Interface > Tunnel Interface > GRE Interface**.
- b Click **Create**. On the page that is displayed, configure the following parameters for the GRE interface.

[< Back](#) **Edit GRE Interface**

Basic Info
* Interface Name
Description

Interface Config
* Interface Type
* Security Zone [Add Security Zone](#)
① Tunnel Interface Address
① IP/Mask

Tunnel Encapsulation Address
* ① Src. IPv4
* ① Dest. IPv4

Advanced Settings
① Tunnel Validity Check
① Tunnel Key Value
① Keepalive
① Keepalive Interval s
① Retransmission Times
① Tunnel MTU

Access Management
Permit HTTPS PING SSH

[Save](#)

c After completing the configuration, click **Save**.

(2) Configure a service data route.

a Choose **Network > Routing > Static Routing > IPv4**.

b Click **Create**. On the page that is displayed, add a static route.

< Back **Create Static Routing**

IP Type IPv4

* Dest. IP Range/Mask 22.1.1.0/24

Next-Hop Address

Interface greipv4

* ⓘ Priority 5

Link Detection Link Detection

Description

c After completing the configuration, click **Save**.

(3) Configure an IPv4 address pool object.

a Choose **Object > Address > IPv4 Address**. The address object configuration page is displayed.

b Click **Create**. On the page that is displayed, add a local address object.

< Back **Edit IPv4 Address Object**

Basic Info

* Name greipv4

Description

IP Address/Range

* ⓘ IP Address/Range 20.1.1.0/24

Save

c After completing the configuration, click **Save**.

d Click **Create**. On the page that is displayed, add a remote address object.

< Back **Edit IPv4 Address Object**

Basic Info

* Name greipv4-peer

Description

IP Address/Range

* ⓘ IP Address/Range 22.1.1.0/24

Save

- e After completing the configuration, click **Save**.
- (4) Configure security policies.
- a Choose **Policy > Security Policy > Security Policy**. The security policy configuration page is displayed.
 - b Click **Create**. On the page that is displayed, add a security policy for traffic from the local end to the remote end.

< Back

Edit Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Keyword Filtering Enable Disable [⊕ Add Keyword Filter](#)

Advanced

- c After completing the configuration, click **Save**.
- d Click **Create**. On the page that is displayed, add a security policy for traffic from the remote end to the local end.

< Back

Edit Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group ⊕ Add Group

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

Time Range ⊕ Add One-Off Time Plan ⊖

Action Settings

Action Option Permit Deny

Content Security

Intrusion Prevention Enable Disable ⊕ Add Intrusion Prevention Template

Virus Protection Enable Disable ⊕ Add Virus Protection Template

URL Filtering Enable Disable ⊕ Add URL Filtering

Keyword Filtering Enable Disable ⊕ Add Keyword Filter

Advanced

Settings

- e After completing the configuration, click **Save**.
- Configuring Firewall 2
 - (1) Configure a GRE interface.

- a Choose **Network > Interface > Tunnel Interface > GRE Interface**.
- b Click **Create**. On the page that is displayed, configure the following parameters for the GRE interface.

< Back
Edit GRE Interface

Basic Info

* Interface Name

Description

Interface Config

* Interface Type

* Security Zone [Add Security Zone](#)

① Tunnel Interface Address

① IP/Mask

Tunnel Encapsulation Address

* ① Src. IPv4

* ① Dest. IPv4

Advanced Settings

① Tunnel Validity Check

① Tunnel Key Value

① Keepalive

① Keepalive Interval s

① Retransmission Times

① Tunnel MTU

Access Management

Permit HTTPS PING SSH

- c After completing the configuration, click **Save**.
- (2) Configure a service data route.
- a Choose **Network > Routing > Static Routing > IPv4**.
 - b Click **Create**. On the page that is displayed, add a static route.

< Back **Create Static Routing**

IP Type IPv4

* Dest. IP Range/Mask 20.1.1.0/24

Next-Hop Address

Interface greipv4

* Priority 5

Link Detection Link Detection

Description

c After completing the configuration, click **Save**.

(3) Configure an IPv4 address pool object.

a Choose **Object > Address > IPv4 Address**. The address object configuration page is displayed.

b Click **Create**. On the page that is displayed, add a local address object.

< Back **Edit IPv4 Address Object**

Basic Info

* Name greipv4

Description

IP Address/Range

* IP Address/Range 22.1.1.0/24

c After completing the configuration, click **Save**.

d Click **Create**. On the page that is displayed, add a remote address object.

[< Back](#) **Edit IPv4 Address Object**

Basic Info

* Name greipv4-peer

Description

IP Address/Range

* ⓘ IP Address/Range 20.1.1.0/24

- e After completing the configuration, click **Save**.
- (4) Configure security policies.
- a Choose **Policy > Security Policy > Security Policy**. The security policy configuration page is displayed.
 - b Click **Create**. On the page that is displayed, add a security policy for traffic from the local end to the remote end.

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

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Keyword Filtering Enable Disable [⊕ Add Keyword Filter](#)

Advanced

- c After completing the configuration, click **Save**.
- d Click **Create**. On the page that is displayed, add a security policy for traffic from the remote end to the local end.

< Back

Edit Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Keyword Filtering Enable Disable [⊕ Add Keyword Filter](#)

Advanced

e After completing the configuration, click **Save**.

6. Verification

- Checking Interface Status

On the web UI of Firewall 1, choose **Network > Interface > Tunnel Interface > GRE Interface** and check the interface status.

VTI Interface GRE Interface ERSPAN Interface									
<input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/> <input type="text" value="Enter a name."/>									
<input type="checkbox"/>	Interface Name	Security Zone	Interface Type	Interface Status	Tunnel Interface Address	Tunnel Local Address	Tunnel Remote Address	Description	Operation
<input type="checkbox"/>	greipv4	trust	gre	UP	-	50.1.1.1	50.1.1.2	-	Edit Delete
<input type="checkbox"/>	greipv6	trust	gre	UP	-	50.1.1.1	50.1.1.2	-	Edit Delete
<input type="checkbox"/>	greipsec	trust	gre	UP	-	70.1.1.1	70.1.1.2	-	Edit Delete

On the web UI of Firewall 2, choose **Network > Interface > Tunnel Interface > GRE Interface** and check the interface status.

VTI Interface GRE Interface ERSPAN Interface									
<input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/> <input type="text" value="Enter a name."/>									
<input type="checkbox"/>	Interface Name	Security Zone	Interface Type	Interface Status	Tunnel Interface Address	Tunnel Local Address	Tunnel Remote Address	Description	Operation
<input type="checkbox"/>	greipv4	trust	gre	UP	-	50.1.1.2	50.1.1.1	-	Edit Delete
<input type="checkbox"/>	greipv6	trust	gre	UP	-	50.1.1.2	50.1.1.1	-	Edit Delete
<input type="checkbox"/>	greipsec	trust	gre	UP	-	70.1.1.2	70.1.1.1	-	Edit Delete

If the keepalive function is enabled and no keepalive packet is received from the remote device within the detection interval, the interface is switched to the Down state.

- Pinging the Remote Network Address

```

root@firewall:~# ping 22.1.1.2
PING 22.1.1.2 (22.1.1.2) 56(84) bytes of data.
64 bytes from 22.1.1.2: icmp_seq=1 ttl=64 time=0.064 ms
64 bytes from 22.1.1.2: icmp_seq=2 ttl=64 time=0.060 ms
64 bytes from 22.1.1.2: icmp_seq=3 ttl=64 time=0.060 ms
64 bytes from 22.1.1.2: icmp_seq=4 ttl=64 time=0.061 ms
64 bytes from 22.1.1.2: icmp_seq=5 ttl=64 time=0.059 ms
^C
    
```

- Checking Interface Traffic Statistics

Choose **Monitor > Traffic Monitoring > Interface Traffic > Interface Traffic Details** and check detailed interface traffic statistics.

Interface Traffic Statistics						
Interface Traffic Statistics Interface Traffic Details						
<input type="button" value="Export"/> <input type="button" value="Refresh"/> <input type="text" value="Enter an interface name."/>						
<input type="checkbox"/>	Interface	Interface Status	Zone	IP	Uplink	Downlink
<input type="checkbox"/>	Ge0/0		trust	172.17.123.48/26	510bps	11.91Kbps
<input type="checkbox"/>	Ge0/1		trust	50.1.1.2/24	1.91Kbps	3.03Kbps
<input type="checkbox"/>	Ge0/2		trust	60.1.1.2/24	0bps	924bps
<input type="checkbox"/>	Ge0/3		trust	22.1.1.253/24 3011:1/64	0bps	345bps
<input type="checkbox"/>	greipsec		trust		0bps	0bps
<input type="checkbox"/>	greipv4		trust		672bps	672bps
<input type="checkbox"/>	greipv6		trust		0bps	0bps

8.26.5 Configuring an IPv6 over IPv4 GRE Tunnel

1. Applicable Products and Versions

Table 8-35 Products and Versions

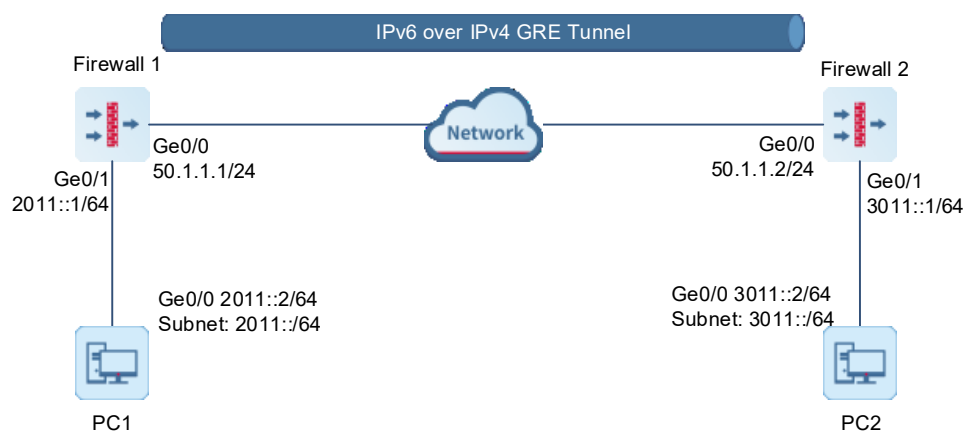
Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R7 or later

2. Service Demands

As shown in [Figure 8-32](#), both Firewall 1 and Firewall 2 have fixed public IP addresses. A GRE VPN tunnel needs to be established between the LANs where Firewall 1 and Firewall 2 reside to enable IPv6 network communication.

- Configure tunnel key values for both ends to authenticate the remote end of the GRE tunnel.
- Enable the checksum function to prevent data tampering.
- Enable the keepalive mechanism to detect whether the remote end is available. If the remote end is unavailable, the corresponding GRE interface is switched to Down to prevent data black holes.

Figure 8-32 Topology of an IPv6 over IPv4 GRE Tunnel



3. Restrictions and Guidelines

- Currently, GRE supports IPv4 tunnel encapsulation but not IPv6 tunnel encapsulation.

4. Prerequisites

You have completed basic network configurations for Firewall 1 and Firewall 2, including interface IP addresses and default routes. Pay attention to the following point during configuration:

- Ensure that Firewall 1 and Firewall 2 can communicate with each other through tunnel encapsulation IP addresses.

5. Procedure

- Configuring Firewall 1

(1) Configure a GRE interface.

a Choose **Network > Interface > Tunnel Interface > GRE Interface**.

b Click **Create**. On the page that is displayed, configure the following parameters for the GRE interface.

Edit GRE Interface

Basic Info

* Interface Name

Description

Interface Config

* Interface Type

* Security Zone [Add Security Zone](#)

Tunnel Interface Address IPv6

IPv6 Protocol Enable

IP/Mask

Tunnel Encapsulation Address

* Src. IPv4

* Dest. IPv4

Advanced Settings

Tunnel Validity Check

Tunnel Key Value

Keepalive

Keepalive Interval s

Retransmission Times

Tunnel MTU

Access Management

Permit HTTPS PING SSH

c After completing the configuration, click **Save**.

(2) Configure a service data route.

a Choose **Network > Routing > Static Routing > IPv6**.

b Click **Create**. On the page that is displayed, add a static route.

< Back **Edit Static Routing**

IP Type IPv6

* Dest. IP Range/Mask 3011::/64

Next-Hop Address

Interface greipv6

* ⓘ Priority 5

Description

c After completing the configuration, click **Save**.

(3) Configure an IPv6 address pool object.

a Choose **Object > Address > IPv6 Address**. The address object configuration page is displayed.

b Click **Create**. On the page that is displayed, add a local address object.

< Back **Edit IPv6 Address Object**

Basic Info

* Name greipv6

Description

IP Address/Range

* ⓘ IP Address/Range 2011::/64

c After completing the configuration, click **Save**.

d Click **Create**. On the page that is displayed, add a remote address object.

< Back **Edit IPv6 Address Object**

Basic Info

* Name greipv6-peer

Description

IP Address/Range

* ⓘ IP Address/Range 3011::/64

- e After completing the configuration, click **Save**.
- (4) Configure security policies.
- a Choose **Policy > Security Policy > Security Policy**. The security policy configuration page is displayed.
 - b Click **Create**. On the page that is displayed, add a security policy for traffic from the local end to the remote end.

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

Basic Info
* Name
Enabled State Enable Disable
* Policy Group [⊕ Add Group](#)
Description

Src. and Dest.
* Src. Security Zone
* Src. Address
User/User Group
* Dest. Security Zone
* Dest. Address

Service
Service

App
App

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

Action Settings
Action Option Permit Deny

Content Security
Intrusion Prevention Enable Disable [⊕ Add Intrusion Prevention Template](#)
Virus Protection Enable Disable [⊕ Add Virus Protection Template](#)
URL Filtering Enable Disable [⊕ Add URL Filtering](#)
Keyword Filtering Enable Disable [⊕ Add Keyword Filter](#)

Advanced

- c After completing the configuration, click **Save**.
- d Click **Create**. On the page that is displayed, add a security policy for traffic from the remote end to the local end.

< Back
Edit Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Keyword Filtering Enable Disable [⊕ Add Keyword Filter](#)

Advanced

e After completing the configuration, click **Save**.

- **Configuring Firewall 2**

(1) Configure a GRE interface.

a Choose **Network > Interface > Tunnel Interface > GRE Interface**.

b Click **Create**. On the page that is displayed, configure the following parameters for the GRE interface.

[< Back](#) **Edit GRE Interface**

Basic Info
* Interface Name
Description

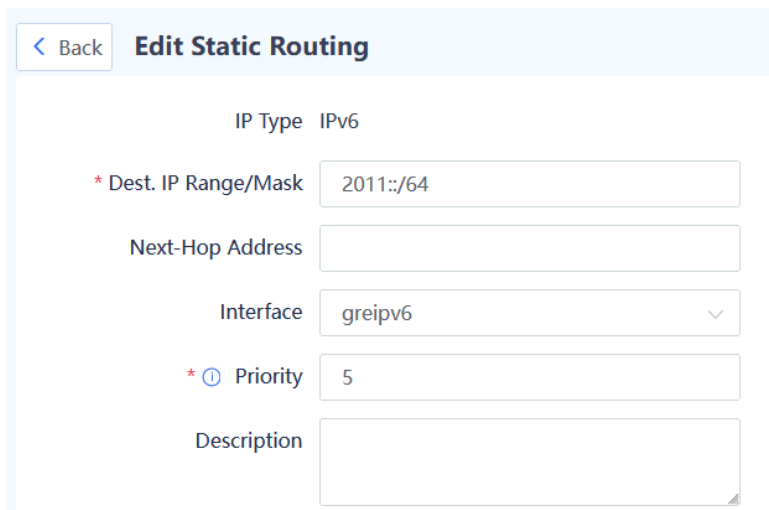
Interface Config
* Interface Type
* Security Zone [Add Security Zone](#)
① Tunnel Interface Address IPv6
① IPv6 Protocol Enable
① IP/Mask

Tunnel Encapsulation Address
* ① Src. IPv4
* ① Dest. IPv4

Advanced Settings
① Tunnel Validity Check
① Tunnel Key Value
① Keepalive
① Keepalive Interval s
① Retransmission Times
① Tunnel MTU

Access Management
Permit HTTPS PING SSH

- c After completing the configuration, click **Save**.
- (2) Configure a service data route.
 - a Choose **Network > Routing > Static Routing > IPv6**.
 - b Click **Create**. On the page that is displayed, add a static route.



Edit Static Routing

IP Type IPv6

* Dest. IP Range/Mask 2011::/64

Next-Hop Address

Interface greipv6

* Priority 5

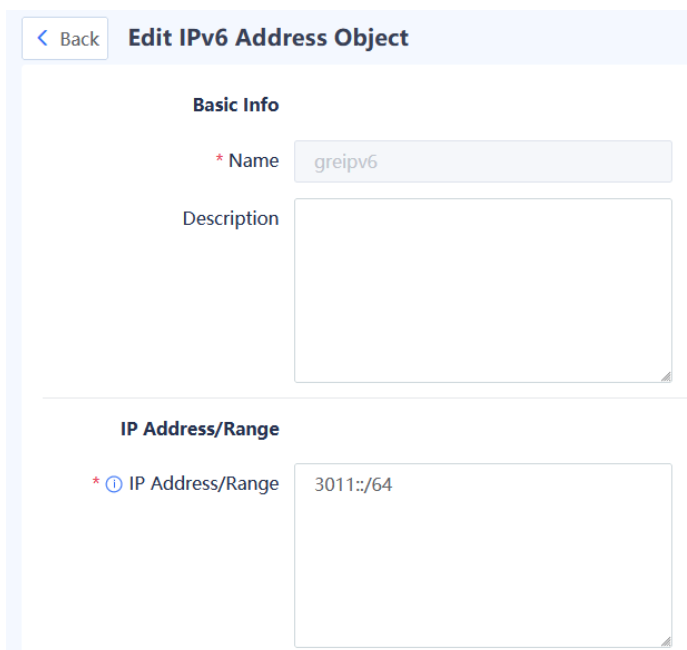
Description

c After completing the configuration, click **Save**.

(3) Configure an IPv6 address pool object.

a Choose **Object > Address > IPv6 Address**. The address object configuration page is displayed.

b Click **Create**. On the page that is displayed, add a local address object.



Edit IPv6 Address Object

Basic Info

* Name greipv6

Description

IP Address/Range

* IP Address/Range 3011::/64

c After completing the configuration, click **Save**.

d Click **Create**. On the page that is displayed, add a remote address object.

< Back Edit IPv6 Address Object

Basic Info

* Name greipv6-peer

Description

IP Address/Range

* IP Address/Range 2011::/64

- e After completing the configuration, click **Save**.
- (4) Configure security policies.
- a Choose **Policy > Security Policy > Security Policy**. The security policy configuration page is displayed.
 - b Click **Create**. On the page that is displayed, add a security policy for traffic from the local end to the remote end.

Edit Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [Add Group](#)

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Keyword Filtering Enable Disable [Add Keyword Filter](#)

Advanced

- c After completing the configuration, click **Save**.
- d Click **Create**. On the page that is displayed, add a security policy for traffic from the remote end to the local end.

e After completing the configuration, click **Save**.

6. Verification

- Checking Interface Status

On the web UI of Firewall 1, choose **Network > Interface > Tunnel Interface > GRE Interface** and check the interface status.

Interface Name	Security Zone	Interface Type	Interface Status	Tunnel Interface Address	Tunnel Local Address	Tunnel Remote Address	Description	Operation
greipv4	trust	gre	UP	-	50.1.1.1	50.1.1.2	-	Edit Delete
greipv6	trust	gre	UP	-	50.1.1.1	50.1.1.2	-	Edit Delete
greipsec	trust	gre	UP	-	70.1.1.1	70.1.1.2	-	Edit Delete

On the web UI of Firewall 2, choose **Network > Interface > Tunnel Interface > GRE Interface** and check the interface status.

Interface Name	Security Zone	Interface Type	Interface Status	Tunnel Interface Address	Tunnel Local Address	Tunnel Remote Address	Description	Operation
greipv4	trust	gre	UP	-	50.1.1.2	50.1.1.1	-	Edit Delete
greipv6	trust	gre	UP	-	50.1.1.2	50.1.1.1	-	Edit Delete
greipsec	trust	gre	UP	-	70.1.1.2	70.1.1.1	-	Edit Delete

If the keepalive function is enabled and no keepalive packet is received from the remote device within the detection interval, the interface is switched to the Down state.

- Pinging the Remote Network Address

```

root@firewall:~# ping 3011::2
PING 3011::2(3011::2) 56 data bytes
64 bytes from 3011::2: icmp_seq=1 ttl=64 time=0.078 ms
64 bytes from 3011::2: icmp_seq=2 ttl=64 time=0.123 ms
64 bytes from 3011::2: icmp_seq=3 ttl=64 time=0.094 ms
64 bytes from 3011::2: icmp_seq=4 ttl=64 time=0.094 ms
64 bytes from 3011::2: icmp_seq=5 ttl=64 time=0.091 ms
    
```

- Checking Interface Traffic Statistics

Choose **Monitor > Traffic Monitoring > Interface Traffic > Interface Traffic Details** and check detailed interface traffic statistics.

Interface	Interface Status	Zone	IP	Uplink	Downlink
Ge0/0	UP		172.17.123.12/24	10.81Kbps	33.10Kbps
Ge0/1	UP	untrust	50.1.1.1/24	1.36Kbps	1.66Kbps
Ge0/2	UP	trust	60.1.1.1/24	0bps	345bps
Ge0/3	UP	trust	20.1.1.253/24 2011:1/64	0bps	924bps
erspan1	UP	trust		0bps	0bps
greipsec	UP	trust		0bps	0bps
greipv4	UP	trust		0bps	0bps
greipv6	UP	trust		672bps	672bps

8.26.6 Configuring GRE over IPsec

1. Applicable Products and Versions

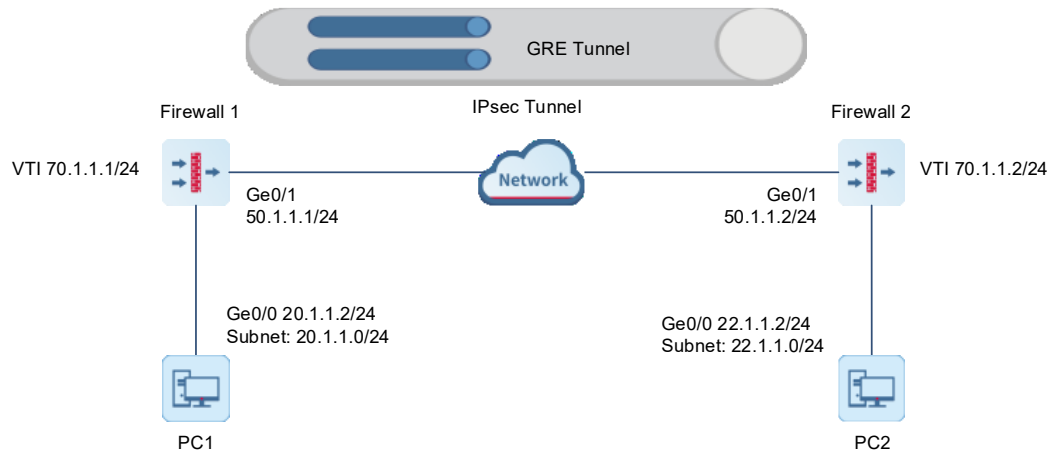
Table 8-36 Products and Versions

Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R7 or later

2. Service Demands

If data encryption is required for a GRE tunnel, GRE over IPsec can be implemented to encrypt data. [Figure 8-33](#) shows the typical topology.

Figure 8-33 Topology of GRE over IPsec



3. Restrictions and Guidelines

- For details about restrictions and guidelines for GRE over IPsec, see "Restrictions and Guidelines" in *RG-WALL 1600-Z-S Cloud-Managed Firewall IPsec VPN Typical Configuration Examples*.
- Currently, GRE supports IPv4 tunnel encapsulation but not IPv6 tunnel encapsulation.

4. Prerequisites

- Ensure that Firewall 1 and Firewall 2 can communicate with each other through IPsec tunnel addresses.

5. Configuring IPsec

- Configuring Firewall 1

(1) Configure a VTI.

- Choose **Network > Interface > Tunnel Interface > VTI Interface**.
- Click **Create**. On the VTI configuration page, configure the following parameters:
 - Set the interface name to **vti1**.
 - Set the IP address to 70.1.1.1/24.

[< Back](#) **Edit VTI Interface**

Basic Info

* Interface Name

* Enabled State Enable Disable

Security Zone [Add Security Zone](#)

Description

Address

IP

Access Management

Permit HTTPS PING SSH

(2) Configure an IPsec tunnel.

a Perform basic configuration.

Choose **Network > IPsec VPN > Custom Tunnel** and click **Create**. On the custom tunnel configuration page, configure the following parameters:

- o Set the tunnel name to **ipsec-gre**.
- o Set **Enabled State** to **Enable**.
- o Associate with the tunnel interface **vti1**. Set the local address to interface Ge0/1 and set the remote address to 50.1.1.2.
- o For the authentication mode, use the default value **Pre-shared Key**. Enter the key **test123** and then enter it again for confirmation.

After completing the basic configuration, click **Next**. The interesting traffic configuration page is displayed.

b Configure interesting traffic.

On the interesting traffic configuration page, click **Create** and configure the following parameters:

- o Set the proxy mode to **Host-to-Host**.
- o Set the local network address to 70.1.1.1 and the remote network address to 70.1.1.2.

Edit Custom Tunnel Details

Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/> Host-to-Host	70.1.1.1	70.1.1.2	Edit Delete

After configuring the interesting traffic, click **Next**. The security parameter configuration page is displayed.

c Configure security parameters.

On the security parameter configuration page, set IKE and IPsec parameters to ensure that the configurations match those of the remote device.

- o IKE: Select all IKE versions. Set the IKE negotiation mode to main mode, the pseudo-random algorithm to SHA-256, the encryption algorithm to AES-128, the verification algorithm to SHA, the DH group to GROUP5, and the SA lifetime to 86400 seconds.
- o IPsec: Set the IPsec protocol to ESP, the encapsulation mode to tunnel, the encryption algorithm to AES-

128, and the verification algorithm to SHA. Disable perfect forward secrecy. Set the SA lifetime to 3600 seconds and the tunnel MTU to 1400.

Basic Config Interesting Traffic Config Security Parameter Config

IKE Parameter

- * IKE Version IKEv1 IKEv2
- * Negotiation Mode: IKEv1 Main Mode
- * Pseudo-Random Algorithm: SHA-256
- * Encryption Algorithm: AES-128
- * Verification Algorithm: SHA
- * DH Group: GROUP5
- * SA Lifetime: 86400 Second

IPsec Parameter

- * Protocol: ESP
- * Encapsulation Mode: Tunnel
- * Encryption Algorithm: AES-128
- * Verification Algorithm: SHA
- Perfect Forward Secrecy:
- * SA Lifetime: 3600 Second
- Tunnel MTU: 1400

Previous Cancel Finish

Click **Finish** to create the IPsec tunnel.

- Configuring Firewall 2

- (1) Configure a VTI.

- Choose **Network > Interface > Tunnel Interface > VTI Interface**.
- Click **Create**. On the VTI configuration page, configure the following parameters:
 - o Set the interface name to **vti1**.
 - o Set the IP address to 70.1.1.2/24.

[< Back](#) **Edit VTI Interface**

Basic Info

* Interface Name

* Enabled State Enable Disable

Security Zone [⊕ Add Security Zone](#)

Description

Address

IP

Access Management

Permit HTTPS PING SSH

(2) Configure an IPsec tunnel.

- a Perform basic configuration.

Choose **Network > IPsec VPN > Custom Tunnel** and click **Create**. On the custom tunnel configuration page, configure the following parameters:

- o Set the tunnel name to **ipsec-gre**.
- o Set **Enabled State** to **Enable**.
- o Associate with the tunnel interface **vti1**. Set the local address to interface Ge0/1 and set the remote address to 50.1.1.1.
- o For the authentication mode, use the default value **Pre-shared Key**. Enter the key **test123** and then enter it again for confirmation.

After completing the basic configuration, click **Next**. The interesting traffic configuration page is displayed.

b Configure interesting traffic.

On the interesting traffic configuration page, click **Create** and configure the following parameters:

- o Set the proxy mode to **Host-to-Host**.
- o Set the local network address to 70.1.1.2 and the remote network address to 70.1.1.1.

Edit Custom Tunnel Details

Proxy Mode	Local Network	Peer Network	Operation
<input type="checkbox"/> Host-to-Host	70.1.1.2	70.1.1.1	Edit Delete

After configuring the interesting traffic, click **Next**. The security parameter configuration page is displayed.

c Configure security parameters.

On the security parameter configuration page, set IKE and IPsec parameters to ensure that the configurations match those of the remote device.

- o IKE: Select all IKE versions. Set the IKE negotiation mode to main mode, the pseudo-random algorithm to SHA-256, the encryption algorithm to AES-128, the verification algorithm to SHA, the DH group to GROUP5, and the SA lifetime to 86400 seconds.

- o IPsec: Set the IPsec protocol to ESP, the encapsulation mode to tunnel, the encryption algorithm to AES-128, and the verification algorithm to SHA. Disable perfect forward secrecy. Set the SA lifetime to 3600 seconds and the tunnel MTU to 1400.

Progress: Basic Config (✓) — Interesting Traffic Config (✓) — Security Parameter Config (3)

IKE Parameter

- * IKE Version: IKEv1 IKEv2
- * Negotiation Mode: IKEv1 Main Mode
- * Pseudo-Random Algorithm: SHA-256
- * Encryption Algorithm: AES-128
- * Verification Algorithm: SHA
- * DH Group: GROUP5
- * SA Lifetime: 86400 Second

IPsec Parameter

- * Protocol: ESP
- * Encapsulation Mode: Tunnel
- * Encryption Algorithm: AES-128
- * Verification Algorithm: SHA
- Perfect Forward Secrecy:
- * SA Lifetime: 3600 Second
- Tunnel MTU: 1400

Buttons: Previous, Cancel, Finish

Click **Finish** to create the IPsec tunnel.

6. Configuring GRE

● Configuring Firewall 1

(1) Configure a GRE interface.

- Choose **Network > Interface > Tunnel Interface > GRE Interface**.
- Click **Create**. On the page that is displayed, configure the following parameters for the GRE interface.

⚠ Caution

The MTU of the GRE tunnel must be the same as that configured for IPsec.

< Back
Edit GRE Interface

Basic Info

* Interface Name

Description

Interface Config

* Interface Type

* Security Zone [Add Security Zone](#)

Tunnel Interface Address

IP/Mask

Tunnel Encapsulation Address

* Src. IPv4

* Dest. IPv4

Advanced Settings

Tunnel Validity Check

Tunnel Key Value

Keepalive

Keepalive Interval s

Retransmission Times

Tunnel MTU

Access Management

Permit HTTPS PING SSH

- c After completing the configuration, click **Save**.
- (2) Configure a service data route.
 - a Choose **Network > Routing > Static Routing > IPv4**.
 - b Click **Create**. On the page that is displayed, add a static route.

< Back
Edit Static Routing

IP Type IPv4

* Dest. IP Range/Mask

Next-Hop Address

Interface

* Priority

Link Detection

Description

- c After completing the configuration, click **Save**.

- (3) Configure an IPv4 address pool object.
 - a Choose **Object > Address > IPv4 Address**. The address object configuration page is displayed.
 - b Click **Create**. On the page that is displayed, add a local address object.

The screenshot shows the 'Edit IPv4 Address Object' configuration page. At the top left, there is a '< Back' button and the title 'Edit IPv4 Address Object'. The page is divided into two main sections: 'Basic Info' and 'IP Address/Range'. Under 'Basic Info', there is a required field '* Name' with the value 'greipv4' and a 'Description' text area. Under 'IP Address/Range', there is a required field '* IP Address/Range' with the value '20.1.1.0/24'.

- c After completing the configuration, click **Save**.
 - d Click **Create**. On the page that is displayed, add a remote address object.

The screenshot shows the 'Edit IPv4 Address Object' configuration page. At the top left, there is a '< Back' button and the title 'Edit IPv4 Address Object'. The page is divided into two main sections: 'Basic Info' and 'IP Address/Range'. Under 'Basic Info', there is a required field '* Name' with the value 'greipv4-peer' and a 'Description' text area. Under 'IP Address/Range', there is a required field '* IP Address/Range' with the value '22.1.1.0/24'.

- e After completing the configuration, click **Save**.
- (4) Configure security policies.
 - a Choose **Policy > Security Policy > Security Policy**. The security policy configuration page is displayed.
 - b Click **Create**. On the page that is displayed, add a security policy for traffic from the local end to the remote end.

< Back

Edit Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Keyword Filtering Enable Disable [⊕ Add Keyword Filter](#)

Advanced

- c After completing the configuration, click **Save**.
- d Click **Create**. On the page that is displayed, add a security policy for traffic from the remote end to the local end.

< Back
Edit Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Keyword Filtering Enable Disable [⊕ Add Keyword Filter](#)

Advanced Settings

Save

e After completing the configuration, click **Save**.

- **Configuring Firewall 2**

(1) Configure a GRE interface.

a Choose **Network > Interface > Tunnel Interface > GRE Interface**.

b Click **Create**. On the page that is displayed, configure the following parameters for the GRE interface.

 **Caution**

The MTU of the GRE tunnel must be the same as that configured for IPsec.

< Back
Edit GRE Interface

Basic Info

* Interface Name

Description

Interface Config

* Interface Type

* Security Zone [Add Security Zone](#)

Tunnel Interface Address

IP/Mask

Tunnel Encapsulation Address

* Src. IPv4

* Dest. IPv4

Advanced Settings

Tunnel Validity Check

Tunnel Key Value

Keepalive

Keepalive Interval s

Retransmission Times

Tunnel MTU

Access Management

Permit HTTPS PING SSH

- c After completing the configuration, click **Save**.
- (2) Configure a service data route.
 - a Choose **Network > Routing > Static Routing > IPv4**.
 - b Click **Create**. On the page that is displayed, add a static route.

< Back
Edit Static Routing

IP Type

* Dest. IP Range/Mask

Next-Hop Address

Interface

* Priority

Link Detection

Description

- c After completing the configuration, click **Save**.
- (3) Configure an IPv4 address pool object.
- a Choose **Object > Address > IPv4 Address**. The address object configuration page is displayed.
 - b Click **Create**. On the page that is displayed, add a local address object.

The screenshot shows the 'Edit IPv4 Address Object' configuration page. At the top, there is a navigation bar with a '< Back' button and the title 'Edit IPv4 Address Object'. Below this, the 'Basic Info' section contains a required field for 'Name' with the value 'greipv4' and an empty 'Description' text area. The 'IP Address/Range' section contains a required field for 'IP Address/Range' with the value '22.1.1.0/24' and an empty text area below it.

- c After completing the configuration, click **Save**.
- d Click **Create**. On the page that is displayed, add a remote address object.

The screenshot shows the 'Edit IPv4 Address Object' configuration page. At the top, there is a navigation bar with a '< Back' button and the title 'Edit IPv4 Address Object'. Below this, the 'Basic Info' section contains a required field for 'Name' with the value 'greipv4-peer' and an empty 'Description' text area. The 'IP Address/Range' section contains a required field for 'IP Address/Range' with the value '20.1.1.0/24' and an empty text area below it.

- e After completing the configuration, click **Save**.
- (4) Configure security policies.
- a Choose **Policy > Security Policy > Security Policy**. The security policy configuration page is displayed.
 - b Click **Create**. On the page that is displayed, add a security policy for traffic from the local end to the remote end.

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

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Keyword Filtering Enable Disable [⊕ Add Keyword Filter](#)

Advanced

- c After completing the configuration, click **Save**.
- d Click **Create**. On the page that is displayed, add a security policy for traffic from the remote end to the local end.

< Back
Edit Security Policy

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [⊕ Add Group](#)

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

User/User Group

* Dest. Security Zone

* Dest. Address

Service

Service

App

App

Time Range

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

Action Settings

Action Option Permit Deny

Content Security

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

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

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

Keyword Filtering Enable Disable [⊕ Add Keyword Filter](#)

Advanced

e After completing the configuration, click **Save**.

7. Verification

- Checking Interface Status

On the web UI of Firewall 1, choose **Network > Interface > Tunnel Interface > GRE Interface** and check the interface status.

VTI Interface GRE Interface ERSPAN Interface									
<input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/> <input type="text" value="Enter a name."/>									
<input type="checkbox"/>	Interface Name	Security Zone	Interface Type	Interface Status	Tunnel Interface Address	Tunnel Local Address	Tunnel Remote Address	Description	Operation
<input type="checkbox"/>	greipv4	trust	gre	UP	-	50.1.1.1	50.1.1.2	-	Edit Delete
<input type="checkbox"/>	greipv6	trust	gre	UP	-	50.1.1.1	50.1.1.2	-	Edit Delete
<input type="checkbox"/>	greipsec	trust	gre	UP	-	70.1.1.1	70.1.1.2	-	Edit Delete

On the web UI of Firewall 2, choose **Network > Interface > Tunnel Interface > GRE Interface** and check the interface status.

VTI Interface GRE Interface ERSPAN Interface									
<input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/> <input type="text" value="Enter a name."/>									
<input type="checkbox"/>	Interface Name	Security Zone	Interface Type	Interface Status	Tunnel Interface Address	Tunnel Local Address	Tunnel Remote Address	Description	Operation
<input type="checkbox"/>	greipv4	trust	gre	UP	-	50.1.1.2	50.1.1.1	-	Edit Delete
<input type="checkbox"/>	greipv6	trust	gre	UP	-	50.1.1.2	50.1.1.1	-	Edit Delete
<input type="checkbox"/>	greipsec	trust	gre	UP	-	70.1.1.2	70.1.1.1	-	Edit Delete

If the keepalive function is enabled and no keepalive packet is received from the remote device within the detection interval, the interface is switched to the Down state.

- Pinging the Remote Network Address

```

root@firewall:~# ping 22.1.1.2
PING 22.1.1.2 (22.1.1.2) 56(84) bytes of data:
64 bytes from 22.1.1.2: icmp_seq=1 ttl=64 time=0.064 ms
64 bytes from 22.1.1.2: icmp_seq=2 ttl=64 time=0.060 ms
64 bytes from 22.1.1.2: icmp_seq=3 ttl=64 time=0.060 ms
64 bytes from 22.1.1.2: icmp_seq=4 ttl=64 time=0.061 ms
64 bytes from 22.1.1.2: icmp_seq=5 ttl=64 time=0.059 ms
  
```

- Checking Interface Traffic Statistics

Choose **Monitor > Traffic Monitoring > Interface Traffic > Interface Traffic Details** and check detailed interface traffic statistics.

Interface Traffic Statistics						
Interface Traffic Statistics Interface Traffic Details						
<input type="button" value="Export"/> <input type="button" value="Refresh"/> <input type="text" value="Enter an interface name."/>						
<input type="checkbox"/>	Interface	Interface Status	Zone	IP	Uplink	Downlink
<input type="checkbox"/>	Ge0/0		trust	172.17.123.48/26	25.90Kbps	18.36Kbps
<input type="checkbox"/>	Ge0/1		trust	50.1.1.2/24	1.86Kbps	2.44Kbps
<input type="checkbox"/>	Ge0/2		trust	60.1.1.2/24	0bps	230bps
<input type="checkbox"/>	Ge0/3		trust	22.1.1.253/24 3011::1/64	0bps	230bps
<input type="checkbox"/>	greipsec		trust		672bps	672bps
<input type="checkbox"/>	greipv4		trust		0bps	0bps
<input type="checkbox"/>	greipv6		trust		0bps	0bps

8.26.7 Common Fault Diagnosis

- Check whether the key values configured for both ends are the same
- Check whether the keepalive configuration is correct.
- Check whether the interface configuration is correct.
- Check whether a route is configured for the tunnel.
- Check whether local defense policies are created.

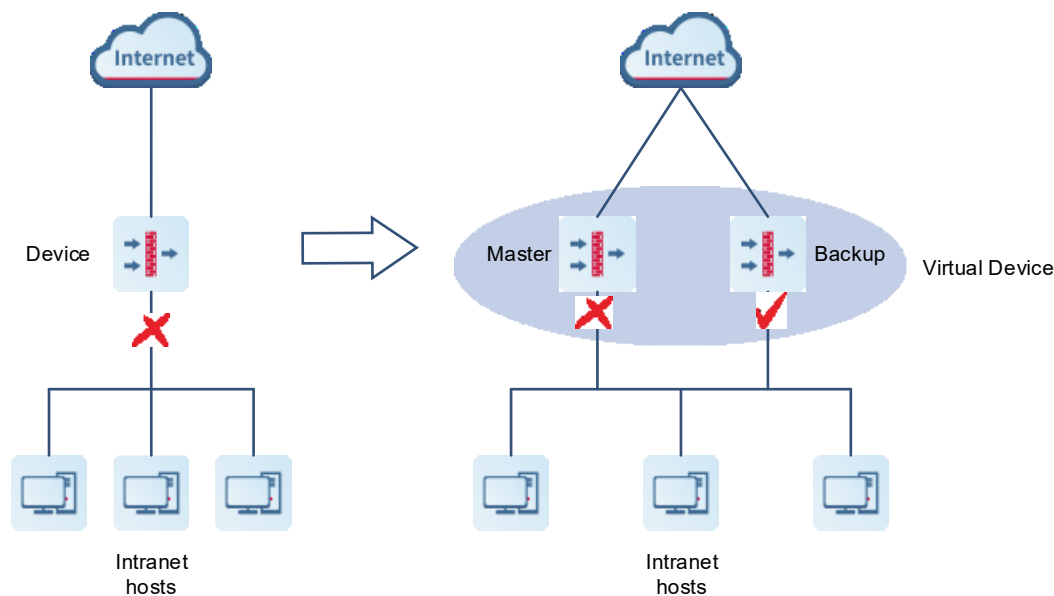
8.27 VRRP

8.27.1 Overview

Virtual Router Redundancy Protocol (VRRP) is a redundancy and fault-tolerance protocol that virtualizes a group of devices that can function as gateways into a virtual device. Intranet hosts only need to obtain the IP address of the virtual device and configure it as their gateway IP address so that they can communicate with the extranet through the virtual device.

Within the VRRP group, a master device is elected among all devices and responsible for forwarding network traffic. The remaining devices act as backup devices. If the master device fails, a new master device is elected from the backup devices to forward traffic, which ensures uninterrupted services.

VRRP improves network reliability, simplifies device configuration, and effectively prevents network interruptions caused by single-link failures.



i Note

Only VRRPv2 is supported.

8.27.2 Working Process

After VRRP is configured, its working process is as follows:

- (1) In a VRRP group, a master device is elected among devices based on priorities, while the remaining devices become backup devices. The master device sends gratuitous ARP messages to inform other devices and hosts of its virtual MAC address and is responsible for forwarding packets.
- (2) The master device periodically sends VRRP messages to advertise its VRRP state, priority, and other information.
- (3) If the master device fails, such as due to an uplink interface failure, a new master device is elected from the backup devices in the VRRP group based on priorities.
- (4) Currently, VRRP supports only the preemption mode: When receiving a VRRP message, a backup device compares its priority with that of the master device in the VRRP message. If the backup device has a higher priority and the preemption delay duration expires, it automatically becomes the new master device.
- (5) When the master role is taken by a new device, the new master device sends a gratuitous ARP message containing the MAC address and virtual IP address of the virtual device to notify other hosts and devices to update their ARP information. The new master device is responsible for forwarding packets. Hosts and devices on the network are unaware of the master device switchover.

For enhanced security, VRRP provides plain text authentication. The master device adds an authentication text in the VRRP message and sends it to the backup devices. Upon receiving the VRRP message, the backup device compares the authentication text with its locally configured text. If the authentication texts match, the received VRRP message is considered valid. Otherwise, the backup device regards the VRRP message as an invalid message and discards it.

8.27.3 Configuring a VRRP Group

Application Scenario

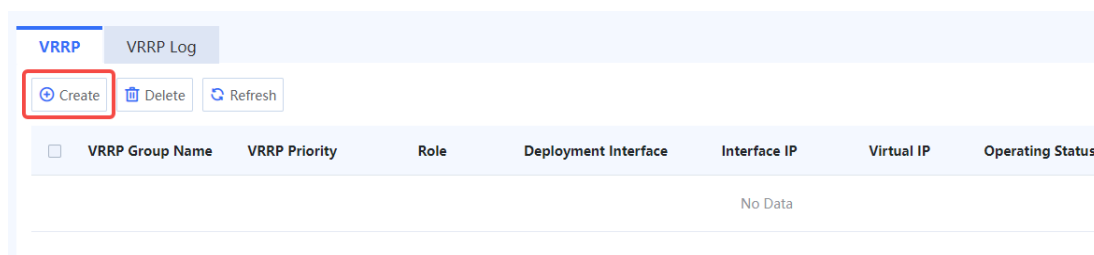
VRRP is suitable for scenarios where redundancy is required at the routing egress to effectively prevent network interruptions caused by single-link failures.

Note

Configuring multiple VRRP groups for load balancing is not supported.

Procedure

- (1) Choose **Network > VRRP**. Click the **VRRP** tab.
- (2) Click **Create** to access the **Add VRRP Group** page.



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

< Back

Add VRRP Group

Basic Info

* VRRP Group Name

① Priority

* ① Deployment Interface

* ① Virtual IP

① Monitoring Interface

⋮ Advanced

① Preemption Delay Second

① Advertisement Interval Second

Authentication

① Plain Text Authentication

Item	Description	Remarks
Basic Info		
VRRP Group Name	Number of the VRRP group. A group of devices with the same VRRP group name forms a virtual device.	[Example] 1
Priority	The priority of the VRRP group. A larger value indicates a higher priority. In a VRRP group, the device with the highest priority is elected as the master device.	[Example] 254
Deployment Interface	Interface on which the VRRP function is enabled. You can specify only a physical interface or logical sub-interface in routing mode configured with an IPv4 address. The deployment interface and monitoring interface cannot be the same.	[Example] Ge0/4

Item	Description	Remarks
Virtual IP	IP address of the virtual device, which is different from the IP address of the deployment interface but must be on the same network segment as the deployment interface.	[Example] 192.168.1.1
Monitoring Interface	Interface used to monitor uplink interface status changes of the device. This parameter can only be configured on the master device.	[Example] Ge0/2
Association Priority	When the status of the monitoring interface changes, this parameter determines how the VRRP priority of the local device is modified. If the monitoring interface goes Down, the priority of the device is reduced by the specified value. At this point, another device with the highest priority in the VRRP group can be elected as the new master device.	[Example] 10
Advanced		
Preemption Delay	Delay in seconds that a backup device waits before declaring itself as the master device when its priority is higher than that of the current master device.	[Example] 1
Advertisement Interval	Interval in seconds at which the master device sends VRRP messages. All devices within the same VRRP group must be configured with the same advertisement interval.	[Example] 1
Authentication		
Plain Text Authentication	Determines whether VRRP messages are valid. Both the master and backup devices must be configured with the same plain text authentication key.	[Example] x30dn78k

Confirm the configuration and click **Save**.

Follow-up Procedure

- Choose **Policy > Security Policy > Security Policy**. On the **Security Policy** page, configure a policy to permit traffic on relevant interfaces. Otherwise, network connectivity issues may occur.
- Adding, deleting, or modifying VRRP configurations may cause VRRP group state changes. Eventually, the VRRP group will enter in a stable state. You can view running logs on the **VRRP Log** tab page.

8.27.4 Viewing VRRP Logs

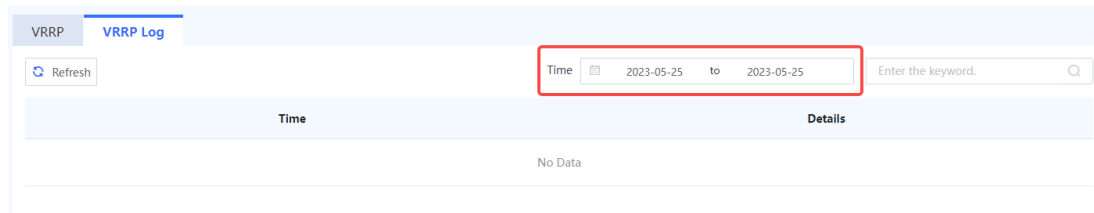
Application Scenario

A log entry is generated once the status of the master and backup devices in the VRRP group changes. This helps you check the running status of VRRP.

Procedure

Choose **Network > VRRP**. Click the **VRRP Log**.

Select a query period and the **VRRP Log** tab page displays the logs generated within the specified period.



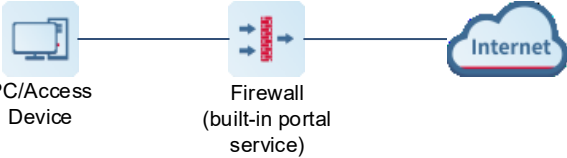
8.28 Web Authentication

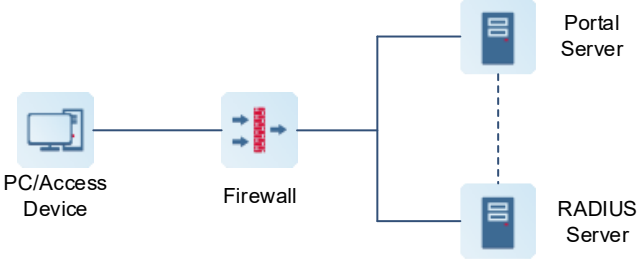
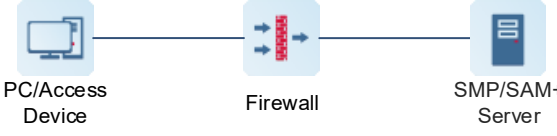
8.28.1 Application Scenario

Web authentication is an identify authentication mechanism that is widely used in web applications and online services. Its objective is to ensure that only authorized users can access specific resources or perform specific operations. With web authentication, users can log in to the system with unique and secure identity credentials.

During the web authentication process, users typically need to provide valid credentials (username and password) to verify that they are legitimate. After the authentication succeeds, a user is granted corresponding access permissions and can securely browse web pages, access online services, and conduct interactions.

The web authentication function of RG-WALL 1600-Z series firewalls falls into local portal authentication and external portal authentication based on the location of the portal server. Additionally, real-name user information synchronization is supported. Web authentication applies to the following scenarios.

Scenario	Description
Local portal authentication	<p>The firewall provides a built-in portal service. After obtaining the user's username and password, the portal service authenticates the user's identity information. After passing the authentication, the user can access specific resources or perform specific operations.</p> <div style="text-align: center;">  <p>PC/Access Device Firewall (built-in portal service) Internet</p> </div> <p>Configuration notes:</p> <ul style="list-style-type: none"> ● Set Local Portal Authentication to Enabled. ● Set the authentication template name to Local Portal in authentication policy configuration. ● Toggle on WEBAUTH in authentication domain configuration. ● Configure User Location in authentication domain configuration. <ul style="list-style-type: none"> ○ To authenticate user information using a firewall, configure Only Local Info or Prefer Local Info. ○ To authenticate user information using an external RADIUS server, configure Only Info on Server or Prefer Info on Server.

Scenario	Description
<p>External portal authentication</p>	<p>When the portal service is deployed externally, the firewall requests authentication from the RADIUS server, and the portal server sends the authentication result to the firewall. After passing the authentication, the user can access specific resources or perform specific operations.</p>  <p>Configuration notes:</p> <ul style="list-style-type: none"> ● On the External Portal page, set Portal Authentication to Enabled. ● In authentication policy configuration, set the authentication template to the template configured on the External Portal page. ● Toggle on WEBAUTH in authentication domain configuration. ● In authentication domain configuration, set User Location to Only Info on Server or Prefer Info on Server. <p>Note: An RG-WALL 1600-Z series firewall cannot act as an external RADIUS server.</p>
<p>Real-name user information synchronization</p>	<p>When a Red-Giant Security Management Platform (RG-SMP) or Ruijie Security Accounting Management System (RG-SAM+) device is deployed on the live network, the real-name user information synchronization function can be used to synchronize user information on the RG-SMP or RG-SAM+ device to the firewall. This mode applies to Network Access Server (NAS) scenarios where user going online and offline information needs to be synchronized from the server to firewall.</p>  <p>Configuration notes:</p> <ul style="list-style-type: none"> ● On the Real-Name User Info Reception page, enable Link-SAM Association.

8.28.2 Limitations

- In a NAT scenario where traffic traverses the bridge network of the firewall twice, the firewall cannot correctly identify the packets sent from the PC to the firewall and discards the packets, resulting in an authentication failure.

Workaround: Add the local IP address to the allowlist of a specific authentication policy.

- When both built-in authentication and external authentication are enabled and users need to be authenticated on different servers, the domains to which the users belong must be specified.

- Local portal authentication does not support MAC Authentication Bypass (MAB) in a Layer 3 network environment.
- After users go online, they will not be forced to go offline due to policy changes, but can be forced to go offline in the user center.
- In a external portal authentication scenario, user information can only be stored on an external server. User information configured on the local firewall cannot be used.
- The web authentication function does not support networking issue identification through packet tracing in the diagnostic center.
- When web authentication is used in an IPsec VPN scenario and all user information is configured at the hub, users at spokes cannot be authenticated through local portal authentication at the hub, but can be authenticated through external portal authentication (using an external portal server).
- When external portal authentication is used in a Virtual Router Redundancy Protocol (VRRP) scenario, the portal server cannot be connected using a virtual IP address.

Workaround: Add the physical interface IP address of the firewall on the portal and RADIUS servers.

8.28.3 Configuration Example of Local Portal Authentication

1. Applicable Products and Versions

Table 8-37 Products and Versions

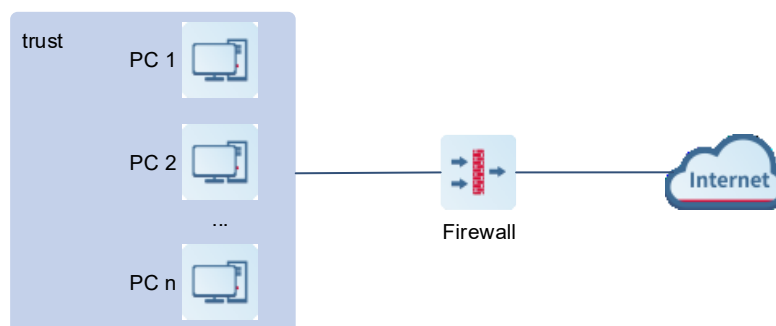
Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS1.0R6 or later

2. Service Demands

As shown in the following figure, the intranet PC needs to be authenticated through local portal authentication on the firewall before going online. The requirements are as follows:

- When an intranet user uses a browser to access the web service with destination port 80, 443, or 8080, the firewall redirects the access page to the local portal authentication page. The user can access the Internet only after entering a valid username and password and passing the authentication.
- The username and password information of intranet users are configured on the local firewall.

Figure 8-34 Network Topology of Local Portal Authentication



3. Restrictions and Guidelines

- The local portal authentication service of the firewall supports only the HTTP protocol.

4. Prerequisites

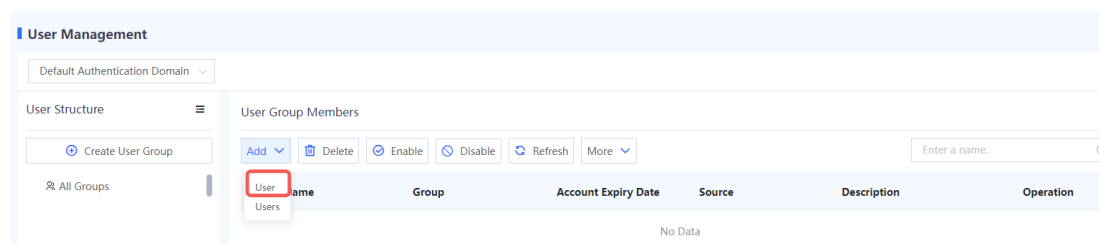
Basic network configurations of the firewall, including the interface IP address, security zone, and security policies, have been completed. Pay attention to the following points during configuration:

- Check user information location.
- Check the user source zone, and configure it in a specific authentication policy.
- Check the redirection action upon successful local portal authentication, and configure the redirection page when setting local portal authentication.

5. Procedure

(1) Configuring User Information

- a Choose **Object > User Authentication > User Management**.
- b On the page that is displayed, click **Add** and choose **User**.



- c Configure user information for Internet access.
 - Login Username: **test**
 - Parent Group: **/default**. In this example, the predefined default user group is selected. In actual configuration, you can select a custom user group as required.
 - Password: **test@123**

[< Back](#) **Add User**

Basic Info

* Login Username

Enabled State Enable Disable

Displayed Username

* Parent Group

Description

Password

*

* Confirm Password

Advanced Settings

d Click **Save**.

(2) Configuring an Authentication Domain

- a Choose **Object > User Authentication > Authentication Domain**.
- b In this example, the default authentication domain is edited. In actual configuration, you can configure a custom authentication domain as required.
 - o Toggle on **WEBAUTH**.
 - o Set **User Location** to **Only Local Info**.

[← Back](#) **Edit Authentication Domain**

Basic Info

* Name

Enabled State Enable Disable

Description

*** Scenario**

SSL VPN Access ⓘ

User Location ▾

WEBAUTH ⓘ

User Location ▾

☰ Advanced Settings

c Click **Save**.

(3) Configuring Local Portal Authentication

a Choose **Object > User Authentication > Authentication Settings > Local Portal**.

b On the page that is displayed, toggle on **Local Portal Authentication**.

o Authentication Port: Set the default port 8081.

o Redirection upon Authentication: In this example, **No Redirection** is selected. Upon successful authentication, the local portal authentication success page is still displayed, without redirecting to a new web page.

Redirect to Previous Web Page indicates that the previous web page is displayed upon successful authentication. **Redirect to Custom URL** indicates that the specified web page is displayed upon successful authentication.

Local Portal Custom Portal Real-Name User Info Reception Allowlist

Local Portal Authentication

Authentication Port

Redirection upon Authentication No Redirection
 Redirect to Previous Web Page
 Redirect to Custom URL

c Click **Apply**.

(4) Configuring an Authentication Policy

- a Choose **Object > User Authentication > Authentication Policy**.
- b On the page that is displayed, click **Create** and configure an authentication policy according to the following figure.
 - o Name: **test**
 - o Src. Security Zone: **trust**
 - o Src. Address: **any**. This indicates that all users in the trust security zone need to pass authentication before accessing the Internet.
 - o Authentication Action: **Authentication**
 - o Authentication Template Name: **Local Portal**

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

* Name

Enabled State Enable Disable

Description

* Src. Security Zone

* Src. Address

Authentication Action Authentication Authentication-free

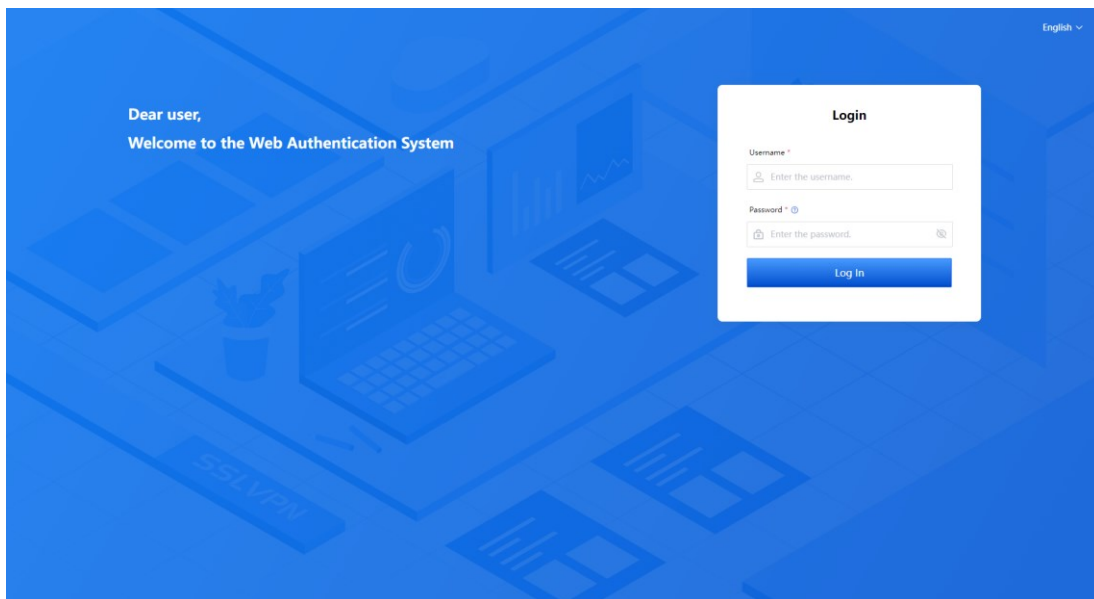
* Authentication Template Name

6. Verification

- (1) On an intranet PC, open a browser, and enter the URL with destination port 80, 443, or 8080 in the address bar. The browser is redirected to the following portal authentication page.
- (2) Enter the username **test** and password **test@123**, and click **Log In**.

⚠ Caution

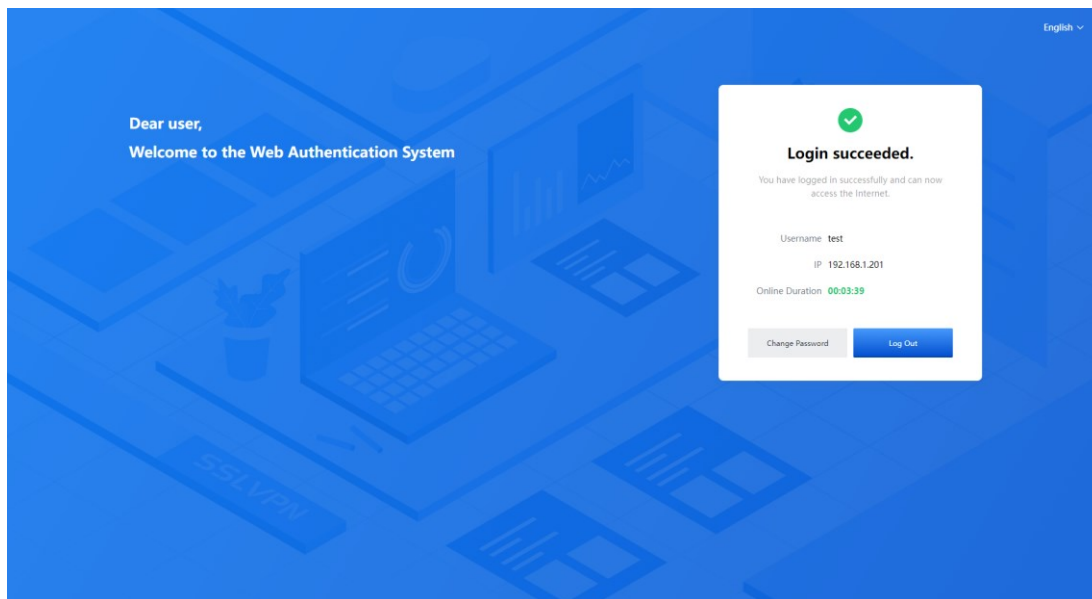
If the authentication domain is not **default**, enter the username in the format of *Username@Domain name*. For example, if the username is **test** and the domain name is **domain1**, enter **test@domain1** for login.



- (3) Upon successful login, the authentication success page is still displayed.

i Note

In this example, **No Redirection** is selected. Therefore, the authentication success page is still displayed upon successful login. To set a redirection page, choose **Object > User Authentication > Authentication Settings > Local Portal** and configure on the page that is displayed.



(4) Enter the URL with destination port 80, 443, or 8080 in the address bar again. The corresponding web page is displayed.

8.28.4 Configuration Example of External Portal Authentication

1. Applicable Products and Versions

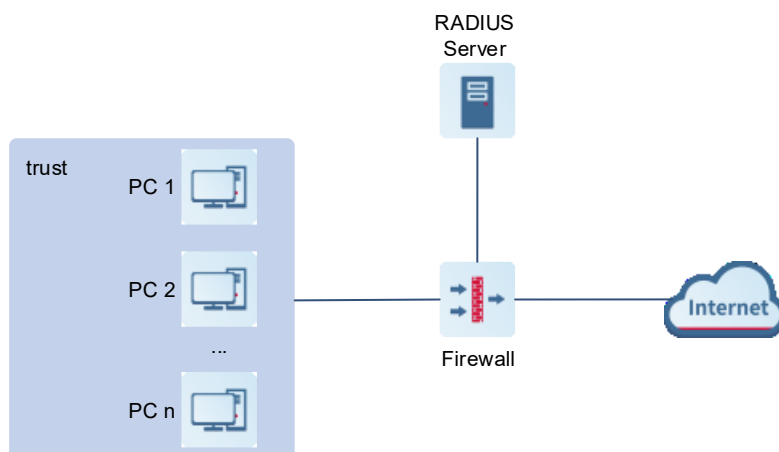
Table 8-38 Products and Versions

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS1.0R6 or later

2. Service Demands

As shown in the following figure, the intranet PC needs to be authenticated by an external portal server before going online. The requirements are as follows:

- When an intranet user uses a browser to access the web service with destination port 80, 443, or 8080, the firewall redirects the access page to the external portal authentication page. The user can access the Internet only after entering a valid username and password and passing the authentication.
- The username and password information of intranet users are configured on the external RADIUS server.

Figure 8-35 Network Topology of External Portal Authentication

3. Restrictions and Guidelines

- An RG-WALL 1600-Z series firewall cannot act as a RADIUS server. In a external portal authentication scenario, a dedicated RADIUS server in the authentication domain must be configured as the authentication server.

4. Prerequisites

Basic network configurations of the firewall, including the interface IP address, security zone, and security policies, have been completed.

The RADIUS server information has been configured and the firewall can communicate with the RADIUS server. Pay attention to the following points during configuration:

- Verify that user authentication information on the RADIUS server is correct.
- Check the user source zone, and configure it in a specific authentication policy.

5. Procedure

(1) Adding a RADIUS Server

- a Choose **Object > User Authentication > Authentication Server**.
- b On the page that is displayed, click **Create** and configure a RADIUS server according to the following figure.

< Back

Add RADIUS Server

Basic Info

* Server Name

* Shared Password

Active Authentication Server IP

* IP

① Authentication Port

① Accounting Port

Tx Interface

Standby Authentication Server IP

IP

① Authentication Port

① Accounting Port

Tx Interface

⌵ Advanced Settings

Retransmission Times

Unit

Response Timeout

① Enable Active Detection

c Click **Save**.

(2) Configuring an Authentication Domain

a Choose **Object > User Authentication > Authentication Domain**.

b In this example, the default authentication domain is edited. In actual configuration, you can configure a custom authentication domain as required.

o Toggle on **WEBAUTH**.

o Set **User Location** to **Only Info on Server**.

< Back
Edit Authentication Domain

Basic Info

* Name

Enabled State Enable Disable

Description

*** Scenario**

SSL VPN Access ⓘ

User Location

WEBAUTH ⓘ

User Location

Authentication Server [⊕ Add RADIUS Server](#)

⌵ Advanced Settings

c Click **Save**.

(3) Configuring External Portal Authentication

a Choose **Object > User Authentication > Authentication Settings > External Portal**.

b Toggle on to enable external portal authentication, and configure a external portal authentication template.

o Portal Authentication Template 1 Name: **portal1**

o Portal Server URL: URL of the redirected portal authentication page

o NAS Configuration: In this example, **Default** is selected. This indicates that the firewall communicates with the NAS through an outbound interface based on the routing policy.

o Custom URL Parameters: Parameters carried in the redirected URL. All the parameters are enabled by default. In actual configuration, you can disable parameters that are not required. Each parameter has a default value, which can be restored when the field name is cleared. The default values of the parameters are as follows:

User IP Field: **wlanuserip**

MAC Field: **mac**

NAS-IP Field: **nasip**

URL Field: **url**

Hostname Field: **hostname**

Custom Parameters: Other custom parameters. The values are empty by default. Up to five custom parameters can be configured.

In this example, default configuration is used for custom URL parameters.

Portal Authentication

[Create](#)

Portal Authentication Template 1 [Delete](#)

Basic Info

* Portal Authentication Template 1 Name:

* Portal Server URL:

URL Config Result:

NAS Configuration Default ip Interface

Custom URL Parameters

User IP Field <input checked="" type="checkbox"/>	Field Name: <input type="text" value="Enter the field name."/>	Encryption Mode: <input type="text" value="Select an encryption mode."/>
MAC Field <input checked="" type="checkbox"/>	Field Name: <input type="text" value="Enter the field name."/>	Encryption Mode: <input type="text" value="Select an encryption mode."/>
Address Format: <input type="text" value="XX-XX-XX-XX-XX-XX"/>		
NAS-IP Field <input checked="" type="checkbox"/>	Field Name: <input type="text" value="Enter the field name."/>	Encryption Mode: <input type="text" value="Select an encryption mode."/>
URL Field <input checked="" type="checkbox"/>	Field Name: <input type="text" value="Enter the field name."/>	Encryption Mode: <input type="text" value="Select an encryption mode."/>
Hostname Field <input checked="" type="checkbox"/>	Field Name: <input type="text" value="Enter the field name."/>	Encryption Mode: <input type="text" value="Select an encryption mode."/>
Custom Parameter1 <input checked="" type="checkbox"/>	Parameter Name: <input type="text" value="Enter a parameter name."/>	Parameter Value: <input type="text" value="Enter a value."/>
		Encryption Mode: <input type="text" value="None"/>

- c Configure a portal server.
 - o Portal Server IP: Set an IPv4 address.
 - o Port: UDP port number of the portal server. (The default value is 50100.)
 - o Shared Key: Key for the connection, which is also used to encrypt fields specified in **Custom URL Parameters**.
 - o Sending Source: In this example, **Default** is selected. The device uses the outbound interface selected by the routing policy as the sending source.
 - o MAB: If this function is enabled, a user only needs to enter the username and password once, and can subsequently go online without authentication. This function is disabled in this example.
 - o Server Detection: Set ICMP or Portal Protocol to detect server availability. This function is disabled in this example.
 - o Escape: If this function is enabled, user Internet access is not affected when the server goes Down. This function is disabled in this example.
 - o Listening Port: Local listening port of the firewall. In this example, the default port number 2000 (UDP) is used.

Portal 3.0

Basic Info

* Portal Server IP: Port:

* Shared Key:

Sending Source Default Interface

MAB:

Advanced Settings

Server Detection:

Server Detection Protocol Type:

Detection Interval:

Detection Retries:

Escape: If the portal server goes down after this function is enabled, specific network access permissions can be granted to users to support basic network access requests.

Listening Port

Listening Port:

- d Click **Apply**.
- (4) Configuring an Authentication Policy
- a Choose **Object > User Authentication > Authentication Policy**.
 - b On the page that is displayed, click Create and configure an authentication policy according to the following figure.
 - o Name: **test**
 - o Src. Security Zone: **trust**
 - o Src. Address: **any**. This indicates that all users in the trust security zone need to pass authentication before accessing the Internet.
 - o Authentication Action: **Authentication**
 - o Authentication Template Name: Select the external portal authentication template name **portal1** configured in the previous section.

The screenshot shows the 'Edit Authentication Policy' configuration page. The page has a light blue header with a back button labeled '返回' and the title 'Edit Authentication Policy'. Below the header, there are several configuration fields:

- Name:** A text input field containing 'test'.
- Enabled State:** Radio buttons for 'Enable' (selected) and 'Disable'.
- Description:** A text input field containing 'test_policy'.
- Src. Security Zone:** A dropdown menu showing 'trust'.
- Src. Address:** A dropdown menu showing 'any'.
- Authentication Action:** Radio buttons for 'Authentication' (selected) and 'Authentication-free'.
- Authentication Template Name:** A dropdown menu showing 'portal1'.

- c Click **Save**.

6. Verification

On an intranet PC, open a browser, and enter the URL with destination port 80, 443, or 8080 in the address bar. The firewall redirects the access page to the external portal authentication page. Enter a valid username and password, and click **Log In**. Check whether the authentication succeeds.

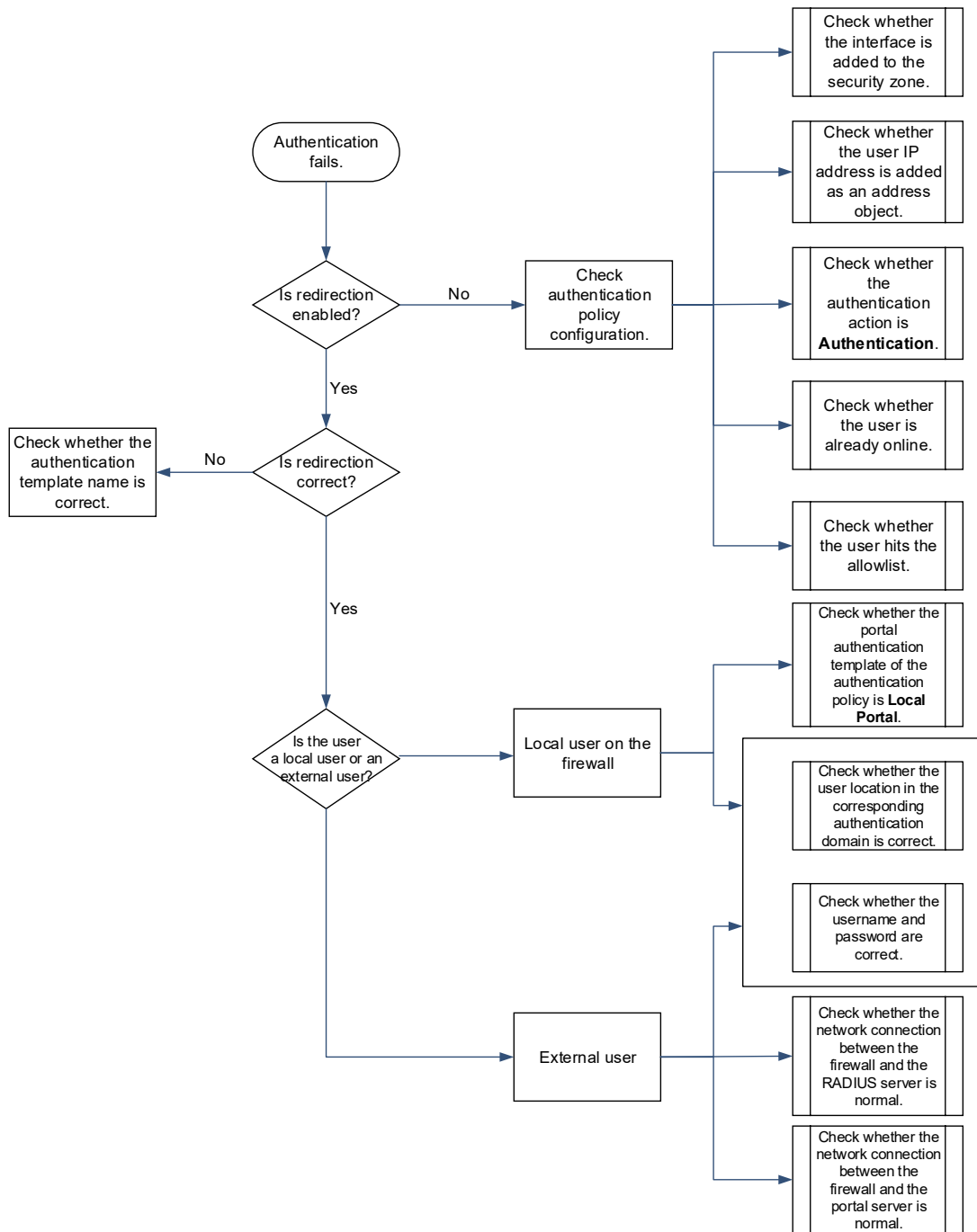
8.28.5 Common Faults and Troubleshooting Roadmap

Common web authentication faults are as follows:

- Redirection fails.
- User authentication fails.

The following figure shows the troubleshooting roadmap.

Figure 8-36 Troubleshooting Roadmap of Web Authentication



- To view authentication policies, choose **Object > User Authentication > Authentication Policy**.
- To view authentication domains, choose **Object > User Authentication > Authentication Domain**.

8.29 Overload Protection


Application Scenario

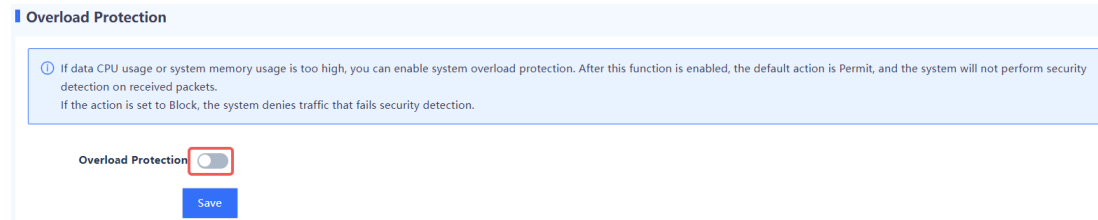
If overload protection is enabled, when the CPU usage or memory usage of the system is too high, the device permits traffic by default and does not perform application-level resolution on received packets. In scenarios with

high security requirements, you can set the action to blocking to deny traffic that is not detected by intrusion prevention, virus protection, or threat intelligence.

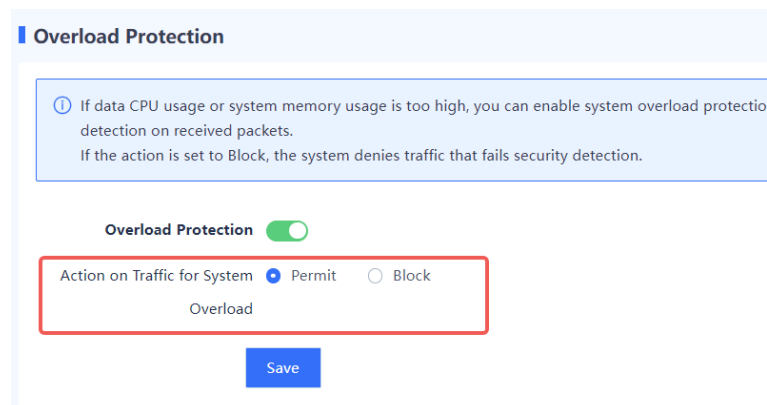
Procedure

(1) Choose System > Overload Protection.

(2) Toggle on  to enable the overload protection function.



(3) Configure the action to be taken on traffic when overload is detected.



(4) Click **Save**.

8.30 Information Push

8.30.1 Overview

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.

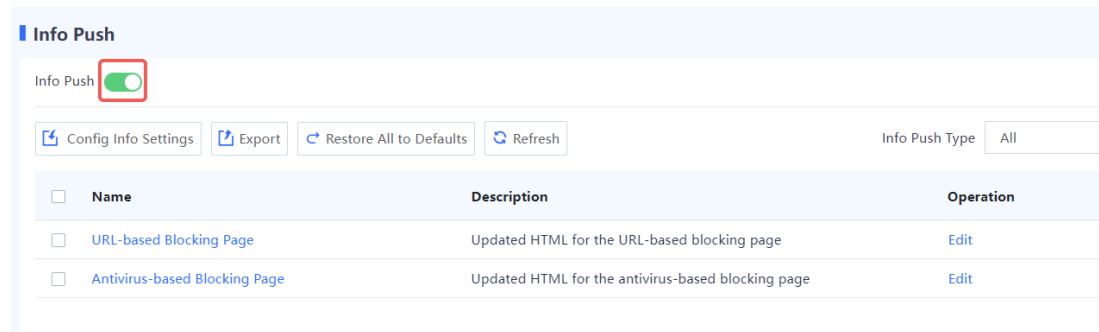
8.30.2 Setting the Logo Image

Application Scenario

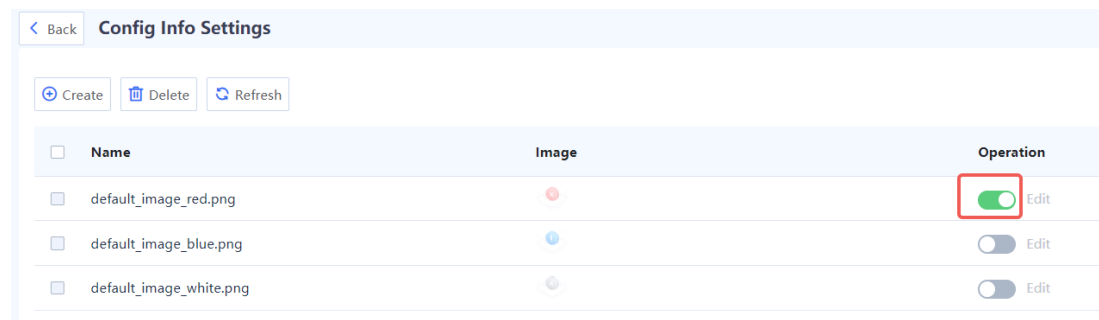
The device provides three predefined logos, which cannot be edited or deleted. You can also customize the logo image.

Procedure

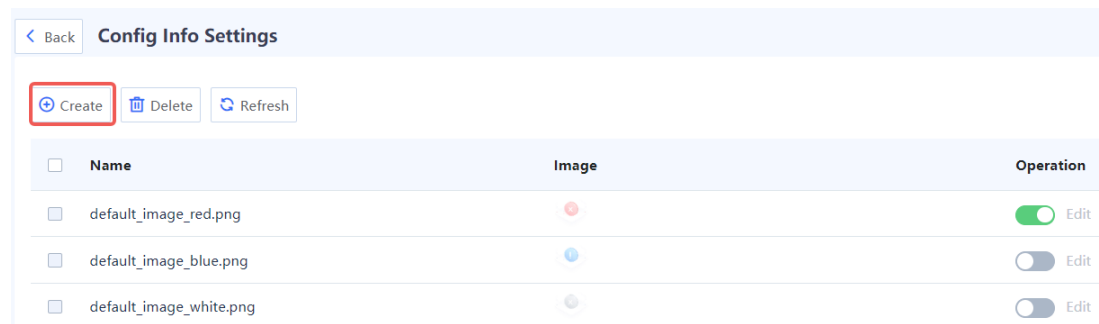
- (1) Choose System > Info Push.
- (2) Toggle on  to enable information push.



- (3) 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.



- (4) Click Create.



- (5) Add a logo image. The image format must be PNG or JPEG, and the image size cannot exceed 32 KB.

Add Config Info ✕

* Name

Image

+

(6) Click Confirm.

Follow-up Procedure

You can modify or delete a custom logo image.

8.30.3 Editing Text Information

Application Scenario

The device supports online editing of push information for virus protection and URL filtering. After traffic is blocked by a security service (virus protection or URL filtering), 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) Toggle on to enable information push.

Info Push

Info Push

Info Push Type: All

	Name	Description	Operation
<input type="checkbox"/>	URL-based Blocking Page	Updated HTML for the URL-based blocking page	Edit
<input type="checkbox"/>	Antivirus-based Blocking Page	Updated HTML for the antivirus-based blocking page	Edit

(3) Click **Edit** in the **Operation** column.

Info Push

Info Push

Info Push Type: All

	Name	Description	Operation
<input type="checkbox"/>	URL-based Blocking Page	Updated HTML for the URL-based blocking page	Edit
<input type="checkbox"/>	Antivirus-based Blocking Page	Updated HTML for the antivirus-based blocking page	Edit

(4) Configure the push text.

[< Back](#) | **Configure Info Push for URL-based Blocking Page**

Info Push Preview

Web Access blocked

According to the network control policy, you have no privilege to visit this web page.If you have proper reason to access this specific website, please contact your network administrator for help.

Edit Info Push

* Title

* Description

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.

(5) Click **Save**.

(6) (Optional) Click **Restore Defaults** to restore the default text.

< Back **Configure Info Push for URL-based Blocking Page**

Info Push Preview

Web Access blocked

According to the network control policy, you have no privilege to visit this web page.If you proper reason to access this specific website, please contact your network administrator fo

Edit Info Push

* Title

* Description

Follow-up Procedure

Info Push

Info Push

Info Push Type:

<input type="checkbox"/>	Name	Description	Oper
<input type="checkbox"/>	URL-based Blocking Page	Updated HTML for the URL-based blocking page	Edit
<input type="checkbox"/>	Antivirus-based Blocking Page	Updated HTML for the antivirus-based blocking page	Edit

- 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.

8.31 Subinterface

8.31.1 Overview

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

8.31.2 Configuration Examples of VLAN Interconnection on Sub-interfaces

1. Applicable Products and Versions

Table 8-39 Applicable Products and Versions

Device Type	Device Name	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	All versions

2. Service Demands

A firewall is deployed at the egress of an internal network to connect to a device with the VLAN function enabled and forward VLAN packets (with the VLAN ID of 10).

3. Topology

Figure 8-37 Topology

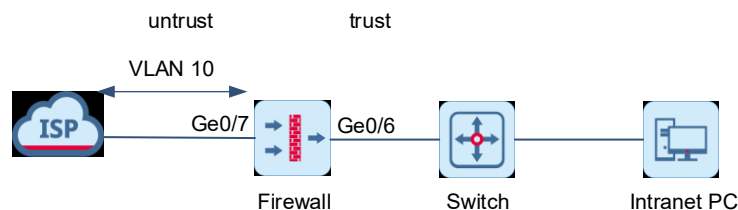


Table 8-40 Configuration Description

Information	Description
ISP	The port connected to the ISP forwards packets which should carry VLAN tags.

4. Restrictions and Guidelines

The basic network configurations, such as the interface IP addresses and default routes, have been completed on the firewall.

5. Configuration Roadmap

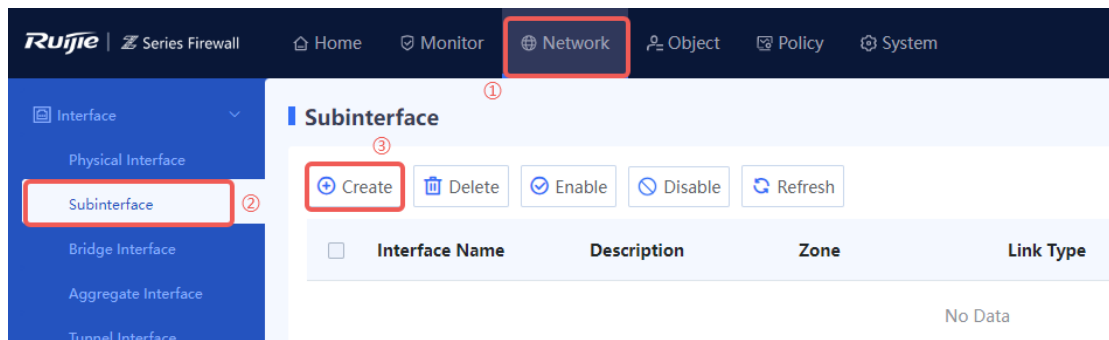
Configure a sub-interface on the interface connecting the firewall to the ISP and set the VLAN ID of the sub-interface to 10.

Add the sub-interface to the **untrust** zone and create a security policy to allow packets from the **trust** zone to the **untrust** zone.

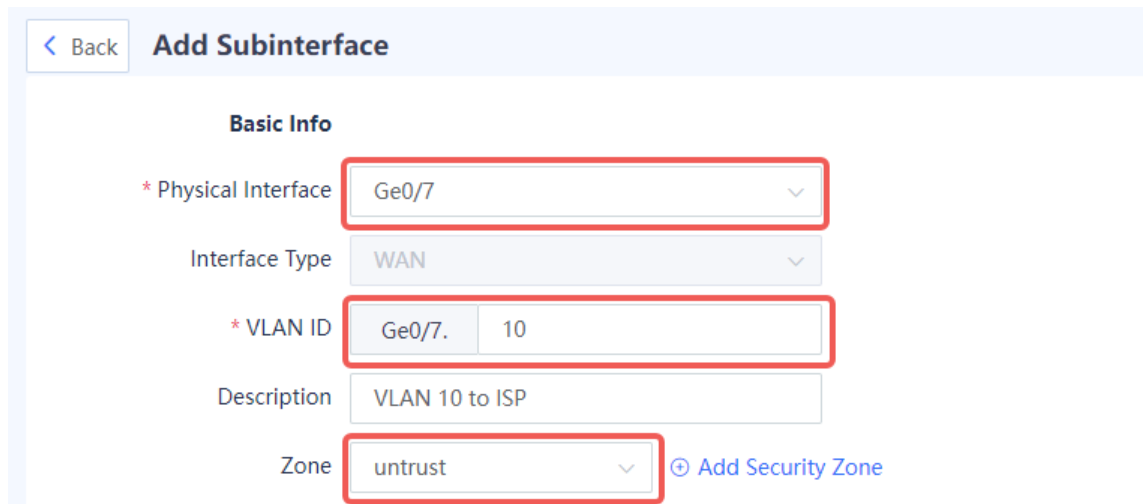
6. Procedure

(1) Configuring a Sub-interface

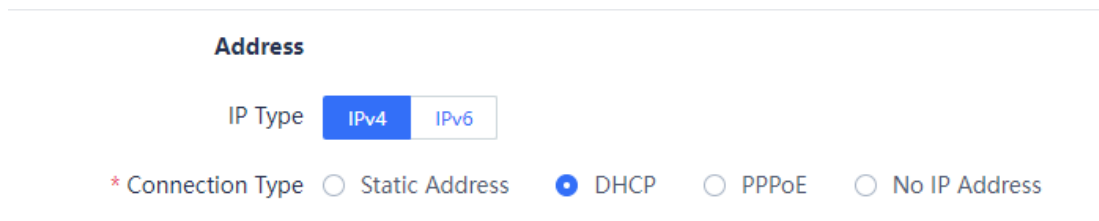
- a Choose **Network > Interface > Subinterface**, click **Create**, and create a sub-interface on the physical interface connecting the firewall to the ISP device.



- b Select a physical interface (Ge0/7 in this example), set the VLAN ID to 10 (the same as the sub-interface ID), and set **Zone** to **untrust**.



- c Configure the connection type based on actual requirements. In this example, configure the sub-interface to automatically obtain an IP address from the ISP device. Therefore, set **Connection Type** to **DHCP**.



(2) Configuring a Security Policy

- a Choose **Policy > Security Policy** and click **Create** to create a security policy as follows.
 - o Set **Src. Security Zone** to **trust**.
 - o Set **Src. Address** to **any**, indicating packets with all IP addresses in the source security zone are permitted.
 - o Set **Dest. Security Zone** to **untrust**.
 - o Set **Dest. Address** to **any**, indicating that a user is allowed to access resources with all IP addresses in the destination security zone.
 - o Set **Action Option** to **Permit**.

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

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [Add Group](#)

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

* Dest. Security Zone

* Dest. Address

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

7. Verification

Check that the sub-interface has obtained an IP address, and the intranet PC can ping the ISP gateway and other public IP addresses.

8.32 Bridge Interface

8.32.1 Overview

Bridge interfaces are applicable to firewall deployment in transparent mode.

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

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

8.32.2 Configuration Examples of Layer-2 Transparent Transmission

1. Applicable Products and Versions

Table 8-41 Applicable Products and Versions

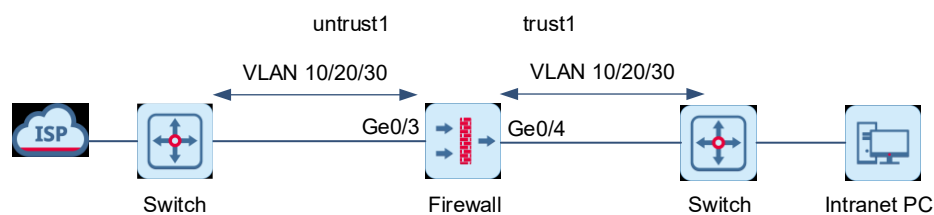
Device Type	Device Name	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	All versions

2. Service Demands

A firewall needs to be deployed between two switches in transparent mode to transparently transmit Layer 2 packets from multiple VLANs (for example, VLANs 10, 20, and 30).

3. Topology

Figure 8-38 Topology



4. Restrictions and Guidelines

Basic network configurations are completed on uplink and downlink switches, and the **trunk permit vlan 10 20 30** configuration has been configured on interfaces connected to the firewall.

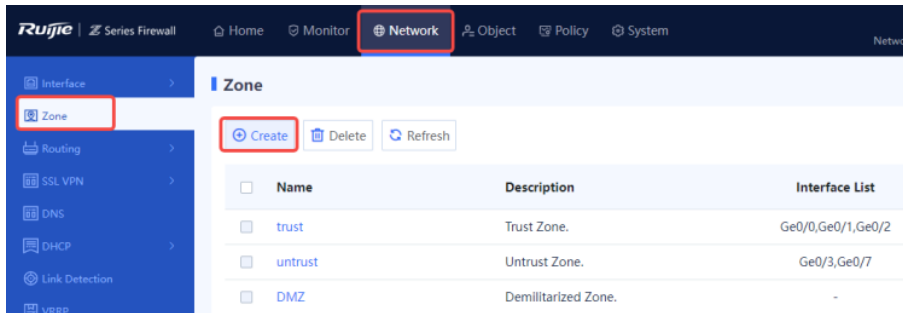
5. Configuration Roadmap

- (1) Create a bridge interface and add a pair of transparent transmission interfaces to the bridge interface.
- (2) Add the uplink interface to **untrust1** and the downlink interface to **trust1**, and then create a security policy to allow traffic from **trust1** to **untrust1**.

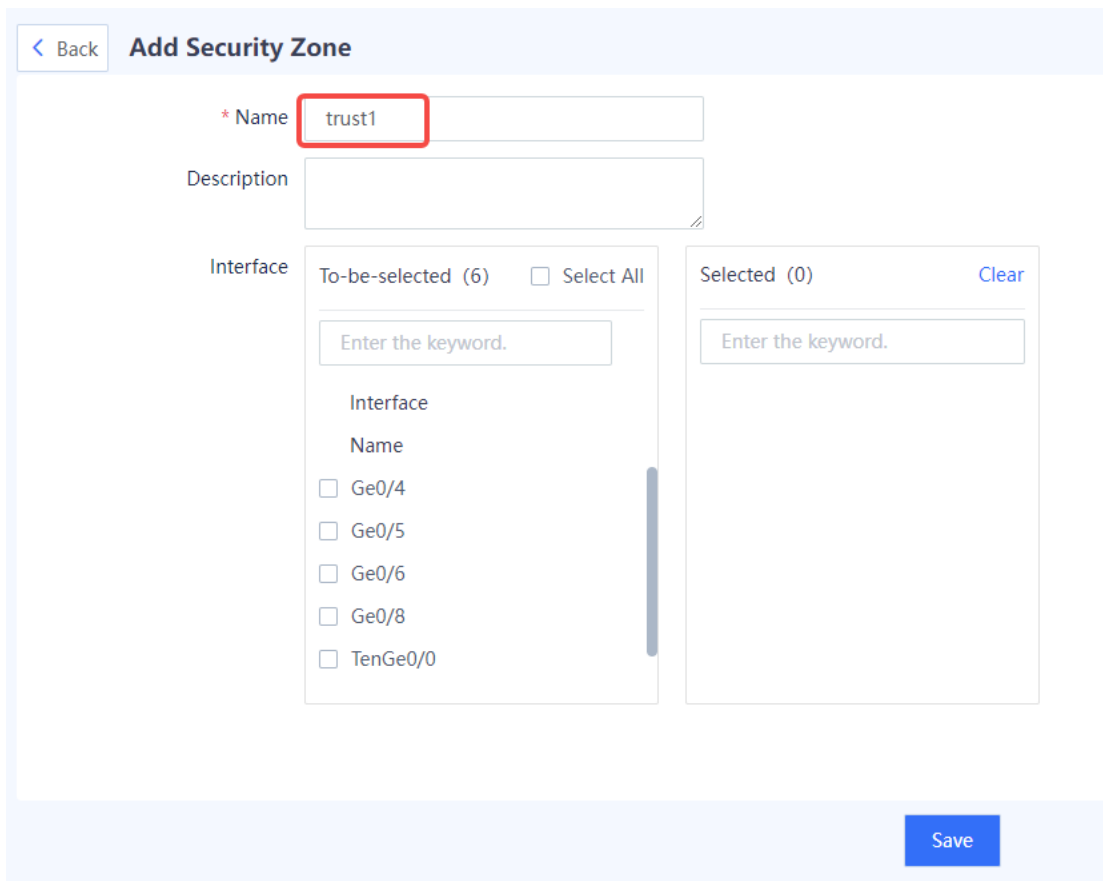
6. Procedure

(1) Creating Security Zones

a Choose **Network** > **Zone** and click to create a security zone.



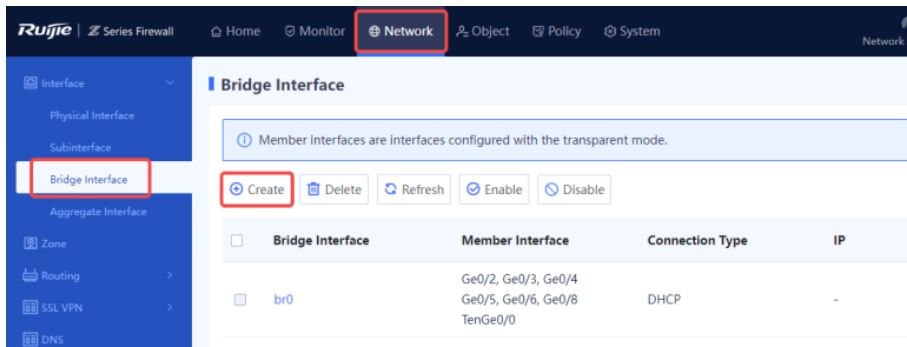
b Create the security zone **trust1** and click **Save**.



c Repeat the previous steps to create the security zone **untrust1**.

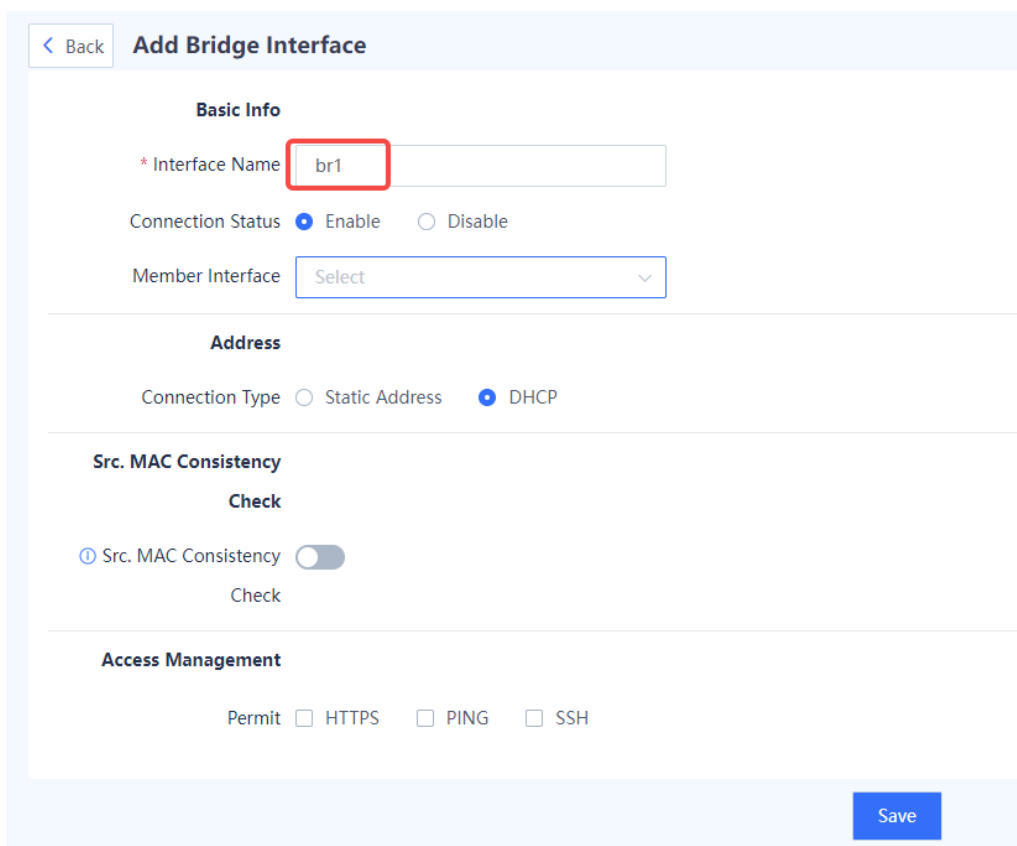
(2) Creating a Bridge Interface

a Choose **Network** > **Interface** > **Bridge Interface** and click **Create** to create the bridge interface **br1**.



b Configure the bridge interface **br1** as follows and click **Save**.

Select a connection type according to actual requirements. In this example, set **Connection Type** to **DHCP**.



c Configure a pair of physical interfaces to work in transparent transmission mode, add them to the bridge interface **br1**, and assign the interfaces to security zones. In this example, set the uplink interface to Ge0/3, and the security zone to **untrust1**; set the downlink interface to Ge0/4, and the security zone to **trust1**.

d Choose Network > Interface > Physical Interface, select Ge0/4, and click Edit.

e Set Mode to Transparent Mode, Bridge Interface to br1, Zone to trust1 for Ge0/4, and click Save.

< Back

Edit Physical Interface

Basic Info

Interface Name

Description

Connection Status Enable Disable

Mode Routing Mode **Transparent Mode** Off-Path Mode

* Bridge Interface + Add Bridge Interface

* Zone + Add Security Zone

Interface Type WAN Interface LAN Interface

Advanced

MTU

MAC Restore Default MAC

f Add the uplink interface Ge0/3 to **untrust1** in the same way, and set the parameters consistent with those in the preceding figure.

(3) Creating a Security Policy

- a Choose **Policy > Security Policy** and click **Create** to create the **sec_1** security policy as follows.
 - o Set **Src. Security Zone** to **trust1**.
 - o Set **Src. Address** to **any**, indicating packets with all IP addresses in the source security zone are permitted.
 - o Set **Dest. Security Zone** to **untrust1**.
 - o Set **Dest. Address** to **any**, indicating that a user is allowed to access resources with all IP addresses in the destination security zone.
 - o Set **Action Option** to **Permit**.

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

Basic Info

* Name

Enabled State Enable Disable

* Policy Group [+ Add Group](#)

* Adjacent Policy

Description

Src. and Dest.

* Src. Security Zone

* Src. Address

* Dest. Security Zone

* Dest. Address

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

7. Verification

Layer 2 packets from all VLANs can be transparently transmitted through the firewall, and intranet users can successfully ping the uplink VLAN gateway address.

You can view traffic details in the security policy matching record.

Priority	Name	Address	Service	App	Time Range	Action	Content Security	Hit Count	Hit Session	Operation
Default Policy Group										
1	sec_2	ny	any	any	any	Permi		2612	Clear	View Details... Edit Delete
2	sec_1	ny	any	any	any	Permi		5076	Clear	View Details... Edit Delete
3	allow_trus...	ny	any	any	any	Permi		0	Clear	View Details... Edit Delete
4	allow_all	ny	any	any	any	Permi		0	Clear	View Details... Edit Delete
5	Default Po...	ny	any	any	any	Deny		0	Clear	View Details... Edit Delete

9 Routine Maintenance

9.1 Checking Indicators on the Hardware Device Panel

Figure 9-1 and Table 9-1 describe the indicators on the device panel of the RG-WALL 1600-Z3200-S.

Figure 9-1 Front Panel

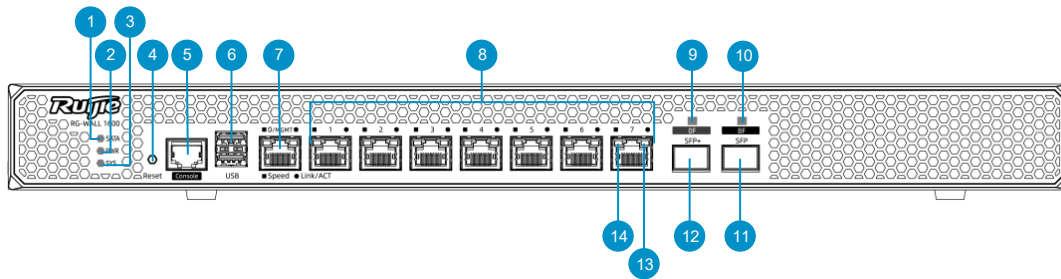


Table 9-1 Components on the Front Panel

No.	Component	Description
1	SATA hard disk status LED (SATA)	<ul style="list-style-type: none"> Steady green: A hard disk is connected. Blinking green: Data is being read or written.
2	Power module status LED (PWR)	<ul style="list-style-type: none"> Steady green: The power supply is normal. Off: The power supply is cut off or fails.
3	System status LED (SYS)	<ul style="list-style-type: none"> Blinking green: The device is powered on and being initialized. Steady green: Initialization is complete. Steady red: An alarm is generated.
4	Reset button	<ul style="list-style-type: none"> Restarting the device: Press the button for less than 3 seconds. Restoring factory settings: Press the button for more than 5 seconds. <p>When you perform either of the preceding operations, device status information is collected. After the device restarts, you can access the web UI of the firewall, choose System > One-Click Collection, and download the information.</p>

No.	Component	Description
5	Console port	<p>It is used to connect to the console for device maintenance and diagnosis.</p> <p>Note:</p> <ul style="list-style-type: none"> ● When the console port is used, set the baud rate to 115,200 bps, data bit to 8, and stop bit to 1, and disable parity check and data flow control. ● The console port is used only in special scenarios. For details, contact technical support personnel.
6	USB port	Two USB 2.0 ports can be used to connect USB drives.
7	MGMT port	It is used to access the device management page upon first login.
8	10/100/1000BASE-T ports	Ports 1 to 7, which are used to connect Ethernet cables.
9	10GE SFP + port LED	<ul style="list-style-type: none"> ● Steady green: The port is connected. ● Blinking green: The port is receiving or sending data. ● Off: The optical port is incorrectly connected.
10	1GE SFP port LED	<ul style="list-style-type: none"> ● Steady green: The port is connected. ● Blinking green: The port is receiving or sending data. ● Off: The optical port is incorrectly connected.
11	1GE SFP port	Port 8F. For details about optical modules that support this port, see Table 1-5 .
12	10GE SFP+ port	Port 0F. For details about optical modules that support this port, see Table 1-5 .
13	Link/ACT status LEDs (square) of 10/100/1000BASE-T ports	<ul style="list-style-type: none"> ● Steady green: The port is connected. ● Blinking green: The port is receiving or sending data. ● Off: The port is incorrectly connected.
14	Speed LEDs (round) of 10/100/1000BASE-T ports	<ul style="list-style-type: none"> ● Steady orange: Gbit/s port speed ● Off: 100/10 Mbit/s port speed

[Figure 9-2](#) and [Table 9-2](#) describe the indicators on the device panel of the RG-WALL 1600-Z5100-S.

Figure 9-2 Front Panel

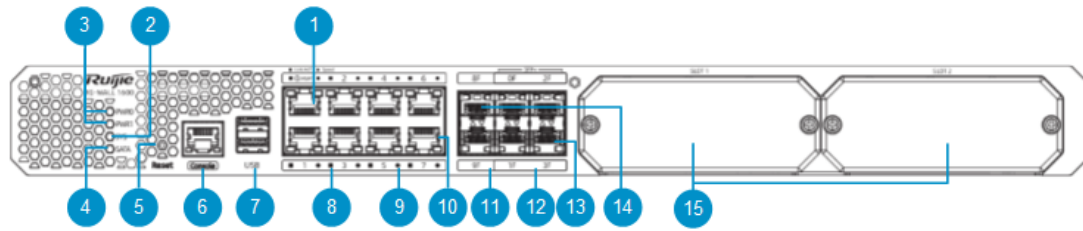


Table 9-2 Components on the Front Panel

No.	Component	Description
1	MGMT port	It is used to access the device management page upon first login.
2	System status LED (SYS)	<ul style="list-style-type: none"> Blinking green: The device is powered on and being initialized, or the system is restoring factory settings. Solid green: Initialization is complete. Solid red: An alarm is generated.
3	Power module status LEDs (PWR0 and PWR1)	<ul style="list-style-type: none"> Solid green: The power module is operating normally. Solid red: The power module is not functioning properly, or the power module is installed but no power cord is connected. Off: No power supply is connected.
4	SATA hard disk status LED (SATA)	Solid green: A hard disk is connected. Blinking green: Data is being read or written.
5	Reset button	<ul style="list-style-type: none"> Restarting the device: Press the button for less than 5 seconds. Restoring factory settings: Press the button for more than 5 seconds. When you perform either of the preceding operations, device status information is collected. After the device starts, you can log in to the web UI of the firewall, choose System > One-Click Collection , and download device status information.
6	Console port	It is used to connect to the console for maintenance and diagnosis. Note: <ul style="list-style-type: none"> When the console port is used, set the baud rate to 115,200 bps, data bit to 8, and stop bit to 1, and disable parity check and data flow control. The console port is used only in special scenarios. For details, contact technical support personnel.
7	USB port	Two USB 2.0 ports can be used to connect USB flash drives.
8	Link/ACT status LEDs (square) of 10/100/1000BASE-T ports	<ul style="list-style-type: none"> Solid green: The link on the port is Up. Blinking green: The port is receiving or sending data. Off: No link is established on the port.
9	Speed LEDs (round) of 10/100/1000BASE-T ports	<ul style="list-style-type: none"> Solid orange: Gbps port speed Off: 100/10 Mbps port speed

No.	Component	Description
10	10/100/1000BASE-T ports	Ports 1 to 7, which are used to connect Ethernet cables.
11	1GE SFP port LEDs	<ul style="list-style-type: none"> ● Solid green: The port is connected. ● Blinking green: The port is receiving or sending data.
12	10GE SFP + port LEDs	<ul style="list-style-type: none"> ● Solid green: The port is connected. ● Blinking green: The port is receiving or sending data.
13	10GE SFP+ ports	Ports 0F to 3F
14	1GE SFP ports	Ports 8F and 9F
15	Module slots	Expansion module slots

9.2 Checking Basic Configurations

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 Monitor > Device Monitoring > Device Hardware Monitoring.
- (2) Set Display Cycle.



- (3) The page displays the CPU usage, memory usage, and hard disk usage in different areas.

Note

The hard disk usage is displayed only when a hard disk is installed on the device.



Follow-up Procedure

Item	Description
CPU Usage	<p>In normal cases, the CPU usage should be lower than 80%. If the CPU usage is too high for a long time, check the device and analyze the causes.</p> <p>The possible causes for high CPU usage are as follows:</p> <ul style="list-style-type: none"> ● App protection or DDoS protection is enabled. ● Too many connections are created, many of which are initiated by attackers.
Memory Usage	<p>In normal cases, the memory usage should be lower than 80%. If the memory usage is too high for a long time, check the device and analyze the causes.</p>
Hard disk Usage	<p>In normal cases, the hard disk usage should be lower than 90%. If the remaining hard disk space is too small for a long time, check the device and clear the hard disk space.</p>

9.3 Log Monitoring

Log information refers to the packet processing information recorded by the firewall. The network administrator can effectively monitor the network running information and diagnose network faults based on the log information. The network administrator can also track, record, and analyze network access of users in real time and audit network access behavior of users. The firewall can export system logs, security logs, and operation logs and back up log files to a third-party server through Syslog.

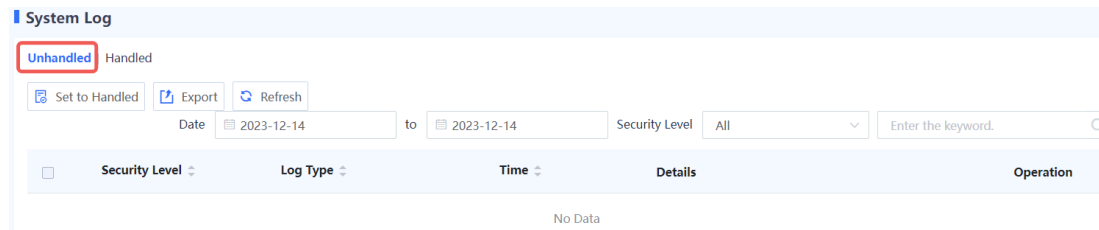
9.3.1 Querying System Logs

Application Scenario

By querying system logs, the administrator can view the runtime logs generated during the system running process and log records related to the hardware environment to check whether the firewall keeps running properly. If a fault occurs, the administrator can locate and analyze the fault based on the system logs.

Procedure

(1) Choose Monitor > Log Monitoring > System Log > Unhandled.



(2) The system log-related information is displayed on the web page.

Field	Description
Security Level	Security level of a system log.
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.

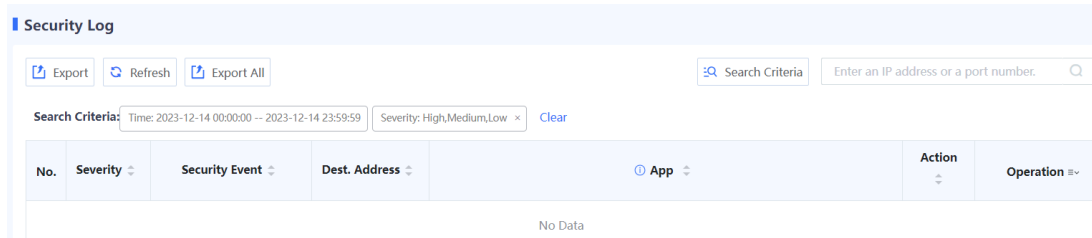
9.3.2 Querying Security Logs

Application Scenario

By querying security logs, the administrator can obtain traffic attack information on the network to check the network bandwidth usage and whether security policies and bandwidth policies are effective.

Procedure

- (1) Choose Monitor > Log Monitoring > Security Log.
- (2) The security log-related information is displayed on the web page.



Field	Description
Severity	Severity level of a problem marked in the security log.
Security Event	Description of a security event recorded in the log.
Log Type	Type of a security event recorded in the log. [Example] IPS attack
Attack Type	Type of the attack recorded in the log. [Example] Heap Overflow
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. 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.
APP	Application type of the session recorded in the log.
Action	Operation result of a security policy on the traffic.

Field	Description
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 a security log.

Note

You can click **Search Criteria** to set the keywords for log query. Only security logs matching the search criteria are displayed on the page.

Follow-up Procedure

- Click **Export** to export security logs to the local device in the Excel format, facilitating subsequent query. Up to 10,000 latest logs in the list can be exported.
- Click **Export All** to export security logs as a compressed package and save it locally for subsequent query. Logs generated within one month can be exported.
- Click **Refresh** to obtain the latest security logs.

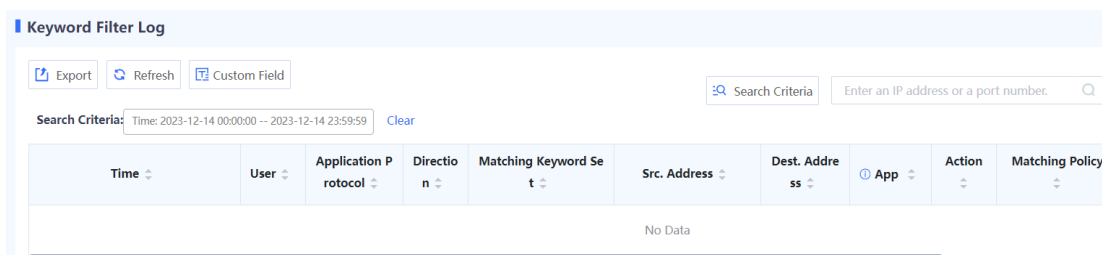
9.3.3 Querying Keyword Filter Logs

Application Scenario

By viewing the logs, administrators can check the hit status of the keyword filtering templates.

Procedure

- (1) Choose Monitor > Log Monitoring > Keyword Filter Log.
- (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.

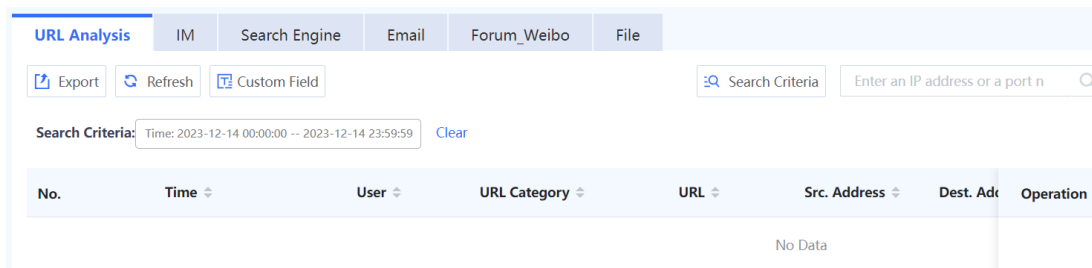
9.3.4 Querying Behavior Analysis Logs

Application Scenario

Content types that support analysis include URL, IM, email, search engine, Weibo posting, forum posting, and files. Logs are generated for administrators to check behavior analysis information.

Procedure

- (1) Choose Monitor > Log Monitoring > Behavior Analysis Log.
- (2) The behavior analysis information is displayed on the web page.



Note

You can click **Search Criteria** to set the keywords for log query. Only behavior analysis logs matching the search criteria are displayed on the page.

Follow-up Procedure

- Click **Export** to export behavior analysis 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 behavior analysis logs.

9.3.5 Querying Session Logs

Application Scenario

By querying session logs, the administrator can view detailed information of each data flow, including 5-tuple information of the data flow (source IP address, source port, destination IP address, destination port, and protocol) as well as the security policy hit by the data flow and the application carried in the data flow.

Procedure

- (1) Choose Monitor > Log Monitoring > Session Log.
- (2) The session log-related information is displayed on the web page.

Session Log

Export Search Criteria Custom Field Refresh 2023-12-14 Start Time 11:00:00 End Time 11:59:59 Enter an IP address or a port number.

Search Criteria: Log Record Time: 2023-12-14 11:00:00 -- 2023-12-14 11:59:59 Clear

Log Record Time	Session Duration	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	User	Forward Packets	Forward Bytes	Reverse Packets	Reverse Bytes	Security Policy	Operation
2023-12-14 11:00:00	12Second	10.51.210.92	10.51.21...	59607	161	UDP	Applicati...	10.51.21...	3	240	-	-	__visit_lo...	View Details
2023-12-14 11:00:00	12Second	10.51.212.212	10.51.21...	58649	58649	ICMP	Echo-re...	10.51.21...	1	84	1	84	__visit_lo...	View Details
2023-12-14 11:00:00	12Second	10.51.212.212	172.30.4...	58648	58648	ICMP	Echo-re...	10.51.21...	1	84	1	84	__visit_lo...	View Details
2023-12-14 11:00:00	42Second	10.51.212.210	10.51.21...	37652	22	TCP	SSH	10.51.21...	43	5269	34	4734	__visit_lo...	View Details
2023-12-14 11:00:00	2Second	10.51.212.212	10.51.21...	48752	53	UDP	UDP-DNS	10.51.21...	1	61	1	301	__visit_lo...	View Details
2023-12-14 11:00:00	2Second	10.51.212.212	172.30.4...	40687	53	UDP	UDP-DNS	10.51.21...	1	61	1	77	__visit_lo...	View Details
2023-12-14 11:00:00	11Second	10.51.210.92	10.51.21...	59602	161	UDP	Applicati...	10.51.21...	3	240	-	-	__visit_lo...	View Details
2023-12-14 11:00:00	11Second	10.51.212.212	172.30.4...	58647	58647	ICMP	Echo-re...	10.51.21...	1	84	1	84	__visit_lo...	View Details
2023-12-14 11:00:00	11Second	10.51.212.212	10.51.21...	58646	58646	ICMP	Echo-re...	10.51.21...	1	84	1	84	__visit_lo...	View Details
2023-12-14 11:00:00	11Second	10.51.212.212	10.51.21...	40752	22	TCP	SSH	10.51.21...	12	2330	12	2333	__visit_lo...	View Details

Note

You can click **Search Criteria** to set the keywords for log query. Only session logs matching the search criteria are displayed on the page.

Follow-up Procedure

- Click **Export** to export session logs to the local device in the Excel format, facilitating subsequent query.
- Click **Custom Field** to set the fields to be displayed on the page.
- Click **Refresh** to obtain the latest session logs.

9.3.6 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 Monitor > Log Monitoring > Operation Log.

Operation Log

Export Refresh Search Criteria Enter an IP address.

Search Criteria: Time Range: 2024-01-15 00:00:00 -- 2024-01-15 23:59:59 Admin: All Users Source: All Types Clear

Admin	Host IP	Operation Object	Operation	Operation Time	Source	Description	Operation
admin	10.52.0.83	User logs in	Log in	2024-01-15 10:57:17	eweb	Log in [Success]	View Details

(2) The operation log-related information is displayed on the web page.

Field	Description
Admin	Name of the administrator who performs the operation.
Host IP	Host IP address used by the administrator to log in to the firewall.
Operation Object	Type of the object managed by the administrator.
Operation	Specific operation performed by the administrator.
Operation Time	Time when the administrator performs the operation.
Description	Description of the operation log.
Operation	Click View Details to obtain details about an operation log.

Note

You can click **Search Criteria** to set the keywords for log query. Only operation logs matching the search criteria are displayed on the page.

Follow-up Procedure

- Click **Export** to export operation logs to the local device in the Excel format, facilitating subsequent query.
- Click **Refresh** to obtain the latest operation logs.

9.4 Traffic Monitoring

9.4.1 Interface Traffic

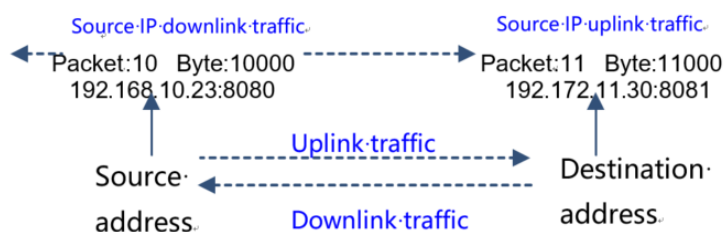
Application Scenario

You can use the interface traffic monitoring function to display the trend of uplink and downlink traffic on a specific interface. This function provides administrators with valuable insights into the current network traffic status, enabling them to take appropriate traffic management measures.

Background

- Uplink traffic: traffic transmitted from the interface.
- Downlink traffic: traffic received by the interface.

The following figure shows the uplink traffic and downlink traffic:



Procedure

- (1) Choose **Monitor > Traffic Monitoring > Interface Traffic**.
- (2) Click **Interface Traffic Statistics**, select the interface to be queried, and then set the query cycle. The system displays the interface traffic trend chart, including the uplink traffic and downlink traffic.



- (3) Click **Interface Traffic Details** to view the detailed traffic information of the interface.

The screenshot shows the 'Interface Traffic Statistics' page with the 'Interface Traffic Details' tab selected and highlighted with a red box. The page includes 'Export' and 'Refresh' buttons, and a search box for 'Enter an interface name.'. Below is a table listing interface traffic details.

<input type="checkbox"/>	Interface	Interface Status	Zone	IP	Uplink	Downlink
<input type="checkbox"/>	Ge0/0		trust	10.51.212.212/24	9.46Kbps	3.18Kbps
<input type="checkbox"/>	Ge0/1		zone1	10.10.10.1/24 2000:10::1/64	2.82Mbps	47.89Kbps
<input type="checkbox"/>	Ge0/2		zone2	20.20.20.1/24 2000:20::1/64	50.44Kbps	2.79Mbps
<input type="checkbox"/>	Ge0/3				0bps	0bps
<input type="checkbox"/>	Ge0/4		test3		0bps	0bps
<input type="checkbox"/>	Ge0/5		zone4	42.194.197.1/24	0bps	0bps
<input type="checkbox"/>	Ge0/6		trust		0bps	0bps
<input type="checkbox"/>	Ge0/7		untrust		0bps	0bps
<input type="checkbox"/>	TenGe0/0		monitor		0bps	0bps

Follow-up Procedure

- Click **Export** to export interface traffic information to the local device in the Excel format.
- Click **Refresh** to obtain the latest interface traffic information.

9.4.2 Real-Time Traffic


Application Scenario

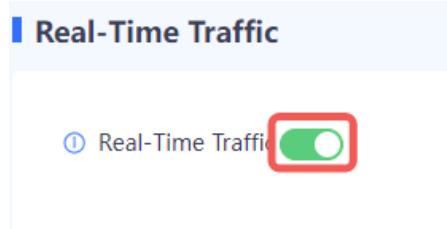
Enable this function to display the distribution of real-time uplink and downlink traffic on interfaces.

Precautions

- If no hard disk is installed, only real-time traffic information can be displayed.
- If a hard disk is installed, you can specify a time range for querying the real-time traffic information of the device.

Procedure

- (1) Choose **Monitor > Traffic Monitoring > Real-Time Traffic**.
- (2) Toggle on  to enable real-time traffic statistics.

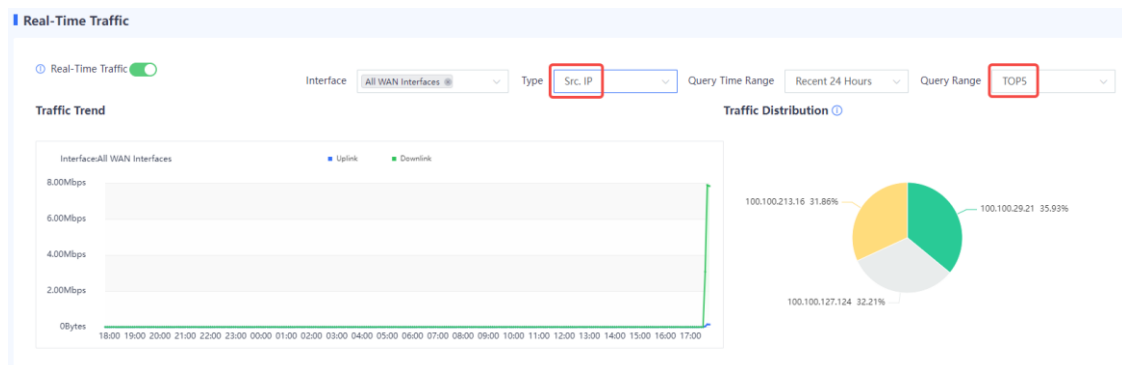


- (3) Set the traffic range for statistics collection. Traffic statistics can be collected based on the source IP address, application, and user.

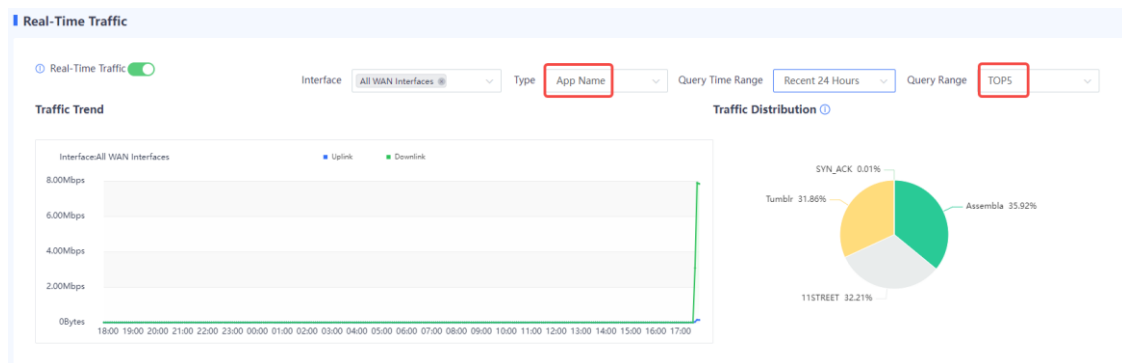
Note

Set **Interface** to view traffic statistics on specified interfaces. Set **Query Time Range** to view real-time traffic statistics or traffic statistics within the last 24 hours or 7 days. Set **Query Range** to view traffic distribution statistics in a specified range.

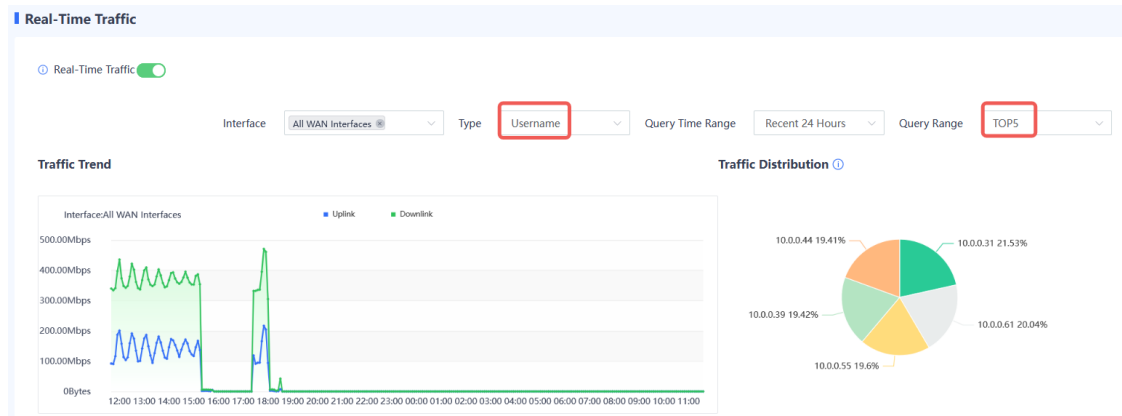
- o Set **Type** to **Src. IP** to display top 5 source IP addresses with the highest traffic and corresponding traffic information.



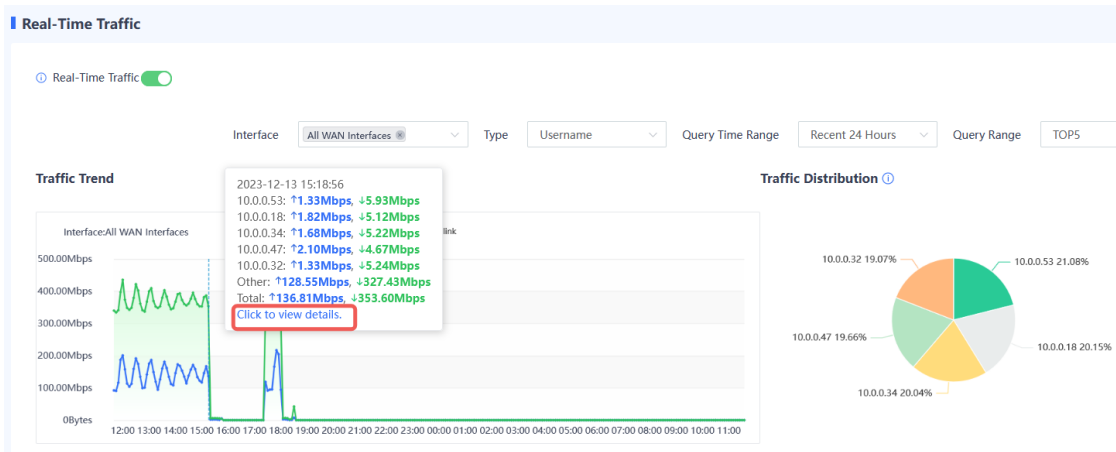
- o Set **Type** to **App Name** to display top 5 applications with the highest traffic and corresponding traffic information.



- o Set **Type** to **Username** to display top 5 users with the highest traffic and corresponding traffic information.



- (4) Click the line chart to view the traffic ranking list.



Ranking List

The current interface is All WAN Interfaces. Uplink traffic: traffic sent from the interface. Downlink traffic: traffic received by the interface.

Time: 2023-12-13 15:23:56 Query Range: TOP5 Type: Username

Ranking	Username	Uplink Traffic(kbps) (Forward/Suppress)	Downlink Traffic(kbps) (Forward/Suppress)	Total Traffic(kbps) (Forward/Suppress)
1	10.0.0.58	20.785/0	153.443/0	174.228/0
2	10.0.0.33	51.902/0	104.611/0	156.513/0
3	10.0.0.78	39.744/0	82.008/0	121.752/0
4	10.0.0.41	14.649/0	106.752/0	121.401/0
5	10.0.0.32	4.99/0	111.236/0	116.226/0

- (5) Select **Separate VPN and Non-VPN Traffic** to view details about VPN and non-VPN traffic.

Ranking List

The current interface is All WAN Interfaces. Uplink traffic: traffic sent from the interface. Downlink traffic: traffic received by the interface.

Time: 2023-12-13 15:23:56 Query Range: TOP5 Type: Username Enter a username. Separate VPN and Non-VPN Traffic Export

Ranking	Username	VPN Uplink Traffic(kbps) (Forward/Suppress)	Non-VPN Uplink Traffic(kbps) (Forward/Suppress)	VPN Downlink Traffic(kbps) (Forward/Suppress)	Non-VPN Downlink Traffic(kbps) (Forward/Suppress)	Total Traffic(kbps) (Forward/Suppress)
1	10.0.0.58	20.785/0	0/0	153.443/0	0/0	174.228/0
2	10.0.0.33	51.902/0	0/0	104.611/0	0/0	156.513/0
3	10.0.0.78	39.744/0	0/0	82.008/0	0/0	121.752/0
4	10.0.0.41	14.649/0	0/0	106.752/0	0/0	121.401/0
5	10.0.0.32	4.99/0	0/0	111.236/0	0/0	116.226/0

Follow-up Procedure

Ranking List

The current interface is All WAN Interfaces. Uplink traffic: traffic sent from the interface. Downlink traffic: traffic received by the interface.

Time: 2023-12-13 15:23:56 Query Range: TOP5 Type: Username Enter a username. Separate VPN and Non-VPN Traffic Export

Ranking	Username	VPN Uplink Traffic(kbps) (Forward/Suppress)	Non-VPN Uplink Traffic(kbps) (Forward/Suppress)	VPN Downlink Traffic(kbps) (Forward/Suppress)	Non-VPN Downlink Traffic(kbps) (Forward/Suppress)	Total Traffic(kbps) (Forward/Suppress)
1	10.0.0.58	20.785/0	0/0	153.443/0	0/0	174.228/0
2	10.0.0.33	51.902/0	0/0	104.611/0	0/0	156.513/0
3	10.0.0.78	39.744/0	0/0	82.008/0	0/0	121.752/0
4	10.0.0.41	14.649/0	0/0	106.752/0	0/0	121.401/0
5	10.0.0.32	4.99/0	0/0	111.236/0	0/0	116.226/0

- Enter an application name, source IP address, or username in the search box to query the traffic details about a specified object.
- Click **Export** to export the ranking list and save it locally.

9.4.3 Traffic Statistics

Application Scenario

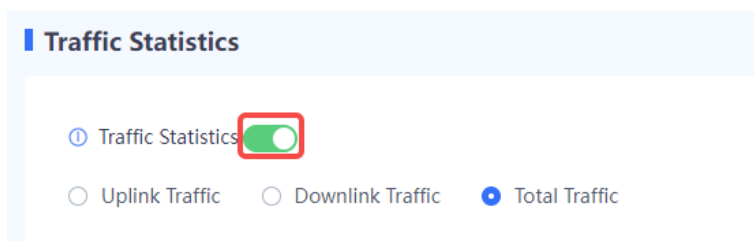
Enable this function to display the distribution of historical uplink and downlink traffic on interfaces.

Precautions

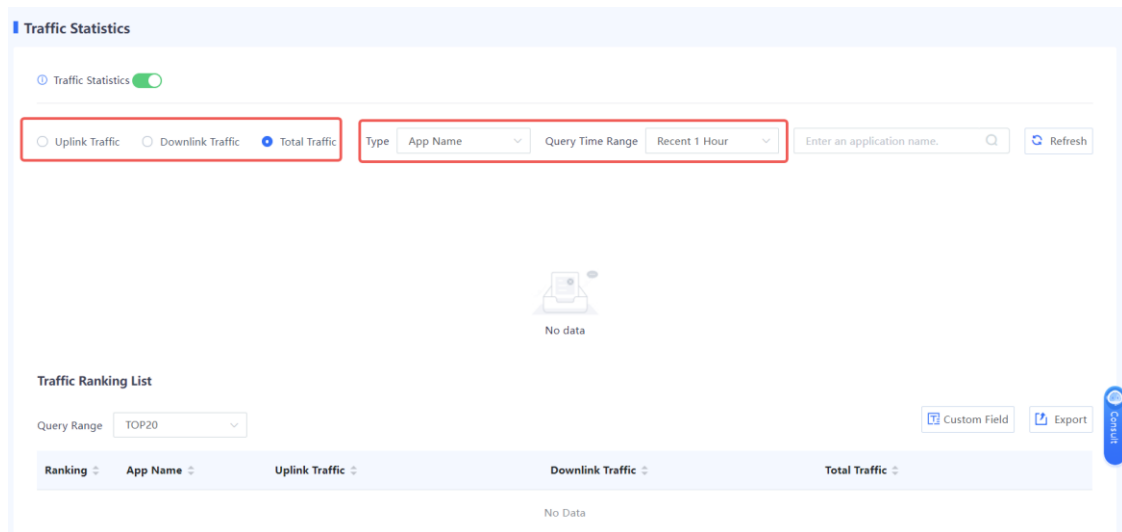
- If no hard disk is installed, only traffic statistics in the last 1 hour can be displayed.
- If a hard disk is installed, you can specify a time range for querying the traffic statistics of the device.

Procedure

- (1) Choose **Monitor > Traffic Monitoring > 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.
- 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.

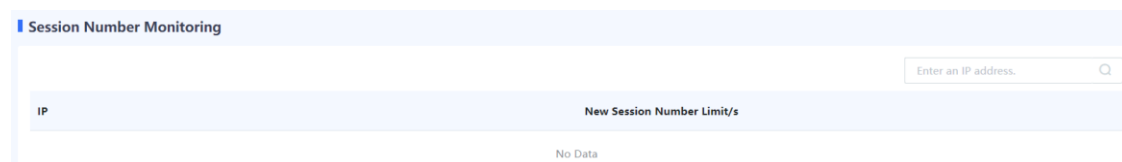
9.4.4 Session Number Monitoring

Application Scenario

The device counts the number of new sessions established per second based on the source IP addresses of packets. You can check the statistics to determine whether attacks exist on the network and configure session suppression policies to limit the rate of new sessions accordingly. After session suppression is configured, you can also check whether session suppression takes effect on the **Session Number Monitoring** page. For details about session suppression configuration, see 2. [Configuring the New Session Limit](#).

Procedure

- (1) Choose Monitor > Traffic Monitoring > Session Number Monitoring.
- (2) The source IP addresses of sessions and the numbers of new sessions per second are displayed.



9.5 Session Monitoring

9.5.1 Overview

The firewall displays the status of a connection established between two parties in the communication by session. One session indicates a connection between the communicating parties. A session records 5-tuple information

(source IP address, source port, destination IP address, destination port, and protocol) of a connection. Packets with the same 5-tuple information belong to the same connection, that is, the same session.

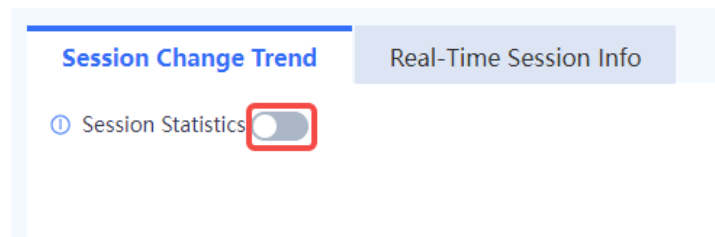
9.5.2 Session Change Trend

Application Scenario

The session change trend function supports real-time monitoring and visualization of the changes in new sessions and concurrent sessions (including average and peak values of new session rates and numbers of concurrent sessions) within a specified time period.

Procedure

- (1) Choose **Monitor > Traffic Monitoring > Session > Session Change Trend**.
- (2) Toggle on **Session Statistics**.



- (3) In the dialog box that is displayed, click **OK**.

Tip



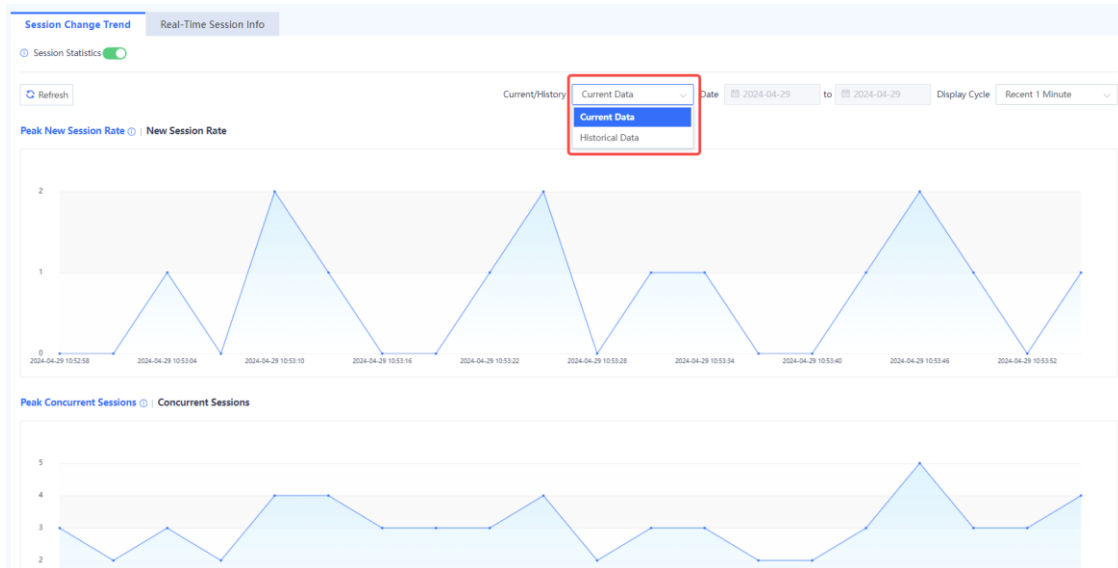
! Are you sure you want to enable real-time session statistics?

When this function is enabled, the device performance is greatly affected.

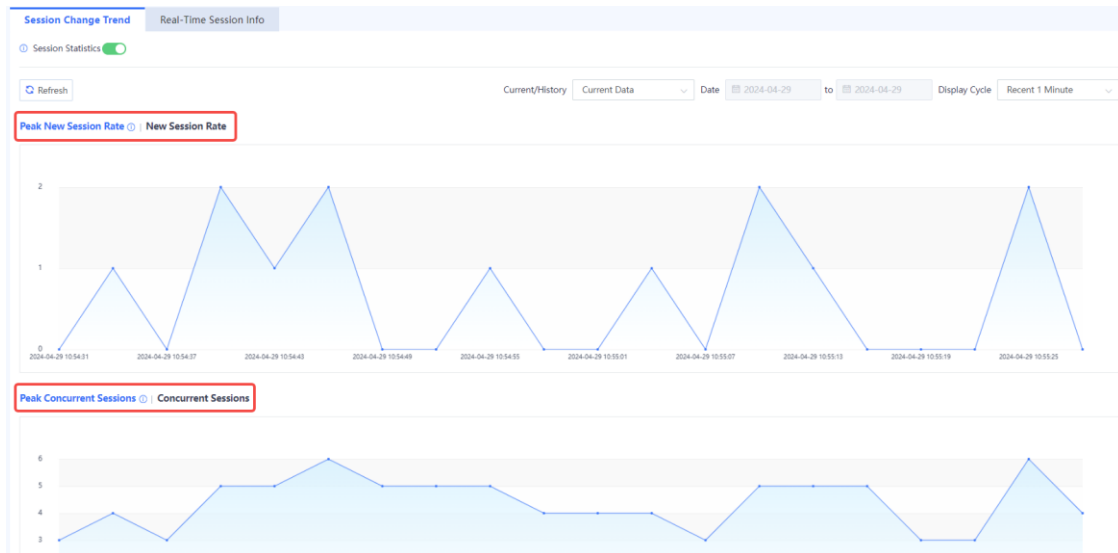
OK

Cancel

- (4) You can query current or historical data:
 - o **Current Data**: displays trends in new and concurrent sessions over the last 24 hours.
 - o **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.



9.5.3 Real-Time Session Information

Application Scenario

The real-time session information function is used to collect and display the current number of sessions. You can block a session based on service needs. After a session is blocked, the firewall discards subsequent packets transmitted over this session and the session is no longer displayed on the page.

Procedure

- (1) Choose Monitor > Traffic Monitoring > Session > Real-Time Session Info.
- (2) Select the desired session and click **View Details** to view the session creation time, hit security policy, number of forward packets, and number of reverse packets.

Session Change Trend		Real-Time Session Info										
<input type="checkbox"/> Block	<input type="text" value="Search Criteria"/>	<input type="text" value="Custom Field"/>	<input type="button" value="Refresh"/>								Refresh Interval	30s
Search Criteria: Session Creation Time: 60Minute <input type="button" value="Clear"/>												
<input type="checkbox"/>	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Security Policy	Operation		
<input type="checkbox"/>	2023-07-28 17:42:19	29Minute58Second	172.17.97.28	10.51.212.212	53302	443	TCP	HTTPSprotocol	__visit_local__	Block View Details		
<input type="checkbox"/>	2023-07-28 17:42:19	29Minute58Second	172.17.97.28	10.51.212.212	53304	443	TCP	HTTPSprotocol	__visit_local__	Block View Details		
<input type="checkbox"/>	2023-07-28 17:32:42	28Minute14Second	10.52.24.249	10.51.212.212	10863	22	TCP	SSH	__visit_local__	Block View Details		
<input type="checkbox"/>	2023-07-28 17:42:19	29Minute58Second	172.17.97.28	10.51.212.212	53303	443	TCP	HTTPSprotocol	__visit_local__	Block View Details		
<input type="checkbox"/>	2023-07-28 17:28:56	22Minute19Second	100.100.121.50	200.200.116.196	56419	443	TCP	Global New	L7	Block View Details		
<input type="checkbox"/>	2023-07-28 17:42:19	29Minute58Second	172.17.97.28	10.51.212.212	53306	443	TCP	HTTPSprotocol	__visit_local__	Block View Details		
<input type="checkbox"/>	2023-07-28 17:34:45	25Minute57Second	100.100.44.200	200.200.160.243	50197	443	TCP	NBC News	L7	Block View Details		
<input type="checkbox"/>	2023-07-28 17:30:17	29Minute58Second	10.51.212.212	34.111.156.117	34854	5683	TCP	HTTPSprotocol	__visit_local__	Block View Details		
<input type="checkbox"/>	2023-07-28 17:32:38	29Minute1Second	10.51.212.212	47.104.206.152	44440	25857	TCP	HTTPSprotocol	__visit_local__	Block View Details		
<input type="checkbox"/>	2023-07-28 17:41:20	30Minute0Second	100.100.213.16	200.200.107.6	53791	443	TCP	Tumblr	L7	Block View Details		

Session Description



Basic Info

Session Creation Time:2023-03-15 00:06:55 Time Before Session Timeout:1Second

Src. and Dest.

Src. Address:10.101.1.102 Dest. Address:172.20.37.124

Src. Port:7807 Dest. Port:443

NAT Src. Address:- NAT Dest. Address:-

NAT Src. Port:- NAT Dest. Port:-

More

Protocol:TCP App:HTTPSprotocol

Inbound Interface:Ge0/7 Outbound Interface:lo

Forward Packets:7 Forward Bytes:816

Reverse Packets:4 Reverse Bytes:320

Security Policy:local Session State:connection being closed and connection resources being reclaimed

Disable

(3) (Optional) Click **Search Criteria** to set the criteria for filtering sessions.

Session Change Trend **Real-Time Session Info**

Block Refresh Interval: 30s

Search Criteria: Session Creation Time: 60Minute

<input type="checkbox"/>	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Security Policy	Operation
<input type="checkbox"/>	2023-07-28 17:43:19	2Second	10.52.24.249	10.51.212.212	4894	443	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:32:42	27Minute16Second	10.52.24.249	10.51.212.212	10863	22	TCP	SSH	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:28:56	21Minute21Second	100.100.121.50	200.200.116.196	56419	443	TCP	Global New	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:43:19	2Second	172.17.97.28	10.51.212.212	54171	443	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:34:45	24Minute59Second	100.100.44.200	200.200.160.243	50197	443	TCP	NBC News	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:30:17	30Minute0Second	10.51.212.212	34.111.156.117	34854	5683	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:32:38	29Minute27Second	10.51.212.212	47.104.206.152	44440	25857	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:41:20	30Minute0Second	100.100.213.16	200.200.107.6	53791	443	TCP	Tumblr	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:42:57	8Second	10.51.212.212	114.118.7.163	55213	123	UDP	ApplicationBeing Identified	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:43:19	30Minute0Second	10.52.24.249	10.51.212.212	4895	443	TCP	HTTPSprotocol	__visit_local__	Block View Details

(4) (Optional) Select one or more sessions and click **Block** to block the selected sessions.

Session Change Trend **Real-Time Session Info**

Block Refresh Interval: 30s

Search Criteria: Session Creation Time: 60Minute

<input type="checkbox"/>	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Security Policy	Operation
<input type="checkbox"/>	2023-07-28 17:42:49	30Minute0Second	172.17.97.28	10.51.212.212	53741	443	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:32:42	27Minute46Second	10.52.24.249	10.51.212.212	10863	22	TCP	SSH	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:28:56	21Minute51Second	100.100.121.50	200.200.116.196	56419	443	TCP	Global New	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:34:45	25Minute29Second	100.100.44.200	200.200.160.243	50197	443	TCP	NBC News	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:30:17	29Minute30Second	10.51.212.212	34.111.156.117	34854	5683	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:32:38	29Minute57Second	10.51.212.212	47.104.206.152	44440	25857	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:41:20	30Minute0Second	100.100.213.16	200.200.107.6	53791	443	TCP	Tumblr	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:42:33	29Minute59Second	10.51.212.210	10.51.212.212	40046	22	TCP	SSH	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:42:38	29Minute49Second	10.51.212.212	10.51.213.10	45144	22	TCP	SSH	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:42:49	2Second	172.17.97.28	10.51.212.212	53740	443	TCP	HTTPSprotocol	__visit_local__	Block View Details

(5) (Optional) Click **Custom Field** to set the session fields to be displayed on the page.

Session Change Trend **Real-Time Session Info**

Block Refresh Interval: 30s

Search Criteria: Session Creation Time: 60Minute

<input type="checkbox"/>	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Security Policy	Operation
<input type="checkbox"/>	2023-07-28 17:43:19	2Second	10.52.24.249	10.51.212.212	4894	443	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:32:42	27Minute16Second	10.52.24.249	10.51.212.212	10863	22	TCP	SSH	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:28:56	21Minute21Second	100.100.121.50	200.200.116.196	56419	443	TCP	Global New	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:43:19	2Second	172.17.97.28	10.51.212.212	54171	443	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:34:45	24Minute59Second	100.100.44.200	200.200.160.243	50197	443	TCP	NBC News	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:30:17	30Minute0Second	10.51.212.212	34.111.156.117	34854	5683	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:32:38	29Minute27Second	10.51.212.212	47.104.206.152	44440	25857	TCP	HTTPSprotocol	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:41:20	30Minute0Second	100.100.213.16	200.200.107.6	53791	443	TCP	Tumblr	L7	Block View Details
<input type="checkbox"/>	2023-07-28 17:42:57	8Second	10.51.212.212	114.118.7.163	55213	123	UDP	ApplicationBeing Identified	__visit_local__	Block View Details
<input type="checkbox"/>	2023-07-28 17:43:19	30Minute0Second	10.52.24.249	10.51.212.212	4895	443	TCP	HTTPSprotocol	__visit_local__	Block View Details

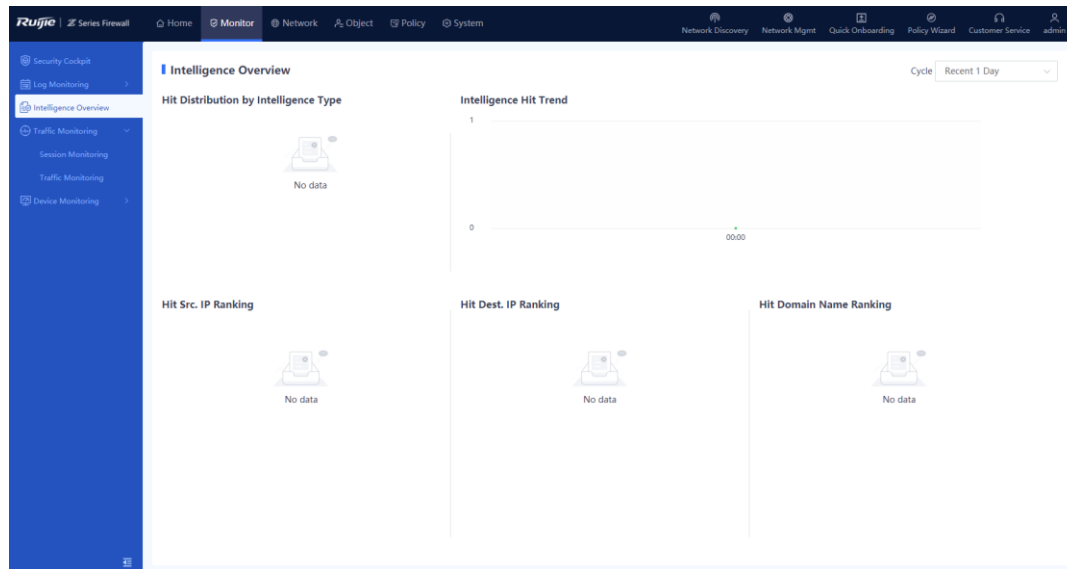
9.6 Intelligence Overview

Application Scenario

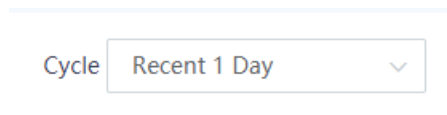
The intelligence overview function is used to display the hit distribution by intelligence type and the intelligence hit trend. This information can help administrators effectively master threats in the current network environment and then develop more refined protection policies to protect LAN hosts.

Procedure

- (1) Choose Monitor > Intelligence Overview.



- (2) Click the drop-down list box in the upper right corner of the page and set a cycle for collecting intelligence hit statistics. The system displays the intelligence hit data in the specified cycle.



- (3) View the intelligence hit data on the page. The information consists of five parts as listed in the following table.

Item	Description
Hit Distribution by Intelligence Type	Displays hit distribution by intelligence type in a pie chart. This information allows administrators to master major threats in the current network environment so that they can intensify protection accordingly. Move the pointer over this area to view the number of hits of each intelligence type and the proportion.
Intelligence Hit Trend	Displays the number of hits of threat intelligence in various periods within the statistical cycle in a line chart. This information helps administrators find periods with high occurrence of attack threats or check whether protection measures are effective. Move the pointer over the line chart to view the number of hits over each period.

<p>Hit Src. IP Ranking</p>	<p>Displays the ranking of source IP addresses with threat intelligence by the number of hits. This information helps administrators analyze the threat source and then develop corresponding protection measures to block the traffic from these source IP addresses.</p> <p>Click an IP address to switch to the security log page. Security logs of this source IP address are automatically filtered out.</p>
<p>Hit Dest. IP Ranking</p>	<p>Displays the ranking of destination IP addresses with threat intelligence by the number of hits. This information helps administrators analyze addresses of compromised hosts on the botnet or IP addresses attacked by malicious programs and then develop corresponding protection measures to protect these hosts.</p> <p>Click an IP address to switch to the security log page. Security logs of this destination IP address are automatically filtered out.</p>
<p>Hit Domain Name Ranking</p>	<p>Displays the ranking of domain name addresses with threat intelligence by the number of hits. This information helps administrators analyze malicious domain names and then develop corresponding protection measures to block and protect the traffic from these domain names.</p> <p>Click a domain name to switch to the security log page. Security logs of this domain name are automatically filtered out.</p>

10 Advanced Features

10.1 ALG

10.1.1 Overview

Application Level Gateway (ALG) analyzes application layer packet information using the multi-channel protocol and performs address translation on the IP address, port number, and special fields in the payload to ensure correct communication at the application layer. For special applications such as TFTP and FTP, data ports must be randomly enabled according to the session process. The Z-S series firewall can identify these protocols and dynamically enable or disable ports during the session control process to guarantee application availability to the maximum extent.

Related Concepts

- **Session:** A session records packet exchange information at the transport layer, including the source IP address, source port, destination IP address, destination port, protocol type, and VPN instance to which the source/destination IP address belongs. Exchange information of the same packet belongs to the same flow. One session corresponds to two flows in the forward and reverse directions.
- **Dynamic channel:** When an application layer protocol packet contains address information, the address information is used to set up a dynamic channel. After that, packets from this address are automatically transmitted over this dynamic channel.

Technical Principles

The ALG feature can be used with the NAT feature to implement address translation on the packet payload and be used with the Application Specific Packet Filter (ASPF) feature to implement dynamic channel detection and application layer status detection.

For a multi-channel application protocol, address information in the data payload of IP packets must be translated to ensure successful setup of subsequent dynamic channel on a NAT-enabled network. The role of ALG is to implement address translation on the payload.

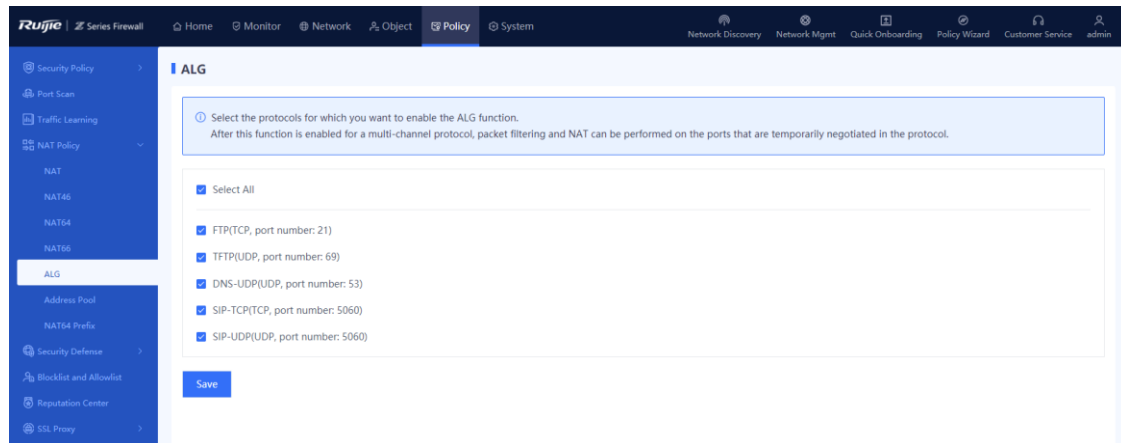
10.1.2 Configuring ALG

Application Scenario

ALG guarantees normal packet filtering and NAT based on the temporarily negotiated port number when a multi-channel protocol is used for data transmission.

Procedure

- (1) Choose Policy > NAT Policy > ALG.



(2) Select the protocol names for which ALG needs to be enabled and click **Save**.

After the ALG function is enabled, information in the packets of these protocols can be translated by NAT.

11 FAQs

11.1 Product Knowledge

11.1.1 What Is the Hardware Architecture of the RG-WALL 1600-Z-S Series Firewall?

The RG-WALL 1600-Z-S series firewall uses a hardware architecture with multi-core CPU and multiple ASIC chips. With the onboard design for the CPU memory, the firewall supports ECC, hardware flow attack defense, dual-boot instruction to reduce the probability of device start failures caused by boot problems. The design of multiple ASIC chips enables the firewall to support eight electrical ports, two GE optical ports, and four 10GE optical ports.

The performance of the RG-WALL 1600-Z-S series firewall can be expanded through license authorization, capable for all the 3G–10G forwarding scenarios. Apart from software performance expansion, the hardware can also be well expanded. The firewall supports two expansion slots and can be expanded to support 40GE port, 4GE electrical port + 4GE optical port, redundant power modules, and 1 TB hard disk.

The overall hardware design adopts the area-based power solution to avoid whole machine restart caused by short circuit of the USB drive or optical module.

11.1.2 What Are the Restrictions of Port MGMT?

It is not recommended to use port MGMT as a service port, and port MGMT cannot be configured to work in transparent or off-path mode.

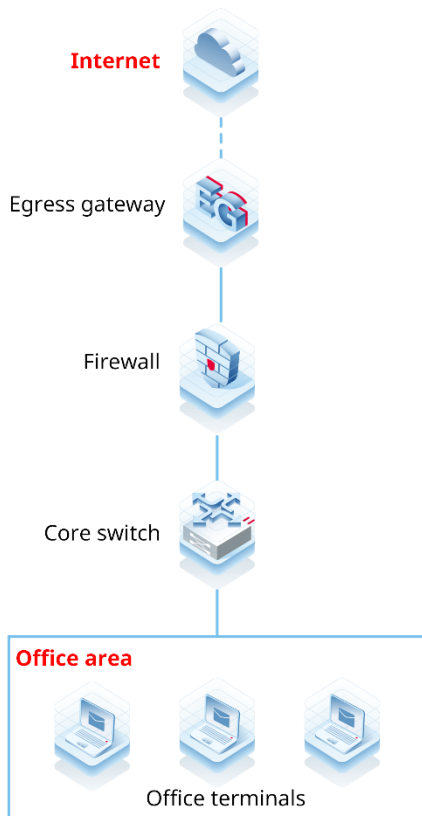
11.2 Firewall Deployment

11.2.1 What Firewall Deployment Modes Are Supported?

As a security device used to protect the network infrastructure, the Z-S series firewall can be widely used on various types of networks. The Z-S series firewall supports multiple deployment modes and network features to adapt to diversified network environments. The major deployment modes of the Z-S series firewalls include:

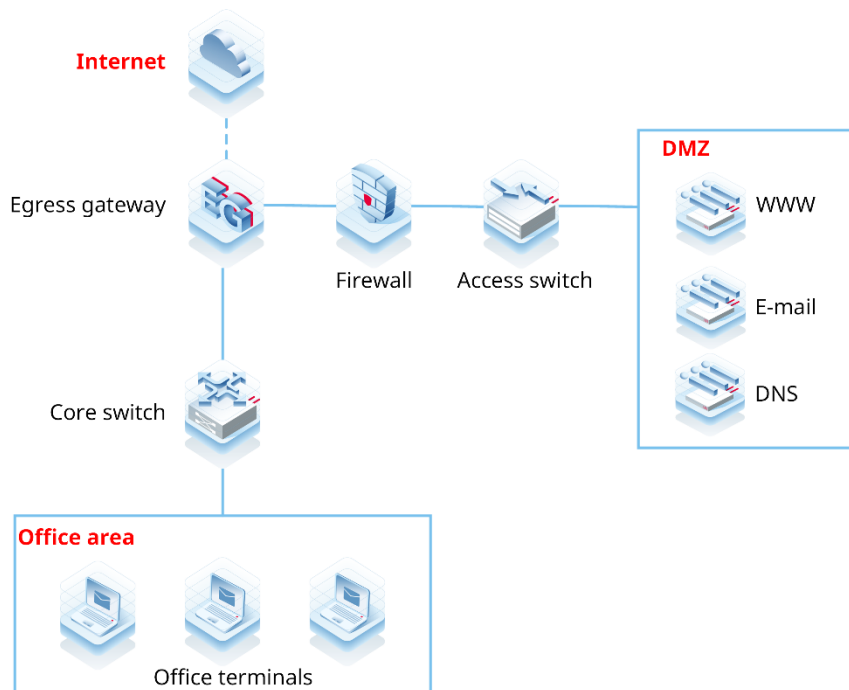
- Transparent mode - office network egress link - single-in single-out

Scenario overview: The firewall is transparently deployed between the egress gateway and core switch through one GE electrical port on each side. Access control policies, IPS policies, DDoS policies, and application control policies are enabled on the firewall to control and protect assets on the public network.



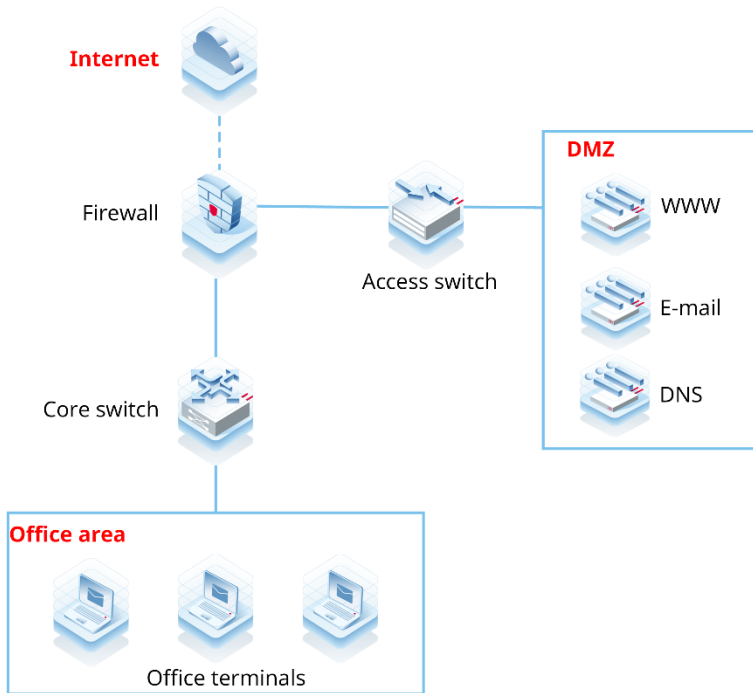
- Transparent mode – area boundary - single-in single-out

Scenario overview: The firewall is transparently deployed at an area boundary (such as the DMZ) between the egress gateway and access switch through one GE electrical port on each side. The firewall generates refined access control policies for users through port scan and traffic learning and is enabled with IPS, DDoS, and application control to control and protect assets (such as servers providing services to external users) in an area.



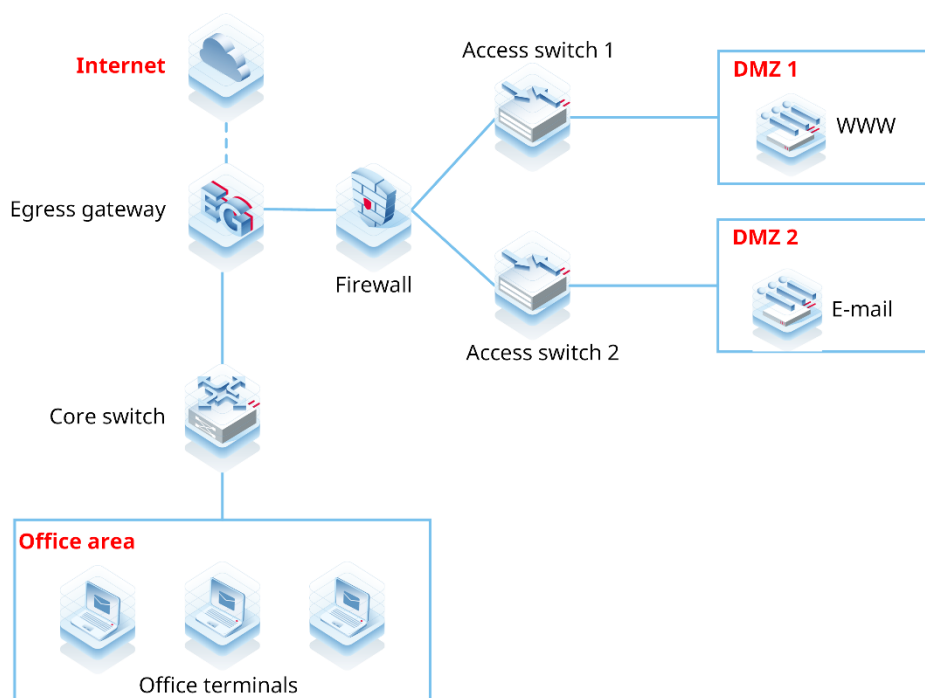
- Gateway mode - single ISP access

Scenario overview: The firewall is deployed at the Internet egress in gateway mode and is connected to a single ISP. The WAN GE port is configured with DHCP or a fixed IP address. The firewall connects to the LAN office area and the DMZ server area through GE electrical ports. NAT and DHCP are enabled on the firewall to allow office terminals to access the Internet. Access control policies, IPS policies, DDoS policies, and application control policies are enabled on the firewall through port scan and traffic learning to control and protect assets and servers on the office network.



- Transparent mode - multi-in single-out

Scenario overview: The firewall is transparently deployed on the network. It connects to the LAN areas through multiple ports and connects to the Internet through the same WAN port to provide services to external users.



11.2.2 Can GE Optical Port and 10GE Optical Port Form a Bridge?

The GE optical port and 10GE optical port can form a bridge.

11.3 Typical Feature Configuration

11.3.1 How Is Source NAT Implemented?

Source NAT means source network address translation for packets, which is implemented through NAT policies. You need to specify the source security zone, source address, destination security zone, destination address, and data packet after translation in a NAT policy.

11.3.2 Does the Firewall Support Link Detection?

The firewalls running NTOS1.0R3 and later versions support link detection.

11.3.3 Does the Z-S Series Firewall Block TCP Sessions in the Secondary Traversal Scenario?

If the same flow passes through a firewall twice, the session status on the firewall is affected, thereby affecting the security functions of the firewall. Therefore, avoid such a scenario in actual service running.

If such a scenario is unavoidable, disable the TCP status detection function to ensure normal traffic forwarding. After this function is disabled, the effects of security functions related to sessions such as IPS and AV will be significantly reduced.

11.3.4 Does the Firewall Support Link Aggregation?

The firewall supports link aggregation. Aggregation is only supported for physical interfaces of the same type with the same bandwidth. For example, 1GE Ethernet ports and 1GE SFP/SFP+ ports cannot be aggregated, and 1GE SFP/SFP+ ports and 10GE SFP/SFP+ ports cannot be aggregated.

Management ports do not support link aggregation.

11.4 Login Management

11.4.1 What Can I Do If I Fail to Log In to the Web Page?

Possible Causes

- The firewall is not fully started.
- A network connection error occurs between the PC and firewall.
- The address `https://Device IP address` is incorrect. (The default address `https://192.168.1.200` can be used.)
- The browser is incompatible.

Solution

- (1) Wait for about 2 minutes until the firewall is started. Observe indicators (including PWR, SYS, and interface status indicators) on the firewall until all of them are on and try again.
- (2) Check the Link/ACT indicator on the interface. If the indicator is blinking green or steady on, the connection is normal. Check whether the IP addresses of the PC and firewall are on the same network segment. (The default address `192.168.1.9` can be used.)
- (3) Confirm that the address (`https://Device IP address`) entered in the address bar is correct. (The default address `https://192.168.1.200` can be used.)
- (4) Change the browser.

11.4.2 What Can I Do If I Fail to Log In to the System Through SSH?

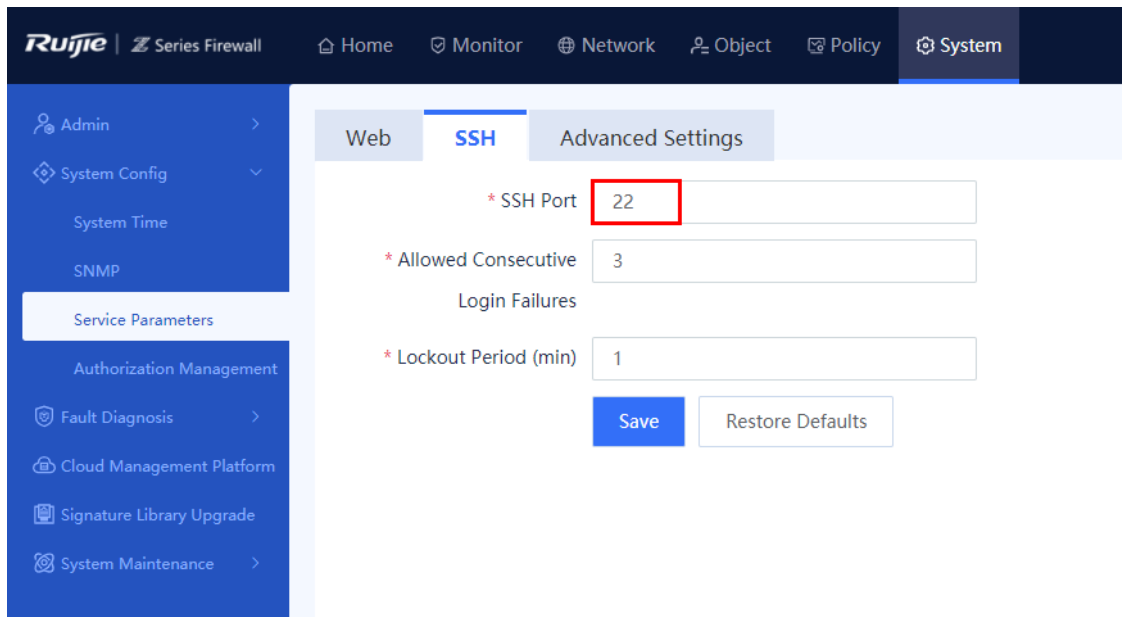
Possible Causes

The SSH port number is incorrect.

Solution

- (1) Check the network connection.
- (2) If the network connection is normal, choose **System > System Config > Service Parameters > SSH** and modify the SSH port number.

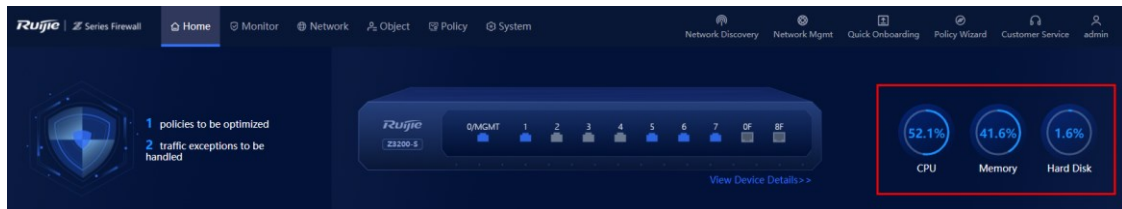
Figure 11-1 Modifying the SSH Port Number



11.5 O&M and Monitoring

11.5.1 How Do I View the CPU, Memory, and Hard Disk Information of the Firewall?

Log in to the web management page, and view the CPU, memory, and hard disk usage on the home page.



11.5.2 How Do I View the Interface Traffic of the Firewall?

Log in to the web management page, choose **Monitor > Traffic Monitoring > Interface Traffic > Interface Traffic Statistics**, and view the interface traffic.



Select an interface and set the display cycle to view the real-time traffic or traffic trend of the interface.

12 Troubleshooting

12.1 Security Policy

12.1.1 Principle

- (1) The NGFW uses security policies to control data flows in a unified manner and facilitate user configuration and management. Security policies can be configured on the firewall to effectively control and manage data flows passing through it.
- (2) After a firewall receives a data packet, the firewall matches the packet information including the direction, source address, destination address, protocol, and port number with security policies configured by the user to determine whether to set up a data flow. After a data flow is set up, the firewall associates the data flow with a policy to permit or discard subsequent packets transmitted over this data flow. You can determine whether to perform Layer 7 service processing on the permitted data flows.
- (3) Layer 7 service processing means that the firewall can block data flows or generate alarms based on the IPS and virus protection rules. The firewall permits data flows that do not match any IPS or virus protection rule.
- (4) If no security policy is configured, the system has a default policy in which all items are set to **any** and the action is **Deny**. In this case, the firewall blocks all the data flows passing through it.
- (5) Security policies are matched from up down to process data flows passing through the firewall. They do not apply to data flows destined to the firewall or data flows sent by the firewall.

12.1.2 Configuration Points of Security Policies

Basic elements of a security policy include matching condition and action. Matching conditions include the data flow direction, source address, destination address, service, and policy effective time range.

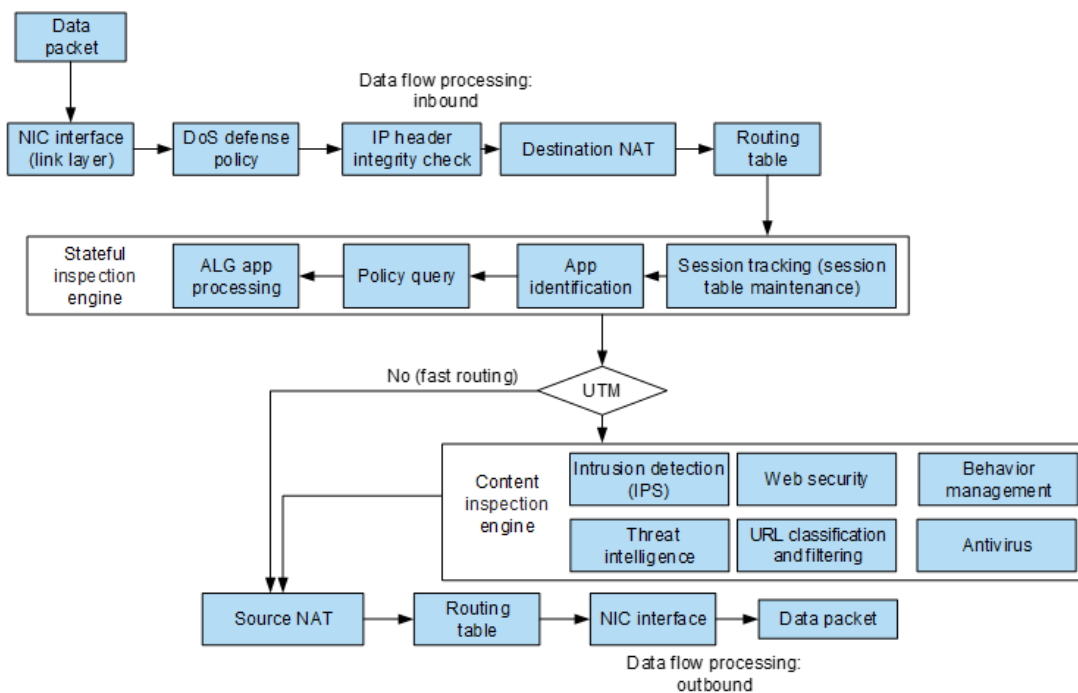
The data flow direction is determined by the source security zone and destination security zone, while the source address, destination address, service, and time range can directly reference defined objects.

- (1) Source security zone: Incoming direction of a data flow, which must be a defined security zone. The value **any** indicates all security zones.
- (2) Source address: Source address of a data flow, which can be referenced from a defined address object or address group object. The value **any** indicates any source address.
- (3) Destination security zone: Outgoing direction of a data flow, which must be a defined security zone. The value **any** indicates all interfaces.
- (4) Destination address: Destination address of a data flow, which can be referenced from a defined address object or address group object or be referenced from a virtually mapped IP address.
- (5) Policy effective time range: Time when a policy takes effect, which can be referenced from a configured time object. The value **any** indicates all the time.
- (6) Service: Service attributes of a data flow, including the protocol, source port, and destination port, which can be referenced from a system pre-defined service or a defined service object or service group object. The value **any** indicates all services.
- (7) Application: Application type of a data flow. The value **any** indicates any application.

- (8) Action: Action performed on data flows meeting the matching conditions. The action can be **Permit** or **Deny**.
- (9) Content security: Content template that can be selected for permitted data flows. The firewall matches the data flows based on rules in the selected template. Currently, only URL filtering, intrusion prevention, and virus protection templates are supported.

12.2 Data Packet Processing

The following figure shows data packet processing of the firewall.



- (1) NIC interface (link layer): The NIC interface drive is responsible for receiving data packets and forwarding the packets to the next node.
- (2) DoS defense policy (disabled by default): The DoS defense policy is responsible for filtering out DoS attacks such as SYN flood, UDP flood, and ICMP flood and limiting the number of concurrent connections of the specified source or destination IP address.
- (3) IP header integrity check: The firewall checks the integrity of the data packet header.
- (4) Destination NAT: The firewall checks the destination IP address in the data packet. If the destination IP address is in the virtual IP (destination NAT) table, the firewall translates the destination IP address into a mapped IP address (real IP address) and port number.
- (5) Routing table: The firewall determines the outbound interface of the data packet based on the destination IP address.
- (6) Stateful inspection engine: The stateful inspection engine consists of the following components:
 - o Policy query: In the session setup stage, this module determines whether to allow data to pass, sets up a session, and determines whether to send the data to the flow-based inspection engine and proxy-based inspection engine based on whether the Unified Threat Management (UTM) function is enabled.
 - o Session tracking: This module maintains the session table and tracks the session status, NAT, and other relevant functions. After a session is set up, the firewall no longer matches policies for subsequent data

packets but directly forwards the packets based on the session status.

- o ALG application processing: This module can dynamically enable policies, be enabled with NAT, automatically modify the payload, and take other measures to ensure normal communication of special applications such as FTP and TFTP.
- o Application identification: This module identifies and classifies session traffic based on traffic characteristics, such as domain names and certificates.

(7) The content inspection engine consists of the following components:

- o IPS: By performing in-depth detection on the traffic passing through the firewall in real time, IPS can identify malicious information hidden in traffic, and report alarms and block traffic in real time to protect user hosts from malicious traffic.
- o Web security: This module performs in-depth detection on traffic accessing the web server in real time to detect threats and defend against them. By performing in-depth detection and semantic detection on the traffic passing through the firewall in real time, the web security module can identify malicious information hidden in traffic, and report alarms and block traffic to protect user hosts and the web server from malicious traffic.
- o Behavior management and analysis: Behavior analysis and management can be performed based on applications accessed by users.
- o Threat intelligence: Drawing on quality threat intelligence sources in the industry, the threat intelligence function of Ruijie Networks features millions of Indicators of Compromise (IOCs) with high accuracy and timeliness. It is a powerful tool for detecting mining, ransomware, trojans, and other malware that cause host failures.
- o URL classification and filtering: URL classification and filtering are performed on network traffic based on the URLs carried in the traffic.
- o Antivirus: The antivirus function conducts in-depth analysis on the protocol content in the traffic, restores the bearer files in the protocol, and performs security check on the files.

(8) Source NAT: If NAT is enabled in a policy, the firewall translates the source IP address and source port of a data packet into the destination interface address or an IP address in an IP address pool (typically a public network IP address).

(9) Routing table: The firewall determines the outbound interface of a data packet and forwards the data packet using the routing engine.

(10) NIC interface (outbound): The outbound NIC interface sends the data packet out of the firewall.

12.3 Diagnostic Center

12.3.1 Network Connectivity Diagnosis

Application Scenario

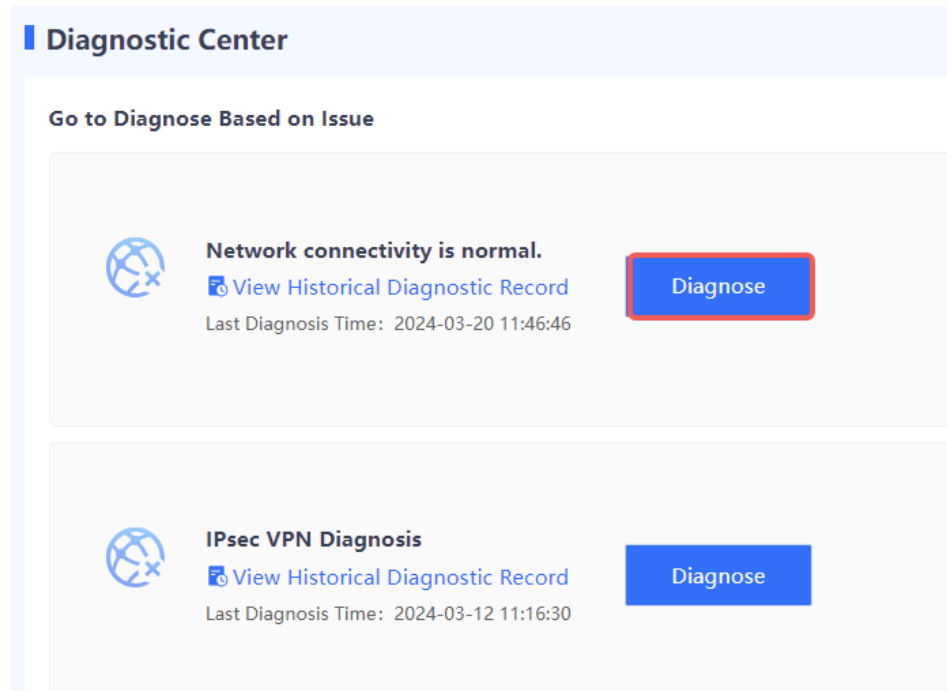
The diagnostic center integrates various functions including traffic receiving detection, basic configuration (security policy and NAT policy) detection, packet tracing, and traffic forwarding detection and provides a standard troubleshooting roadmap to help you locate network faults with one click. It also offers explicit and practicable recommendations to achieve efficient and easy network troubleshooting.

Note

The diagnostic center function is supported from NTOS1.0R3. If your version is lower than NTOS1.0R3, upgrade it to NTOS1.0R3 or higher.

Procedure

- (1) Choose **System > Fault Diagnosis > Diagnostic Center**.
- (2) Click **Diagnose**.



- (3) Enter the source/destination IP address, source/destination port, source/destination MAC address, inbound interface, and protocol, and click **Diagnose**. The firewall checks the network connectivity between the specified source and destination IP addresses.

Network Connectivity Diagnosis

Diagnostic Parameter Settings

The diagnostic parameters will be used throughout the diagnostic process, covering basic configuration detection, packet tracing, and traffic receiving and forwarding detection.
Note: You are advised to minimize the range to achieve a better diagnostic result. If the diagnostic range is too large, only 1000 flows will be obtained. Packet tracing only displays the packets forwarded by the CPU, but not those forwarded through hardware fast forwarding.

* Src. Address Src. Port

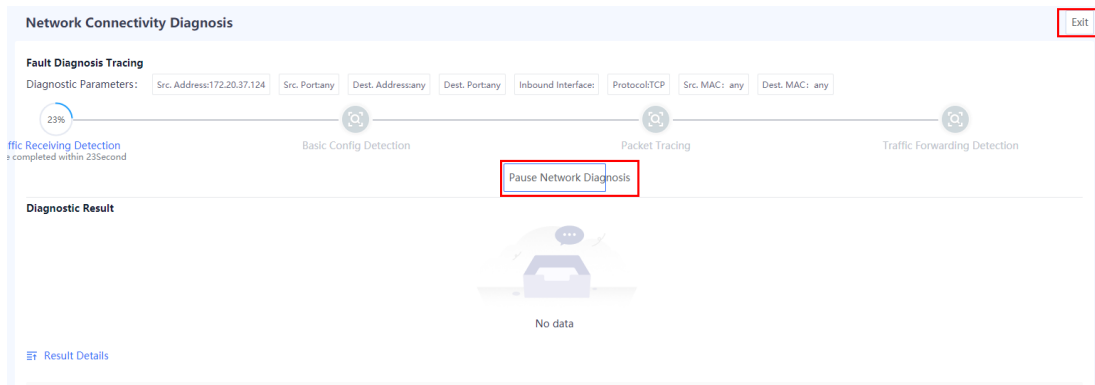
Dest. Address Dest. Port

Inbound Interface * Protocol

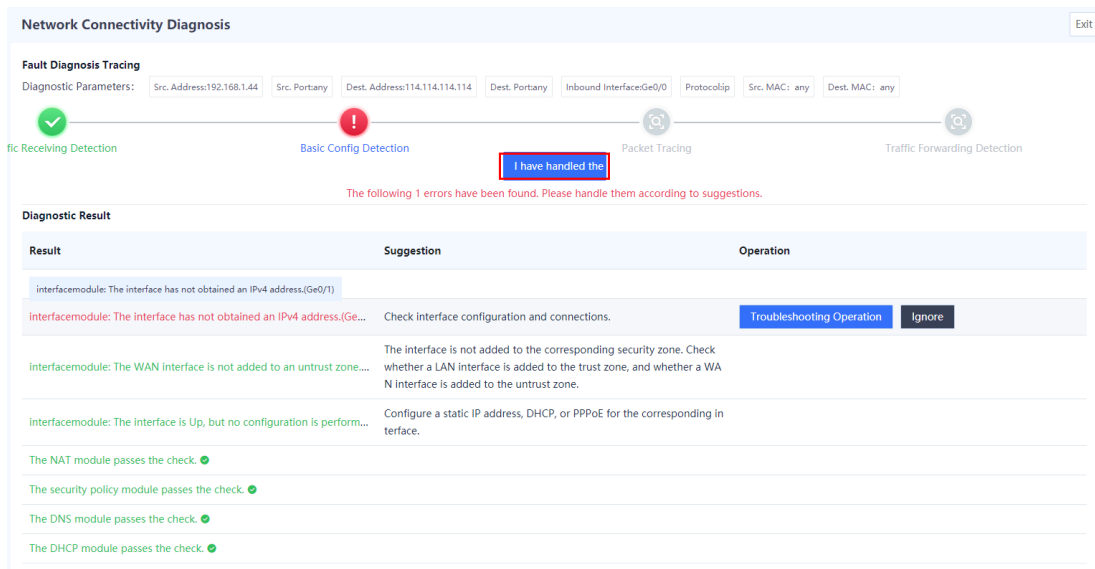
Src. MAC Dest. MAC

Diagnose

- (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) In the **Tip** dialog box, select **Network connectivity is normal**. and click **Confirm**. The firewall continues to check the next item.

i Note

If the fault is not rectified, select **Do not ignore unhandled issues and continue the detection**. The firewall performs the detection again.

Tip**Check the network status.**

On a client, ping the intranet interface IP address, extranet interface IP address, and destination IP address of the firewall in sequence to determine whether network connectivity is normal.

- Network connectivity is normal. End the detection.
- Do not ignore unhandled issues and continue the detection.
- Ignore unhandled issues and go to the next phase.

Confirm

Cancel


(7) Repeat steps (5) and (6) until all the items are checked.


Follow-up Procedure

Click **View Historical Diagnostic Record** to view and download historical diagnostic records.

Diagnostic Center

Go to Diagnose Based on Issue

**Network connectivity is normal.**
[View Historical Diagnostic Record](#)
Last Diagnosis Time: 2024-03-20 11:46:46 **Diagnose**

**IPsec VPN Diagnosis**
[View Historical Diagnostic Record](#)
Last Diagnosis Time: 2024-03-12 11:16:30 **Diagnose**

12.3.2 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 System > Fault Diagnosis > Diagnostic Center.
- (2) Click Diagnose next to IPsec VPN Diagnosis.


Diagnostic Center

Go to Diagnose Based on Issue



Network connectivity is normal.
[View Historical Diagnostic Record](#)
Last Diagnosis Time: 2024-03-20 11:46:46

Diagnose



IPsec VPN Diagnosis
[View Historical Diagnostic Record](#)
Last Diagnosis Time: 2024-03-12 11:16:30

Diagnose

(3) Set diagnostic parameters and click **Diagnose**. The firewall checks tunnel connectivity.

IPsec VPN Diagnosis

Diagnostic Parameter Settings

Diagnosis Type Tunnel Negotiation Error Tunnel Forwarding Error

* Tunnel

Remote IP

* ⓘ Diagnosis Second
Duration

Diagnose

IPsec VPN Diagnosis

Diagnostic Parameter Settings

Diagnosis Type Tunnel Negotiation Error Tunnel Forwarding Error

* Tunnel

Remote IP

* ⓘ Src. Address

* ⓘ Dest. Address

Protocol

ⓘ Src. Port

ⓘ Dest. Port

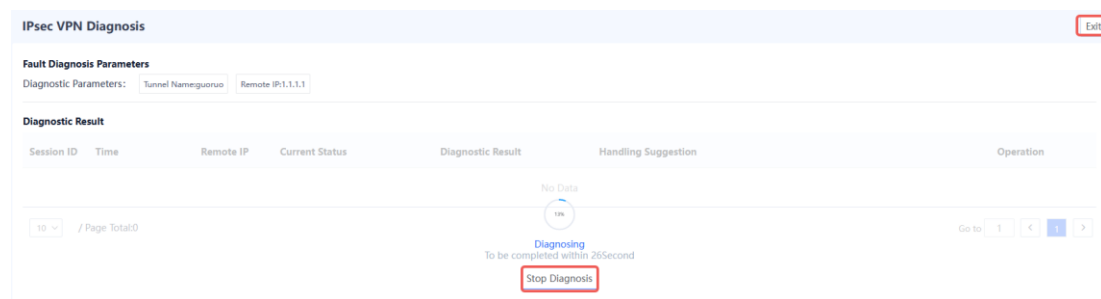
* ⓘ Diagnosis Second
Duration

Diagnose

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.
Remote IP	Remote IP address of the IPsec VPN tunnel.	If the tunnel is in point-to-point mode, the value is automatically set after you select the tunnel. If the tunnel is in point-to-multipoint mode, you need to enter the remote IP address. The diagnosis supports only IPv4 addresses.
Diagnosis Duration	Tunnel diagnosis duration. The diagnosis automatically stops when the duration expires.	The default value is 30 seconds. [Example] 30
Tunnel Forwarding Error		
Tunnel	Name of the tunnel to be diagnosed.	Select an existing IPsec VPN tunnel from the drop-down list.

Item	Description	Remarks
Remote IP	Remote IP address of the IPsec VPN tunnel.	If the tunnel is in point-to-point mode, the value is automatically set after you select the tunnel. If the tunnel is in point-to-multipoint mode, you need to enter the remote IP address. The diagnosis supports only IPv4 addresses.
Src. Address	Source address of interesting traffic.	Only one IP address is supported. [Example] 192.168.1.1
Dest. Address	Destination address of interesting traffic.	Only one IP address is supported. [Example] 192.168.1.2
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**.

IPsec VPN Diagnosis Exit

Fault Diagnosis Parameters

Diagnostic Parameters:

Diagnostic Result ● Diagnosis is stopped. Total Tunnels: 1 Established Tunnels: 0 Rediagnose 2

Session ID	Time	Remote IP	Current Status	Diagnostic Result	Handling Suggestion	Operation
1	2024-04-12 17:34:38	1.1.1.1	Waiting for the response	No response received from peer	Possible reasons: 1.Network failure 2.Inconsistent negotiat...	Configure Details

/ Page Total:1 Go to < 1 >

(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.

Diagnostic Center

Go to Diagnose Based on Issue

Network connectivity is normal.
🔗 View Historical Diagnostic Record Diagnose
Last Diagnosis Time: 2024-03-20 11:46:46

IPsec VPN Diagnosis
🔗 View Historical Diagnostic Record Diagnose
Last Diagnosis Time: 2024-03-12 11:16:30

12.3.3 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 System > Fault Diagnosis > Diagnostic Center.
- (2) Click Diagnose next to SSL VPN Diagnosis.

Diagnostic Center

Go to Diagnose Based on Issue

-  **Network Connectivity Diagnosis**
No diagnostic records Diagnose
-  **IPsec VPN Diagnosis**
No diagnostic records Diagnose
-  **SSL VPN Diagnosis**
No diagnostic records Diagnose

(3) Set diagnostic parameters and click **Diagnose**. The firewall checks tunnel connectivity.


SSL VPN Diagnosis

Diagnostic Parameter Settings

* Gateway

Diagnosis Type Login Failure Resource Access Failure

* Username

*  Gateway
Address

Diagnose

SSL VPN Diagnosis

Diagnostic Parameter Settings

* Gateway

Diagnosis Type Login Failure Resource Access Failure

* Username

* ⓘ Resource
Address

Protocol

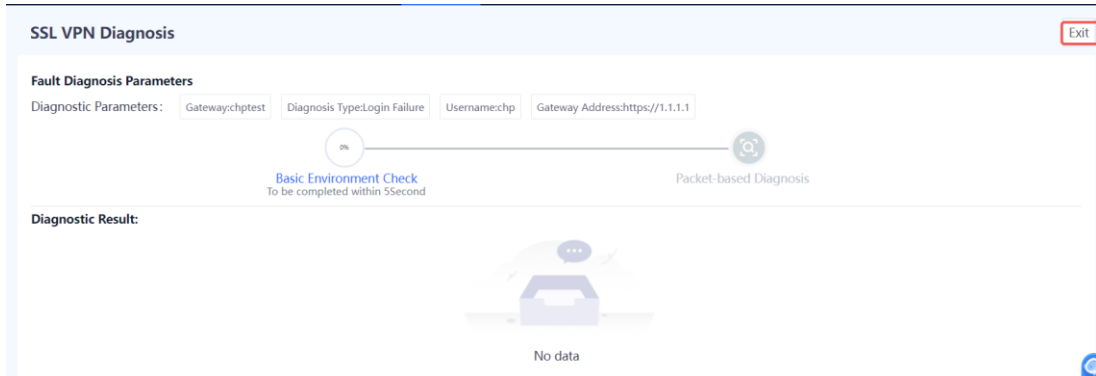
ⓘ Port

Diagnose

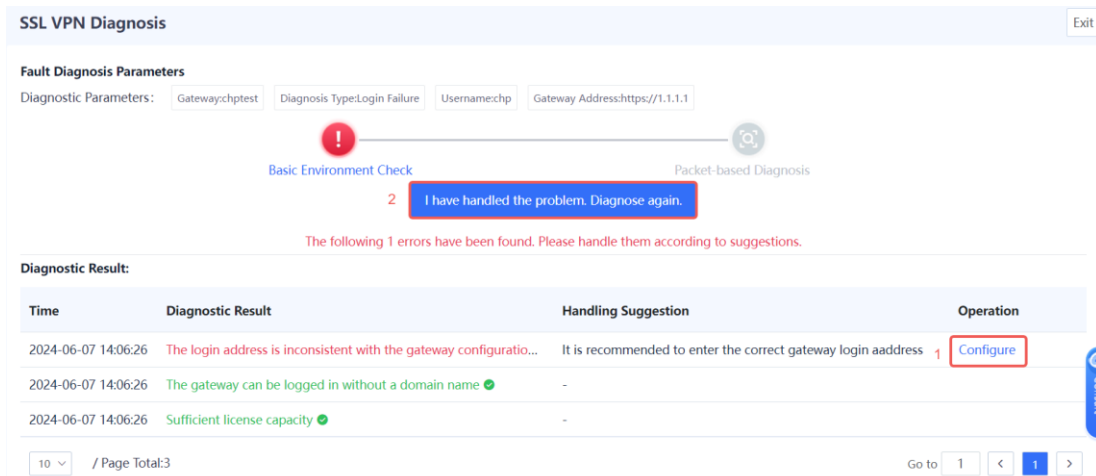
Item	Description	Remarks
Login Failure		
Gateway	Name of the gateway to be diagnosed.	Select an SSL VPN gateway from the drop-down list.
Username	Name of the user who fails to log in to the SSL VPN gateway.	Enter an existing user or select a user from the drop-down list.
Gateway Address	Address of the 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
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.



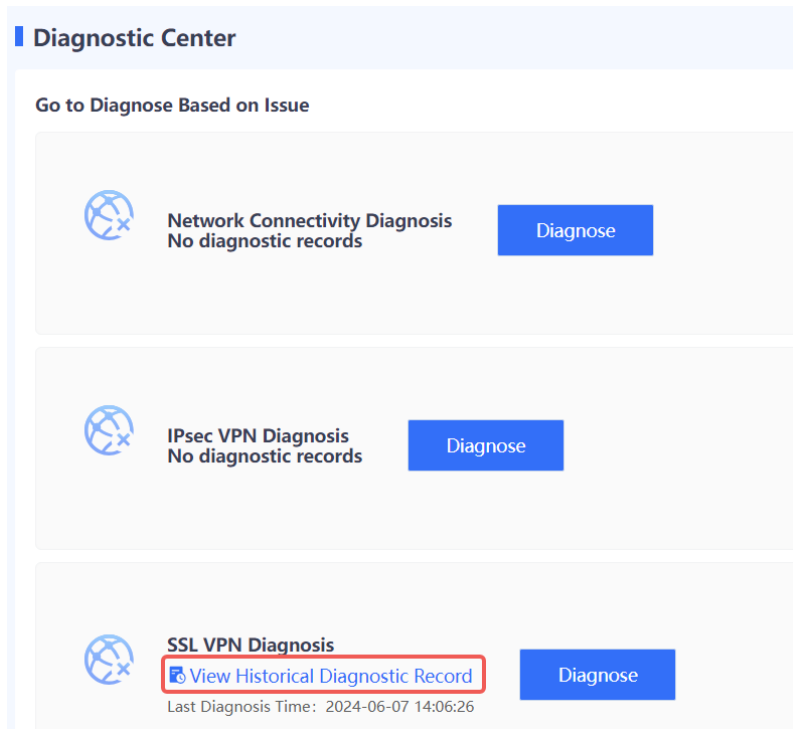
(5) After the diagnosis is complete, the diagnosis result, diagnosis details, and handling suggestions are displayed in the lower part of the page. Click **Configure** in the **Operation** column to rectify the fault based on the diagnosis details and handling suggestions, and then click **I have handled 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.



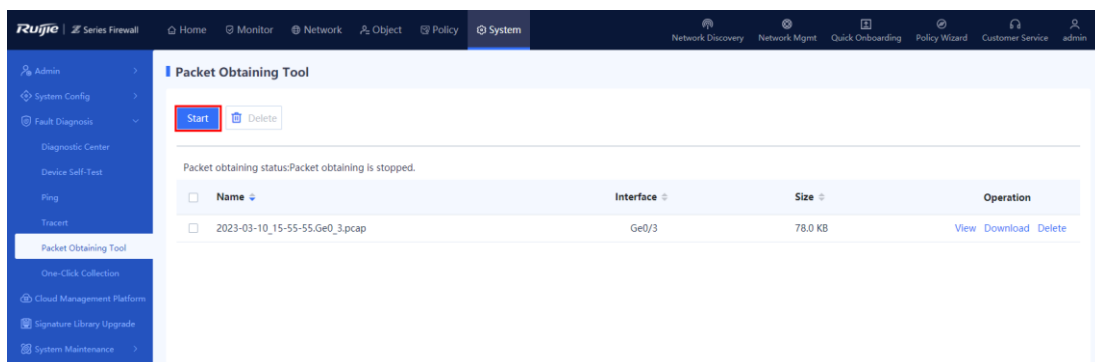
12.4 Packet Obtaining

Application Scenario

The web management page provides the packet obtaining function. If a software fault occurs, administrators can use the packet obtaining tool to assist troubleshooting of R&D personnel. The packet obtaining tool is used to obtain data packets on the network and save them to a file. Development personnel can analyze the obtained data packets to quickly locate software faults.

Procedure

- (1) Choose System > Fault Diagnosis > Packet Obtaining Tool.
- (2) Click **Start**.



Packet Obtaining Option ⊗

i You are advised to enter the complete source MAC address, destination MAC address, source IP address (port number), destination IP address (port number) to improve packet obtaining efficiency. An unspecified item is set to any.

* **Interface**

Packet

Obtaining Rule

Layer 2 Protocol any IP ARP

iSrc. MAC

iDest. MAC

Start

Cancel

(3) Set the packet obtaining option.

- Interface: Select a physical interface or subinterface from which packets are obtained.
- Layer 2 Protocol
 - When you set this parameter to **any**, you can enter the source or destination MAC address. If you enter only one MAC address (source or destination MAC address), the tool obtains data packets of this MAC address. If you enter both the source MAC address and destination MAC address, the tool obtains all the packets exchanged between the two MAC addresses.
 - If you set this parameter to **ARP**, the tool obtains ARP packets only. You can enter the source or destination MAC address. If you enter only one MAC address (source or destination MAC address), the tool obtains data packets of this MAC address. If you enter both the source MAC address and destination MAC address, the tool obtains all ARP packets exchanged between the two MAC addresses.
 - If you set this parameter to **IP**, you can further select **any**, **TCP**, or **UDP**.
- If you specify only the source options (source MAC address, source IP address, and source port) or the destination options (destination MAC address, destination IP address, and destination port), the tool obtains packets with the specified source or destination options. If you specify both the source options and the destination options, the tool obtains all the packets meeting these options.

Configuration Example 1

Packet Obtaining Option



i You are advised to enter the complete source MAC address, destination MAC address, source IP address (port number), destination IP address (port number) to improve packet obtaining efficiency. An unspecified item is set to any.

* **Interface**

Packet

Obtaining Rule

Layer 2 Protocol any IP ARP

Layer 3 Protocol any TCP UDP

iSrc. IP (Port)

iDest. IP (Port)

iSrc. MAC

iDest. MAC

Start

Cancel

The tool obtains all the UDP packets passing through Ge0/0 with the source IP address 192.168.1.1 or destination IP address 192.168.1.1.

Configuration Example 2

Packet Obtaining Option



i You are advised to enter the complete source MAC address, destination MAC address, source IP address (port number), destination IP address (port number) to improve packet obtaining efficiency. An unspecified item is set to any.

* **Interface**

Packet Obtaining Rule

Layer 2 Protocol any IP ARP

Layer 3 Protocol any TCP UDP

iSrc. IP (Port)

iDest. IP (Port)

iSrc. MAC

iDest. MAC

Start

Cancel

The tool obtains all the packets passing through Ge0/0 with the source IP address 192.168.1.1 and destination IP address 192.168.23.100:80 or with the source IP address 192.168.23.100:80 and destination IP address 192.168.1.1.

Follow-up Procedure

After packet obtaining is complete, click **View** to view and analyze the packet obtaining file in online mode and download the packet obtaining result to the PC. The file can be analyzed using a packet obtaining tool such as Wireshark.

12.5 Device Self-Test

12.5.1 Device Self-Test

Application Scenario

The device self-test function can detect the device version, CPU usage, memory usage, and whether risky configuration exists.

i Note

The device self-test function is supported from NTOS1.0R3. If your version is lower than NTOS1.0R3, upgrade it to NTOS1.0R3 or higher.

Procedure

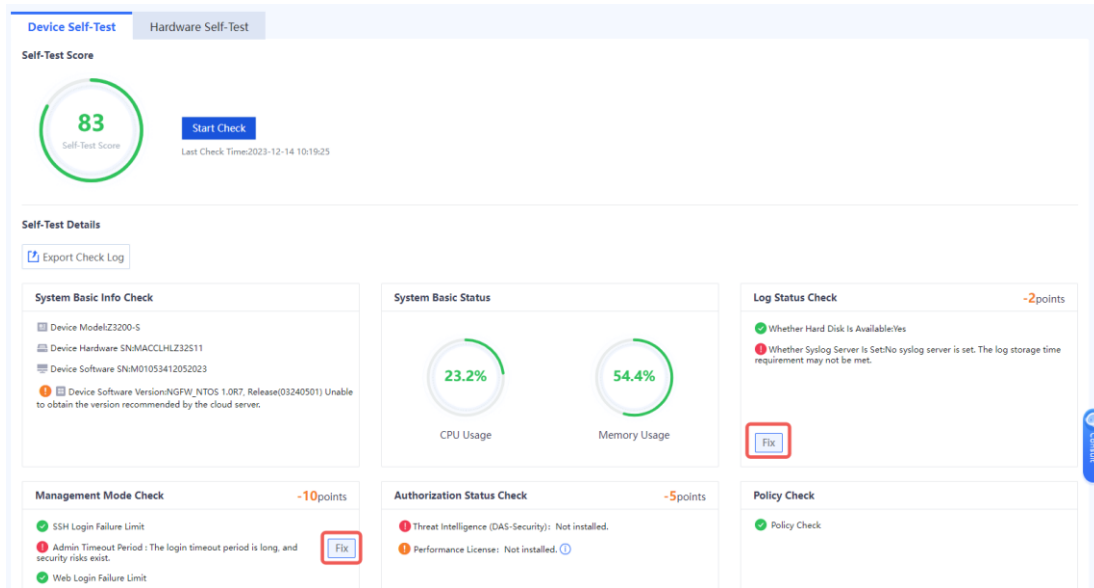
- (1) Choose **System > Fault Diagnosis > Device Self-Test > Device Self-Test**. The Device Self-Test page is displayed.
- (2) Click **Start Check** to start device self-test.

The screenshot displays the 'Device Self-Test' interface. At the top, there are tabs for 'Device Self-Test' (highlighted) and 'Hardware Self-Test'. Below the tabs, a 'Self-Test Score' section shows a score of 93 and a 'Start Check' button. The 'Self-Test Details' section includes an 'Export Check Log' button and several check panels: 'System Basic Info Check' (listing device model, hardware, and software), 'System Basic Status' (showing CPU Usage at 44.5% and Memory Usage at 33.3%), 'Log Status Check' (with a -2 points penalty and a 'Fix' button), 'Management Mode Check' (with a -5 points penalty and a 'Fix' button), 'Authorization Status Check' (listing license statuses), and 'Policy Check' (showing a successful policy check).

- (3) After device self-test is complete, in the dialog box that is displayed, click **OK**.

The screenshot shows a 'Tip' dialog box with a close button (X) in the top right corner. The main text reads 'Check succeeded.' and there is a blue 'OK' button at the bottom center.

- (4) For an abnormal item, click **Fix** to switch to the corresponding configuration page.



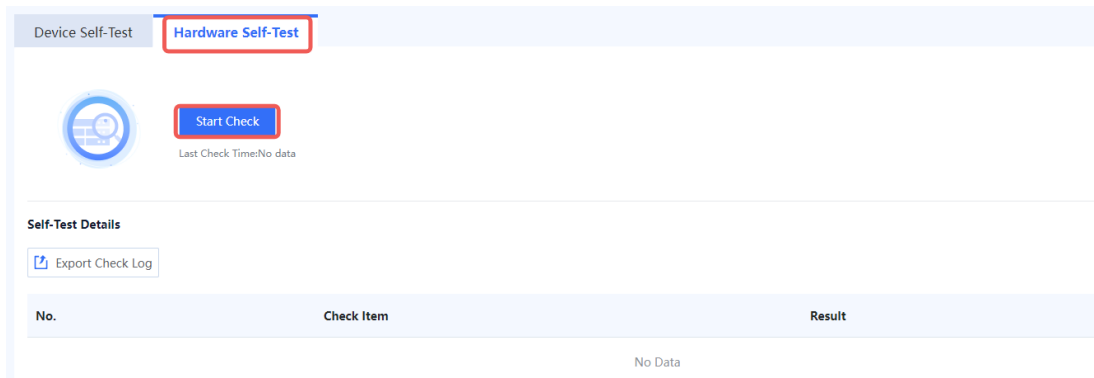
12.5.2 Hardware Self-Test

Application Scenario

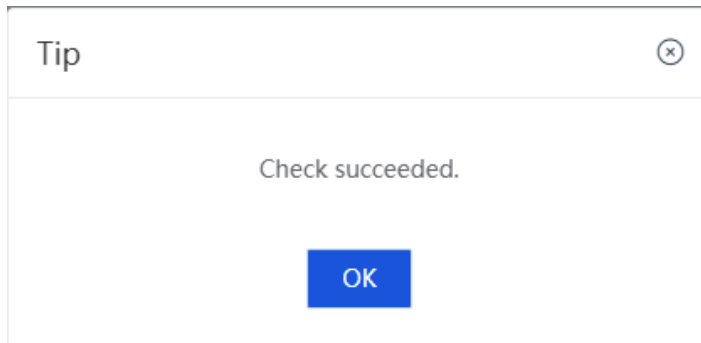
The hardware self-test function can detect whether the hardware status of the device, including the temperature, hard disk, power supply, and voltage, is normal.

Procedure

- (1) Choose **System > 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.

Device Self-Test

Hardware Self-Test



Start Check

Last Check Time:2023-12-14 10:22:41

Self-Test Details

[Export Check Log](#)

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

12.6 One-Click Fault Information Collection

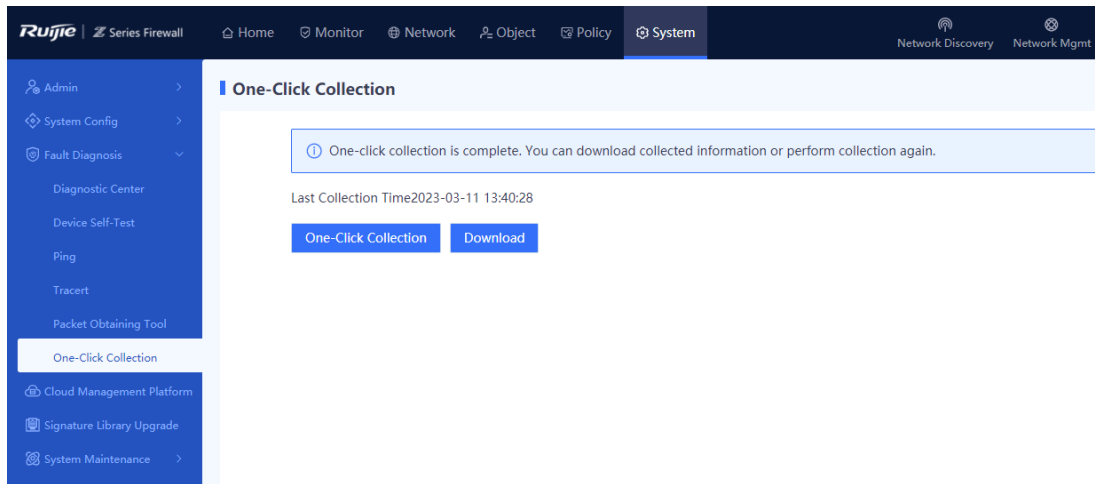
Application Scenario

When a device fault occurs, you can collect the fault information of devices with one click to facilitate analysis by troubleshooting personnel.

Procedure

(1) Access the One-Click Collection page.

Choose **System > Fault Diagnosis > One-Click Collection**.



- (2) Click **One-Click Collection** and wait for 3 to 5 minutes until information collection is complete.
- (3) Click **Download** to download the collected fault information to the PC for fault analysis.

12.7 Data Flow Diagnosis

12.7.1 Packet Statistics Collection

1. cmd debug-support fp exec stats

This command is used to collect the number of sent and received packets of an interface and packet processing information in the forwarding path. The fields with annotation need your attention.

```
firewall> cmd debug-support fp exec stats
==== interface stats:
lo-vr0 port:65534
_eth0-vr0 port:65534
_eth1-vr0 port:65534
_eth2-vr0 port:65534
Ge0_0-vr0 port:65534
  ifs_ipackets:124720    --->Number of packets received by the interface
  ifs_ibytes:14454713  --->Number of bytes in the packet received by the interface
  ifs_opackets:23430   --->Number of packets sent by the interface
  ifs_obytes:29152694  --->Number of bytes in the packet sent by the interface
TenGe0_0-vr0 port:65534
  ifs_opackets:739
  ifs_obytes:33994
....
br0-vr0 port:65534
  ifs_ipackets:306
  ifs_ibytes:18360
==== global stats:
  fp_dropped:11053053
  fp_dropped_excp:14155
  fp_dropped_ether:326
```

```

fp_dropped_bridge:2
fp_dropped_npf:11038563 --->Total number of lost service packets in the flow platform. The data will be
used with statistical analysis of the flow platform later.
fp_dropped_system:6
==== exception stats:
LocalFPTunExceptions:253437
ExceptionByModule:
fp_exception_ether:199272
fp_exception_bridge:734
fp_exception_ip:37548
fp_exception_ipv6:15883
LocalExceptionClass:
FPTUN_EXC_SP_FUNC:206764
FPTUN_EXC_ETHER_DST:28299
FPTUN_EXC_IP_DST:15196
FPTUN_EXC_ICMP_NEEDED:687
FPTUN_EXC_NDISC_NEEDED:2491
LocalExceptionType:
FPTUN_IPV4_OUTPUT_EXCEPT:2491
FPTUN_ETH_INPUT_EXCEPT:250946
FPTUN_ETH_SP_OUTPUT_REQ:2444
ExcpDroppedFpToLinuxUserExcSendtoFailure:102
==== IPv4 stats:
IpForwDatagrams:1648056613
IpInReceives:1648056613
==== arp stats:
arp_unhandled:168695
==== IPv6 stats:
==== TCP stats:
total packets received:6758
# of packets not managed by MCORE_SOCKET:6758
==== UDP stats:
==== vlan stats:
==== dsa stats:
DsaDroppedInOperative:1
==== bridge stats:
L2ForwFrames:251334551
BridgeDroppedNoOutputPort:2
==== ebttables stats:
==== pppoe stats:

```

2. cmd debug-support npf exec stats

This command is used to display statistics of various services in the flow platform.

```

firewall> cmd debug-support npf exec stats
Policy action:          --->Statistical summary of a security policy
1008 Policy permit     ---> Number of flows permitted by the security policy

```

```
0 Policy deny          ---> Number of flows blocked by the security policy
Packets dropped:      --->Total number of lost service packets in the flow platform
0 RPF check drop
0 Connection create failed drop
0 Connection install failed drop
0 Connection threshold drop
0 Connection invalid state drop
0 Invalid connection drop
0 Do SNAT drop
0 Do DNAT drop
0 NAT transition drop
0 Do ALG drop
624879 Route error drop
0 thd-event mlist full drop
0 thd-event error drop
0 Prepend failed drop
0 Header too short drop
0 Fragment failure drop
0 Invalid IP drop
Wrong packets dropped:
0 Interface error
0 Ip header error
0 Frament packet
0 IP header hl error
0 TCP header error
0 UDP header error
0 ICMP header error
0 ICMP packet error
0 ICMP6 header error
0 ICMP6 packet error
0 checksum error
0 Ipv6 header error
0 Ipv6 extension header error
Connection entries:
625887 Connection allocations
0 Connection reverse
625886 Connection release
625884 Connection destructions
0 Connection refresh conflict
0 Connection allocation failures
0 Connection ID limit
0 Connection ID invalid
0 Connection ID no entry
NAT entries:
0 NAT entry allocations
0 NAT entry destructions
```

```

    0 NAT entry allocation failures
    0 NAT port allocation failures
Invalid packet state cases:
    0 cases in total
    0 TCP case invalid first packet
    0 TCP case RST
    0 TCP case invalid transition
    0 TCP case REOPEN
    0 TCP case Out of window range
    0 TCP case Invalid seq
    0 TCP case Invalid ack
TCP Reass:
    0 TCP Reass present
    0 TCP Reass present cover
    0 TCP Reass present overlap
    0 TCP Reass present cut
    0 TCP Reass cache
    0 TCP Reass cache head
    0 TCP Reass cache tail
    0 TCP Reass cache head overlap
    0 TCP Reass cache tail overlap
    0 TCP Reass cache new drop
    0 TCP Reass cache old drop
    0 TCP Reass cache overflow
    0 TCP Reass cache timeout
    0 TCP Reass cache release
    0 TCP Reass error
Packets reentrant:
    0 reentrant
    0 reentrant drop
Packet race cases:
    0 NAT association race
    0 duplicate state race

```

12.7.2 Flow Status

The **show nfp flows stats** command is used to display flow table statistics.

The **show nfp flows** command is used to display all the flow entries in the system.

The **show nfp flows filter** { **app** *appid* | **addr** *address* | **dport** *port* | **dstif** *interface* | **policy** *policy-id* | **proto** *protocol-id* | **saddr** *address* | **session-id** *id* | **sport** *port* | **srcif** *interface* } command is used to display flow tables by filtering condition.

This command is used when flow tables are created based on the specified control flow (for example, data flows in the ALG scenario).

```

firewall> show nfp flows
38:
    proto:17  tsdiff:7  timeout:120  State:established

```

```

FORW 20.0.0.2:39304 -> 114.114.114.114:53
BACK 114.114.114.114:53 -> 20.0.0.2:39304
Srcif:lo  Dstif:Ge0/0  alg:none  flags:0x2000000
vrf:0  Appid:0-0-0-0  Policy:local  action:permit
Send packets:2  bytes:136
Recv packets:2  bytes:622
firewall> show nfp flows filter dport 9209
1191:
  proto:6  tsdiff:1  timeout:1800  State:established
FORW 172.16.33.5:9404 -> 172.18.142.16:9209
BACK 172.18.142.16:9209 -> 20.0.0.2:52438
snat id: 0
Srcif:Ge0/1  Dstif:Ge0/0  alg:none  flags:0x804a000
vrf:0  Appid:0-0-0-0  Policy:8192  action:permit
Send packets:16572  bytes:2435798
Recv packets:8331  bytes:2114493
firewall> show nfp flows stats
The capacity of the flow: 1000000
Allocated flows num: 63
Active flows num: 63

```

Note: The following part describes fields in the flow table.

```

1191:
  proto:6  tsdiff:1  timeout:1800  State:established
FORW 172.16.33.5:9404 -> 172.18.142.16:9209
BACK 172.18.142.16:9209 -> 20.0.0.2:52438
snat id: 0
Srcif:Ge0/1  Dstif:Ge0/0  alg:none  flags:0x804a000
vrf:0  Appid:0-0-0-0  Policy:8192  action:permit  --->Security policy matching result. The value of
local indicates access to the local host or access actively initiated by the local host, which is not restricted. The
value of default indicates that the default block policy is matched. The value of bypass indicates that a whitelist
is matched. If a number is displayed, the number indicates the ID of a specific policy.
  Action:security-defend(1) Reason:flood detect(11) -->Module and cause. The information is displayed
only when packet loss in the flow is not caused by a security policy.
Send packets:16572  bytes:2435798
Recv packets:8331  bytes:2114493
  1191: Flow id/session id
  Proto: Protocol number (1:icmp 6:tcp 17:udp)
  tsdiff: Session idle time (remaining time before session aging)
  timeout: Session aging time
  State: Session status
  FORW: Quadruple information of the forward session flow
  BACK: Quadruple information of the reverse session flow
  snat id: ID of the NAT policy hit by the flow
  Srcif: Source interface of the forward flow
  Dstif: Destination interface of the forward flow
  Alg: ALG type of the flow

```

```

Flags: Flow table status
vrf: vrf id
Appid: Application identification ID
Policy: ID of the security policy hit by the flow
Action: Policy action (permit/deny)
Action: Module with packet loss
security-defend:DDOS
Reason for packet loss (Reason):
XXX
Send packets: Number of sent packets
Recv packets: Number of packets received

```

12.7.3 Packet Tracing

Use command (1) to configure filtering conditions and command (2) to configure the module (type-on field in command 2) to be enabled. In most cases, you are advised to use the recommended command.

Commands:

- (1) **cmd trace-filter enabled true [proto protocol-id] [saddr address] [sport port] [daddr address] [dport port] [ifid1 interface-id] [ifid2 interface-id]**

```

firewall>cmd trace level DEBUG max-number 0 timeout 0 type-off "all" type-on "NFP BASIC"
firewall>cmd trace-filter enabled true proto 1 saddr 10.1.1.10
firewall> show log max-lines 2000
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp_ether_input(ifp=Ge0_6 port=65534)
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp_ether_input_one(ifp=Ge0_6 port=65534)
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp_ip_input_bulk_check: mbuf=0x18ad669c0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: npf_packet_handler: mbuf=0x18ad669c0,
npf_mode=0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: npf: mbuf 0x18ad669c0 find connection 662,
dir=back
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]:          vrfid 0 flags 0x804a000 alg none policy
8192 action permit
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]:          forw proto 1 5.0.64.53:1->
172.18.25.214:1
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]:          back proto 1 172.18.25.214:458->
192.168.101.2:458
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: security_defend returns 0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: conn_reroute returns 0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: conn_update returns 0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: policy_rematch returns 0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: service_chain returns 0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: alg returns 0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: do_nat returns 0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: security_defend returns 0
[2022/02/17 11:24:39]ms 0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp_fast_ip_input_pre_routing: mbuf=0x18ad669c0

```

```

[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp_fast_ip_output_post_routing:
mbuf=0x18ad669c0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp_ether_output: mbuf=0x18ad669c0, ifp=Ge0_1
port=65534
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp_if_output: mbuf=0x18ad669c0, ifp=eth0, port=0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall uwsgi[2445]: <190>1 2022-02-17T03:23:51.525503Z firewall
web 2445 - [operationLog@4881 ip="192.168.1.100"
operator="<E7><AB><AF><E5><8F><8F><A3><E6><98><A0><E5><B0><84>"
operate="<E5><90><AF><E7><94><A8>/<E7><A6><81><E7><94><A8><E7><AB><AF><E5><8F><A3><E
6><98><A0><E5><B0><84>" description="<E7><<AB><AF><E5><8F><A3><E6><98><A0><E5><B0><84>
<E5><90><AF><E7><94><A8>/<E7><A6><81><E7><94><A8><E7><AB><AF><E5><8F><A3><E6><98>
<A0><E5><B0><84><E6><88><90><E5><8A><9F>" timestamp="1645068231" admin="admin"]
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]:
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: fp_ether_input(ifp=eth0 port=0)
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: sbuf data at [0x18e60ab82], len=78
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: 00000000 30 0D 9E 41 D8 D1 22 22 22 22 22 24
C0 10 00 00
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: 00000010 08 00 45 00 00 3C 3E 34 00 00 40 01
31 70 05 00
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: 00000020 40 35 AC 12 19 D6 08 00 19 14 00 01
34 47 61 62
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: 00000030 63 64 65 66 67 68 69 6A 6B 6C 6D 6E
6F 70 71 72
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: 00000040 73 74 75 76 77 61 62 63 64 65 66 67 68
69
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: fp_ether_input(ifp=Ge0_1 port=65534)
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: fp_ether_input_one(ifp=Ge0_1 port=65534)
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: fp_ip_input_bulk_check: mbuf=0x18e60a900
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: npf_packet_handler: mbuf=0x18e60a900,
npf_mode=0
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: npf_packet_handler, 1029: conn 662 is expired,
drop the mbuf 0x18e60a900!packet m=0x18e60a900 dropped at npf_packet_handler():1030
[2022/02/17 11:24:39]Feb 17 11:23:53 firewall fp-rte[1339]: flow-log 1230 send: src 83902517 sport 16374 dst
1964509311 dport 80 natsrc 3232261378 nat sport 9278 natdst 1964509311 natdport 80 proto 6 direct 1
sendbytes 415 rcvbytes 410 sendpkts 8 rcvpkts 2 srcif Ge0_1 dstif Ge0_6 appid 0-0-0-0 policy allow_all
action 0 module reason time 1645068232
[2022/02/17 11:24:39]Feb 17 11:23:53 firewall fp-rte[1339]: flow-log 662 send: src 83902517 sport 1 dst
2886867414 dport 1 natsrc 3232261378 nat sport 458 natdst 2886867414 natdport 458 proto 1 direct 1
sendbytes 54068232
[2022/02/17 11:24:39]Feb 17 11:23:53 firewall fp-rte[1339]: flow-log 710 send: src 83902517 sport 12345 dst
660748687 dport 8000 natsrc 3232261378 nat sport 8959 natdst 660748687 natdport 8000 proto 17 direct 1
sendbytes 205 rcvbytes 0 sendpkts 1 rcvpkts 0 srcif Ge0_1 dstif Ge0_6 appid 0-0-0-0 policy allow_all action
0 module reason time 1645068232
[2022/02/17 11:24:39]Feb 17 11:23:53 firewall fp-rte[1339]: flow-log 138 send: src 83902517 sport 61509 dst
2567170222 dport 8000 natsrc 3232241498 nat sport 8326 natdst 2567170222 natdport 8000 proto 17 direct 1

```

```
sendbytes 1170 rcvbytes 70 sendpkts 6 rcvpkts 1 srcif Ge0_1 dstif Ge0_7 appid 0-0-0-0 policy allow_all
action 0 module reason time 1645068233
[2022/02/17 11:24:39]Feb 17 11:23:53 firewall fp-rte[1339]: Connection 662 is destroyed
```

(2) **cmd trace** [**level** EMERG | ALERT | CRIT | ERR | WARNING | NOTICE | INFO | DEBUG] [**max-number line**] [**timeout seconds**] [**type-off** "all"] [**type-on** "NFP BASIC "]

This command is used to set the output level of debugging logs, the maximum number of rows in a log, maximum record timeout period (in seconds), and module enabling/disabling log.

- o **max-number**: Specifies the maximum number of rows in a printed log.
- o **timeout**: Specifies the time when the log is printed.

 Note

The levels in the command format are ranked in descending order by the severity. The default level is ERR. After a level is set, all the logs higher than or equal to this level will be printed.

The following command is used to display the forwarding packet loss information.

```
cmd trace level DEBUG max-number 0 timeout 180 type-off "all" type-on " NFP BASIC "
```

max-number 0 timeout 180 indicates that log recording is automatically disabled in 3 minutes. If both **max-number** and **timeout** are set to 0, log recording must be disabled manually after information collection.

Use the following command to disable log recording (restoring to the default value).

```
cmd trace level ERR max-number 5000 timeout 60 type-off "all"
```


13 Running Status Check After Product Implementation

13.1 Checking the Software Version

Standards

- The software version must be the latest. Confirm on the Secure Cloud Platform or choose **System > System Maintenance > System Upgrade > Online Upgrade** to check whether a recommended version is available. If no, the system displays that the current version is already the latest version.
- Users have purchased the online upgrade service for the app identification signature library and IPS signature library and the current version is the latest.

Precautions

- The device needs to be restarted after online device upgrade, which may cause customer service interruption.
- Users can upgrade to the latest signature libraries only after they purchase the upgrade service for the Ruijie IPS signature library and virus library.
- DNS and the time zone must be correctly configured to allow the app identification signature library and IPS signature library to access the Internet.

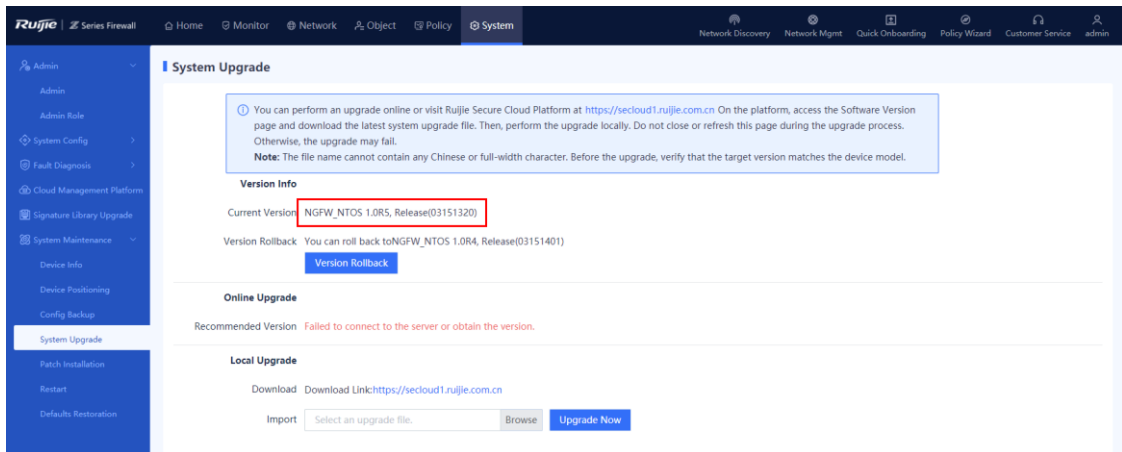
Method

(1) Check whether the software version is recommended using one of the following methods:

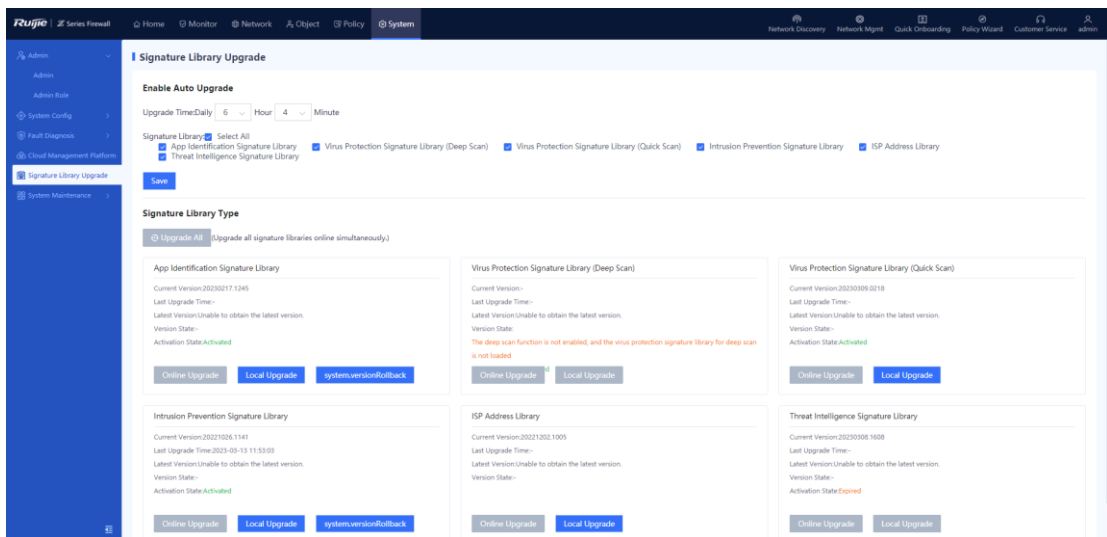
- Method 1: Log in to the Secure Cloud Platform (<https://secloud1.ruijie.com.cn>), click **Version Upgrade**, and select an applicable version to download it.

No.	File Name	Version Number	Release Date	File Size (MB)	MD5	Applicable Model	Hardware Version	Applicable Software Version	Version Description	Operation
1	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2023-01-05	163.74	4C8772E6DCA4...	Z8620.Z8600	1.00	Universal	hgtest: z8600-20...	Download View Version
2	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2023-01-04	163.69	5FA916C58951B8...	Z8620.Z8600	1.00	Universal	hgtest: z8600-20...	Download View Version
3	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2022-12-29	167.41	a7277983ee08653...	Z8620.Z8600	1.00	Universal	lytest1	Download View Version
4	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2022-12-28	127.76	07bee08c49f3c121...	Z5100	1.00	Universal	lytest1	Download View Version

- Method 2: Log in to the web page of the firewall and choose **Home > View Device Detail > Version Info or System > System Maintenance > System Upgrade**.



- (2) Check whether signature libraries (app identification signature library, IPS signature library, virus protection signature library, ISP address library, threat intelligence signature library) are of the latest version.



13.2 Checking the Management Mode

Standards

- Preferentially use secure management modes HTTPS and SSH and test whether the firewall can be remotely managed over the customer LAN or Internet.
- Confirm that the administrator login timeout period is not over 30 minutes. **(A too long timeout period causes security risks.)**
- It is recommended that the allowed consecutive login failures be not higher than 6 and the lockout duration be not less than 300s. (A large login failure count will lead to brute-force attack risks. The re-login interval cannot be set to a too small value.)
- Confirm that the firewall restricts management hosts.

Precautions

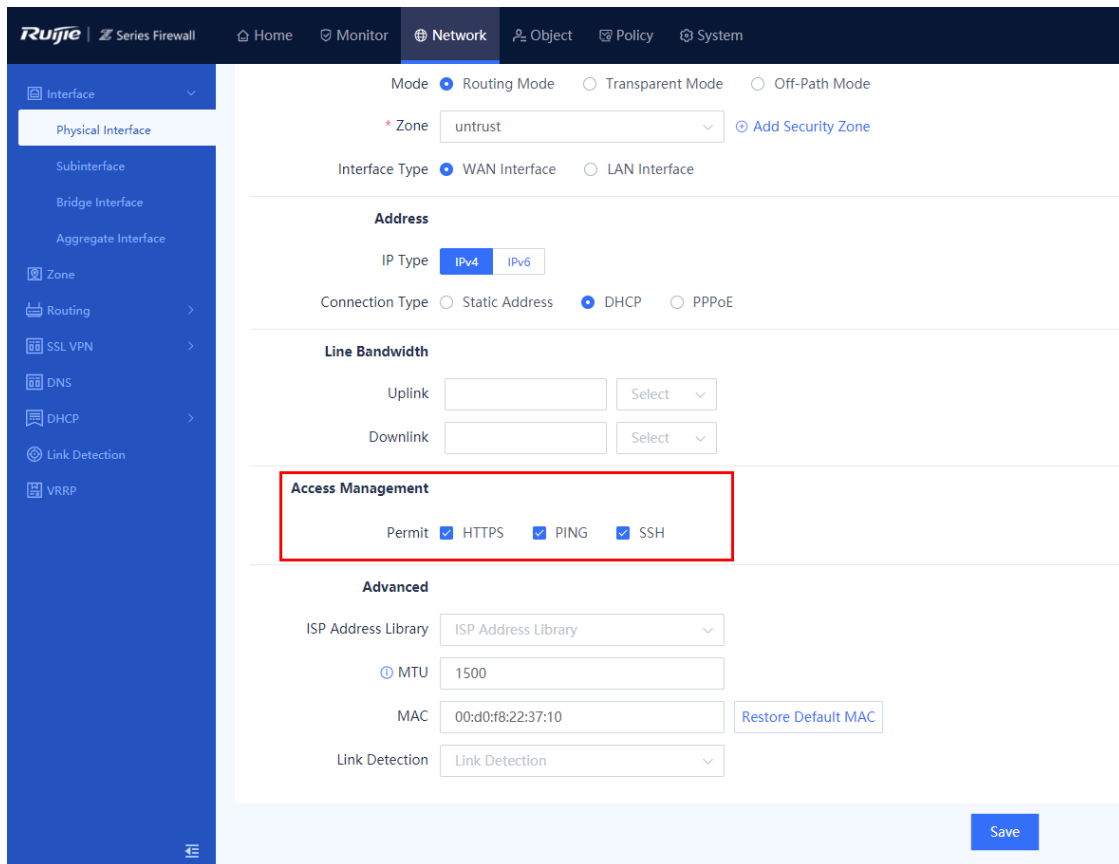
- By default, ping or SSH is disabled on the interface.
- The default timeout period is 30 minutes and maximum configurable timeout period is 1440 minutes.
- The default allowed consecutive login failures is 6 and the re-login interval is 3 minutes.

- A specific host address rather than a network segment must be added for a management host. Fully consider the probability of LAN and WAN management to properly add management hosts.

Method

(1) Check whether remote management is enabled on the interface.

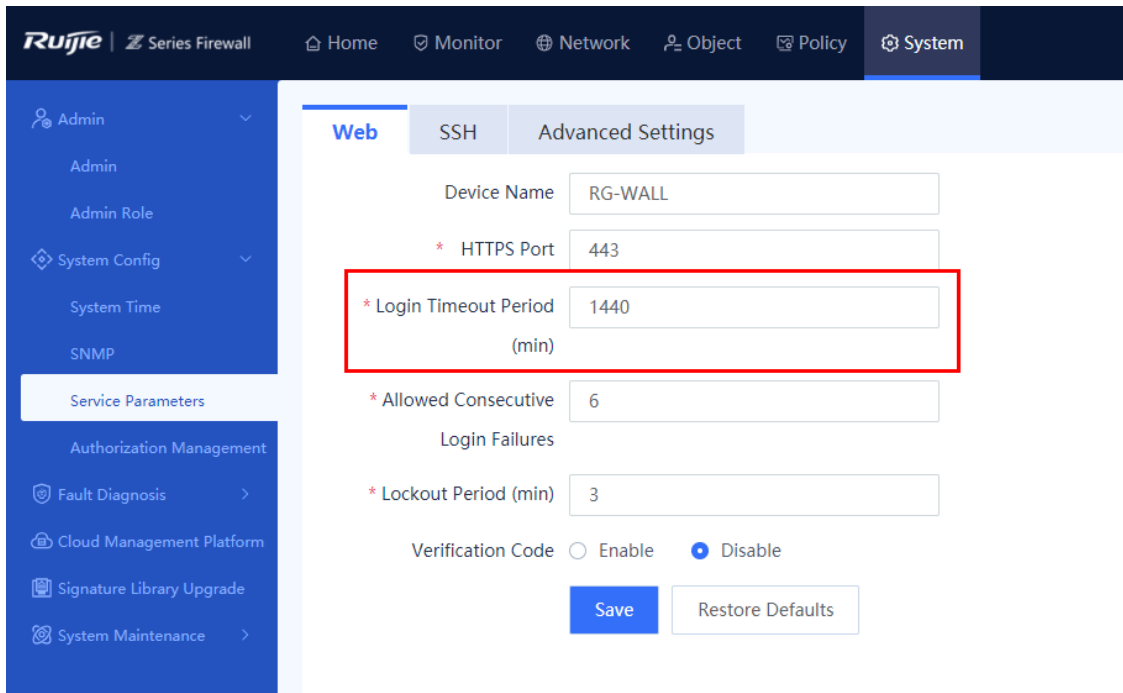
Log in to the web management page and choose **Network > Interface > Physical Interface**.



(2) Check whether web service parameters are set.

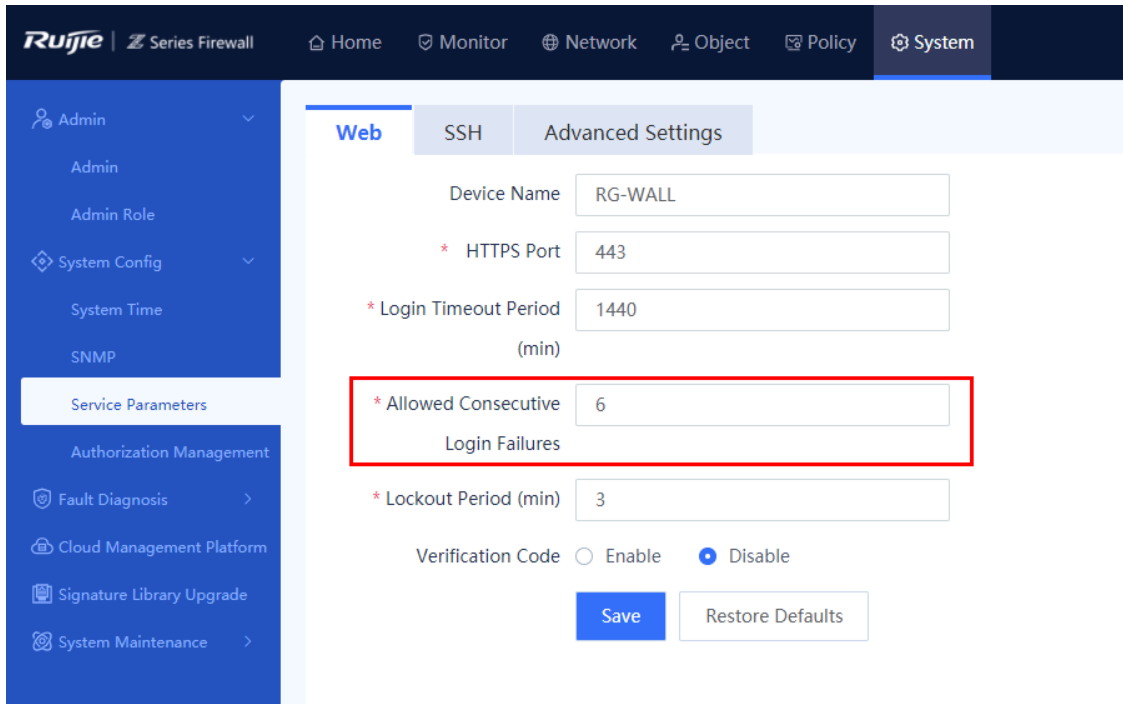
- Administrator login timeout period

Log in to the web management page and choose **System > System Config > Service Parameters**.



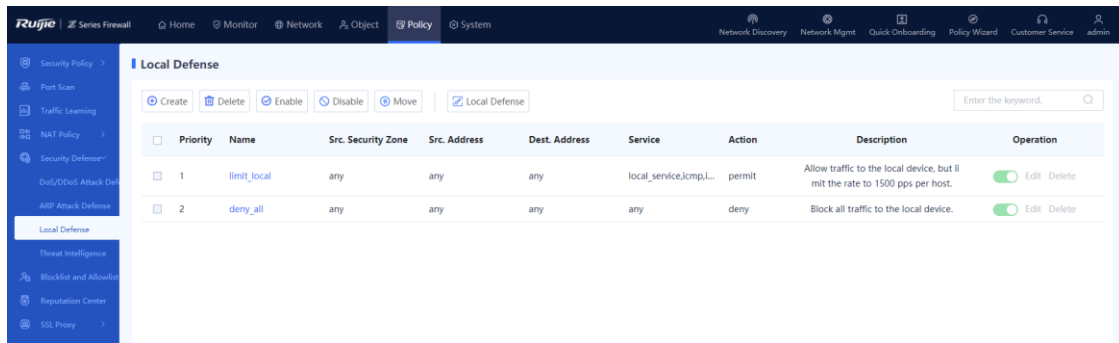
- Limit on administrator login failures

Log in to the web management page and choose **System > System Config > Service Parameters**.



(3) Management host settings

Log in to the web management page and choose **Policy > Security Defense > Local Defense**.



13.3 Checking Firewall Policies

Standards

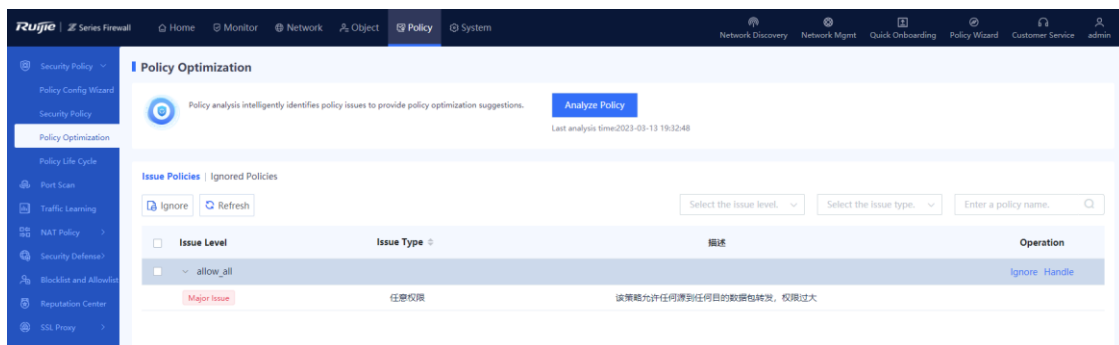
- An any-to-any policy makes the firewall meaningless and cannot achieve the purpose of access control. Administrators must know the data flow direction of customer services and implement access control based on the IP address and port number.
- All policies must be enabled. If a policy is not matched or does not hit any data flow within 90 days, the policy is considered to be improper.
- If the matching scope of one policy covers that of another policy but the two policies define different actions, a policy conflict occurs.

Method

Log in to the web management page and choose **Policy > Security Policy > Policy Optimization**.

Check whether policies with major problems exist in the **Issue Policies** area.

- Policy with all permissions (All objects in the policy are set to **any**.)
- Policy not matched within 90 days (The policy does not match any data flow within 90 days, according to the last time the policy is matched.)
- Completely conflicting policy (The matching scope of policy A covers that of policy B but the two policies define different actions.)



13.4 Checking the Operation Status

Standards

- Ensure that the CPU usage is lower than 75% during the service peak period. If the CPU usage of the firewall

is too high, it may be encountered with attacks or abnormal traffic. In this case, the firewall stops forwarding data or discards packets and the firewall cannot be managed.

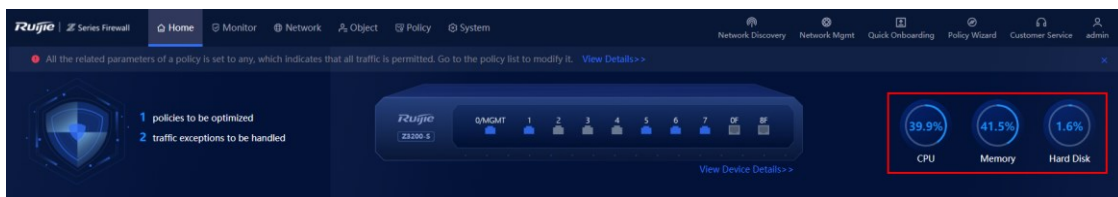
- Ensure that the memory usage is lower than 75% during the service peak period. If the memory usage of the firewall is too high, it may be encountered with attacks or abnormal traffic, or the number of abnormal concurrency is too high, which causes firewall exceptions.

Precautions

- The possible causes for high CPU usage are as follows:
 - The output of the **top** command indicates that some processes consume high CPU.
 - The UTM security function is enabled.
 - Abnormal traffic from attackers such as DDoS and broadcast storm exists.
- The possible causes for high memory usage are as follows:
 - The output of the **top** command indicates that some processes consume high memory.
 - The UTM security function is enabled.
 - The idle memory (cached or swap) is used to improve the system performance, which has no impact on services. You can run the **show memory** command to view the memory allocation information.

Method

Log in to the web management page and click **Home** to view the CPU usage and memory usage.



13.5 Checking the System Status

Standards

- Check whether the NTP server is configured and whether the time zone is correct.
- Confirm that the customer has purchased a license for the upgrade service and the license is still valid.

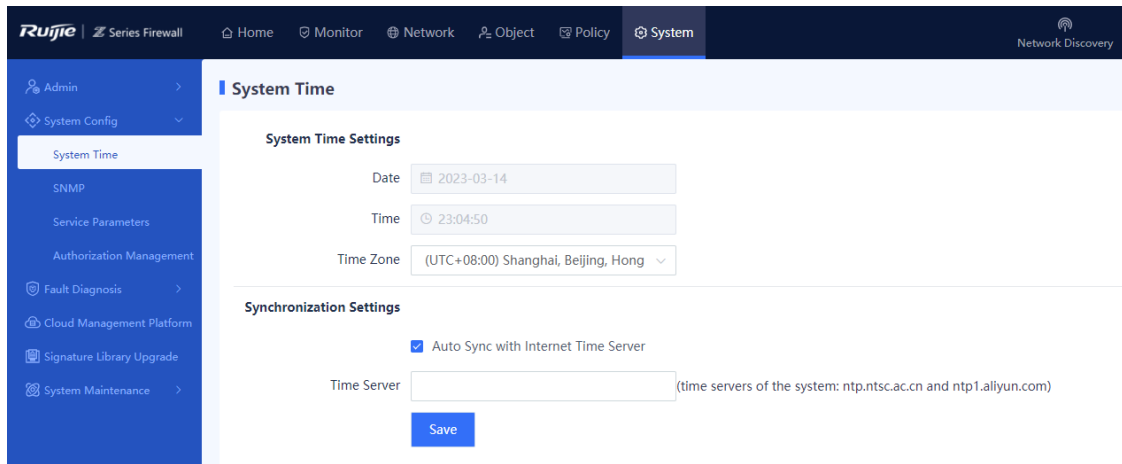
Precautions

Confirm that the customer has purchased the relevant license.

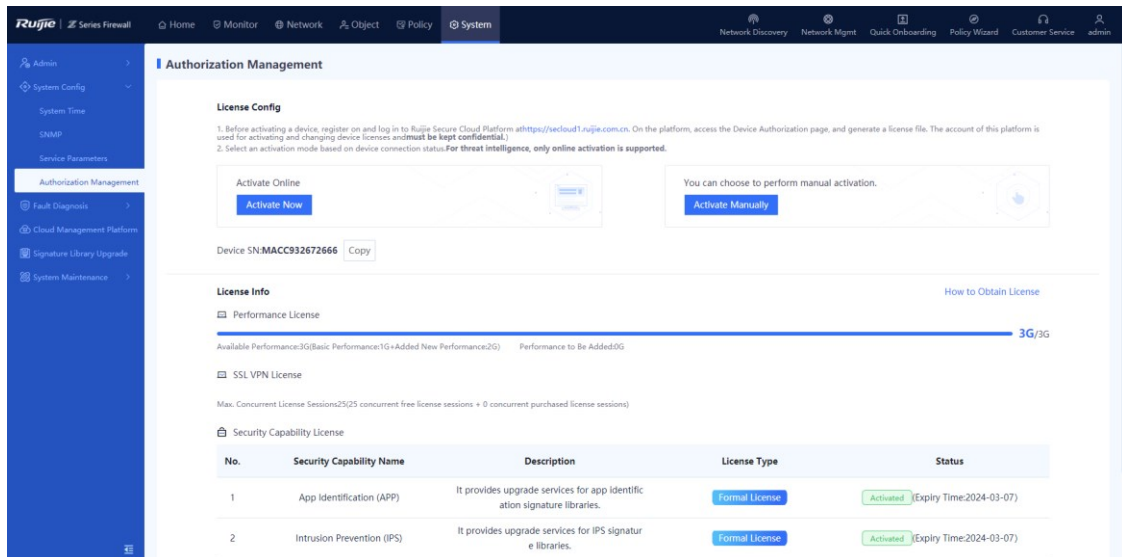
Method

- (1) Check whether the system time is accurate.

Log in to the web management page and choose **System > System Config > System Time**.



(2) Check the license status to confirm that the purchased license for the upgrade service is still valid.



13.6 Checking the Log Status

Standards

- If no hard disk is available, logs cannot be stored for 180 days.
- If no hard disk is available and no Syslog server is configured, the required storage time cannot be satisfied.

Precautions

- Confirm that the customer has purchased a hard disk.
- If no hard disk is available, the Syslog server is configured.

Method

(1) Check whether a hard disk is available.

- Log in to the web management page and choose **Monitor > Device Monitoring > Device Hardware Monitoring**.

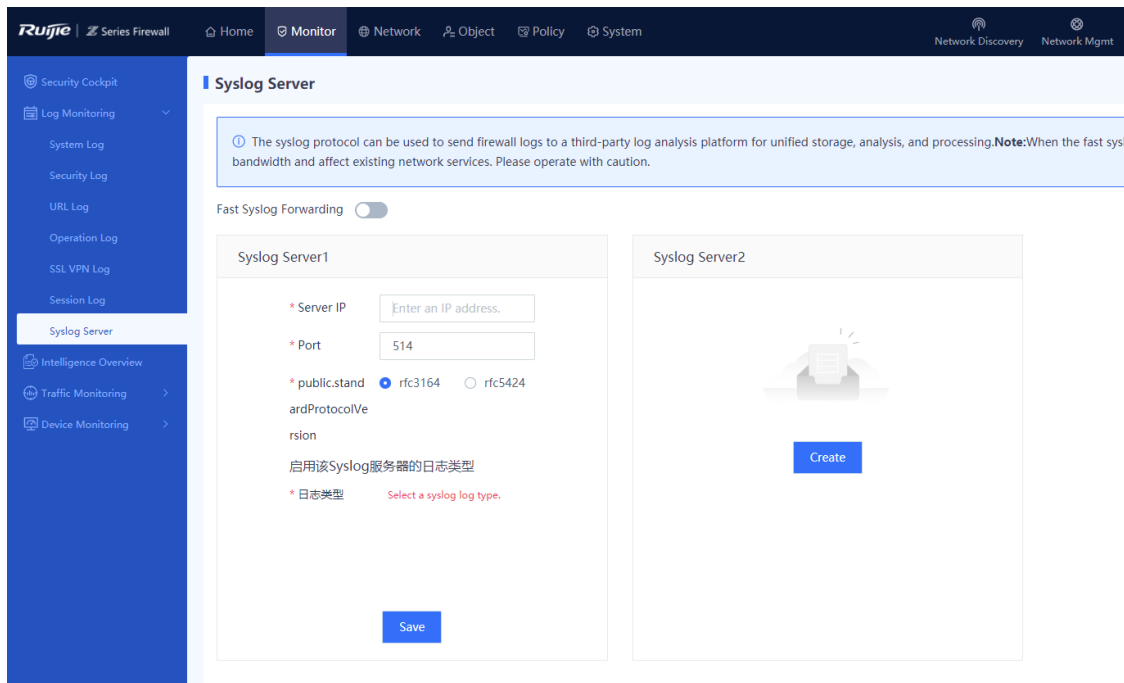


- Run the `firewall> show state system linux` command in the CLI.

```
disk-usage sda
total 1000204886016
partition sda1
fstype ext3
total 1000203835392
available 933954744320
..
```

(2) Check whether the Syslog server is configured and whether Syslog recording is enabled.

Log in to the web management page and choose **Monitor > Log Monitoring > Syslog Server**.



13.7 Checking the Network Connectivity

Standards

Use the traceroute method to check the network connectivity and data forwarding path. The purpose is to test the consistency of each path in the forward and reverse directions in the routing design. Specify a test plan according to the network planning in advance.

- (1) Select typical test items according to the actual service routes of the customer.
- (2) Suggestion: Test packets of the lengths 500, 2000, and 65000 to ensure that packets of different sizes can be normally forwarded.

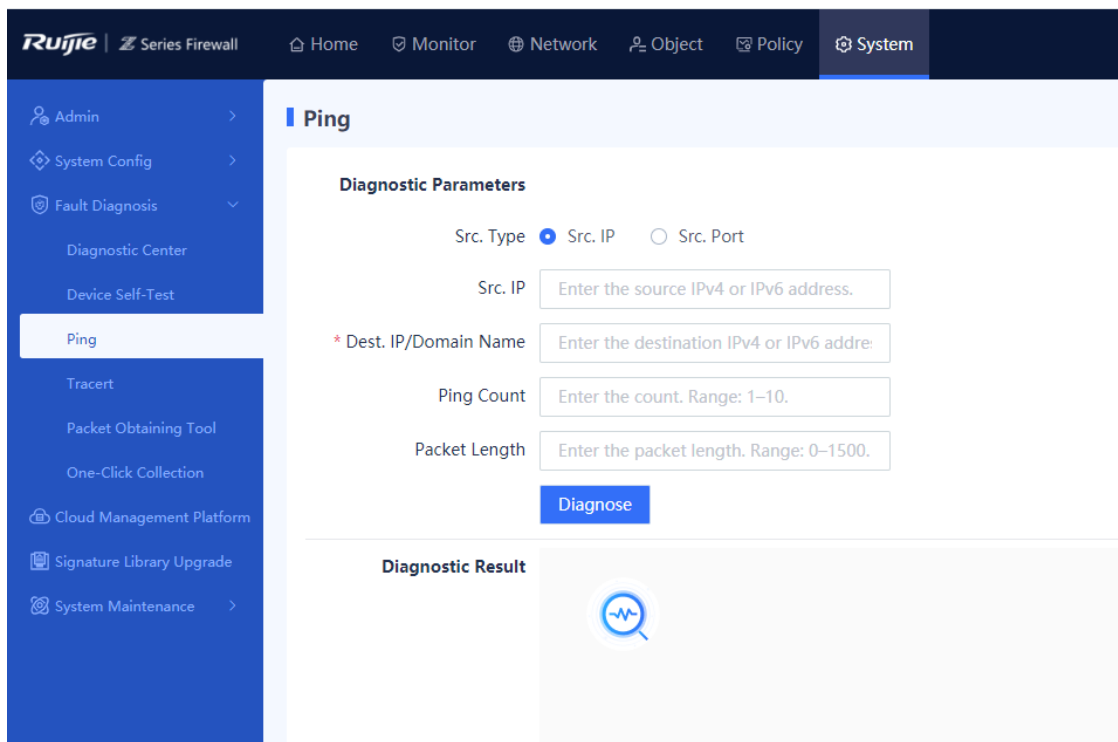
Note

ICMP filtering is enabled on some network devices by default. When you perform the preceding operations on these devices, packet loss may occur periodically. You are advised not to set the destination address to the device IP address during the execution.

Method

Check the service paths and then check the interface negotiation status after a certain time of delay.

Perform the traceroute or ping test on the web management page to check the connectivity of an Internet access device in the LAN.



13.8 Checking the Service Use Status

Method

Select a typical service system to perform subjective inspection on the service application use.

Standards

Verify the network deployment correctness through real service testing.

Check the application service use of the customer and check whether the software service system is normal.

- Internet services: Web browsing, file downloading, QQ, email, online video watching, and other service system access
- Internal customer services: Video conference and OA office. Test specific application services involved in the customer site.