

Ruijie RG-WALL 1600-Z-S Series

Cloud-Managed Firewalls

Cookbook

Document version: V1.9 Date: 2024-09-10 Copyright © 2024 Ruijie Networks

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.



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

Conventions

1. GUI Symbols

Interface symbol	Description	Example
Boldface	 Button names Window names, tab name, field name and menu items Link 	 Click OK. Select Config Wizard. 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.



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

1 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
1.1 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
2.1.1 Logging In to the Device from the Web	9 5
2.1.1 Logging In to the Device from the Web2.1.2 Logging In to the Device from the Console	9 5 9
 2.1.1 Logging In to the Device from the Web 2.1.2 Logging In to the Device from the Console 2.1.3 Logging In to the Device Using SSH 	9 5 9 2
 2.1.1 Logging In to the Device from the Web 2.1.2 Logging In to the Device from the Console 2.1.3 Logging In to the Device Using SSH 2.2 Modifying the Web Login Configuration 	9 5 9 2
2.1.1 Logging In to the Device from the Web	9 5 9 2 4
2.1.1 Logging In to the Device from the Web 9 2.1.2 Logging In to the Device from the Console 14 2.1.3 Logging In to the Device Using SSH 14 2.2 Modifying the Web Login Configuration 24 2.3 Account Permission Settings 24 2.3.1 Administrator Permission Overview 24	9 5 9 2 4 4
2.1.1 Logging In to the Device from the Web 9 2.1.2 Logging In to the Device from the Console 14 2.1.3 Logging In to the Device Using SSH 14 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	9 5 9 2 4 4 5
2.1.1 Logging In to the Device from the Web 9 2.1.2 Logging In to the Device from the Console 14 2.1.3 Logging In to the Device Using SSH 14 2.1.3 Logging In to the Device Using SSH 14 2.1.3 Logging In to the Device Using SSH 14 2.1.4 Modifying the Web Login Configuration 24 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 24	9 5 9 2 4 4 5 0

2.4.2 Importing the Configuration	
2.5 Defaults Restoration	
2.5.1 Web-based One-Click Restoration	
2.5.2 Restoration by Pressing the Reset Button	
2.6 Password Restoration	
2.7 SNMP Management	40
2.7.1 Overview	40
2.7.2 Configuring SNMP	41
3 License Activation	
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	
3.2.3 License Activation Methods	64
3.3 Precautions for License Activation	67
4 Configuring the Syslog Server	
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	
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	
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)	
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 t	he 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	
8.4.1 Configuring a Keyword Set	264
8.4.2 URL Category	265
8.5 URL Filtering	
8.5.1 Custom URL Filtering Template	
8.5.2 Predefined URL Filtering Template	270
8.5.3 Configuration Examples of Blocking Websites	272
8.6 Keyword Filtering	
8.7 Behavior Analysis	
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	
8.10 Port Scan	
8.11 Traffic Learning	
8.12 Security Policy	
8.12.1 Overview	312
8.12.2 Configuring Security Policy (Using Wizard)	314
8.12.3 Configuring Security Policy (Manual)	
8.12.4 Adjusting Policy Order	

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	
8.12.9 Exporting Security Policies	335
8.12.10 Enabling Basic Protocol Packet Control	
8.12.11 Configuration Examples of DHCP + Security Policies	
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	
8.15.1 Overview	
8.15.2 Precautions	
8.15.3 Creating an IPv4 Allowlist	361
8.15.4 Creating an IPv6 Allowlist	
8.15.5 Creating an IPv4 Blocklist	
8.15.6 Creating an IPv6 Blocklist	
8.15.7 Creating a Temporary IPv4 Blocklist	
8.15.8 Creating a Temporary IPv6 Blocklist	
8.16 Security Rule Base Management	

8.17 Connecting to Ruijie Cloud
8.17.1 Overview
8.17.2 Connecting to Ruijie Cloud
8.17.3 Operations on Ruijie Cloud
8.18 DNS Server
8.18.1 Configuring DNS
8.18.2 Configuring DNS Transparent Proxy
8.18.3 Configuring DDNS
8.19 Intelligent Routing
8.20 Address Library Routing (ISP-based Routing)
8.20.1 Overview
8.20.2 Configuring an ISP Address Library
8.20.3 Configuring ISP Routing
8.20.4 Viewing the Routing Table of Address Library401
8.21 Link Aggregation402
8.22 Link Detection
8.23 Outbound Interface Load Balancing411
8.23.1 Overview
8.23.2 Configuring MLLB Based on Uplink Bandwidth for a Network with Specific Routes412
8.23.3 Configuring MLLB Based on Uplink Bandwidth for DNS Transparent Proxy419
8.23.4 Configuring MLLB Based on Link Priority for Intelligent Routing
8.23.5 Configuring MLLB Based on Bandwidth and Sessions for a Network with Specific
Routes
8.23.6 Common Faults Diagnosis
8.24 SSL VPN

8.24.1 Overview
8.24.2 Application Scenario441
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)
8.24.6 Typical Configuration of SSL VPN Access Using a Domain Name over Multiple Lines
(Local Authentication)
8.24.7 Typical Configuration of RADIUS Authentication Access
8.24.8 Typical Configuration of SMS Two-Factor Authentication (Twilio)
8.24.9 Common Faults and Troubleshooting Roadmaps509
8.25 IPsec VPN
8.25.1 Overview
8.25.2 Principles
8.25.3 Application Scenario515
8.25.4 Configuration Examples of Site-to-Site IPsec VPN
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
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 Traversal575
8.25.9 Configuration Examples of IPsec VPN Networking with Link Redundancy598
8.25.10 Common Faults and Troubleshooting Roadmaps611

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	
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 Information70)5
9.6 Intelligence Overview70)7
10 Advanced Features	0
10.1 ALG77	10
10.1.1 Overview	10
10.1.2 Configuring ALG77	10
11 FAQs	2
11.1 Product Knowledge77	12
11.1.1 What Is the Hardware Architecture of the RG-WALL 1600-Z-S Series Firewall?7	12
11.1.2 What Are the Restrictions of Port MGMT?77	12
11.2 Firewall Deployment7	12
11.2.1 What Firewall Deployment Modes Are Supported?7	12
11.2.2 Can GE Optical Port and 10GE Optical Port Form a Bridge?7	15
11.3 Typical Feature Configuration77	15
11.3.1 How Is Source NAT Implemented?77	15
11.3.2 Does the Firewall Support Link Detection?7	15
11.3.3 Does the Z-S Series Firewall Block TCP Sessions in the Secondary Traversal	
Scenario?77	15
11.3.4 Does the Firewall Support Link Aggregation?7	16
11.4 Login Management7	16
11.4.1 What Can I Do If I Fail to Log In to the Web Page?77	16
11.4.2 What Can I Do If I Fail to Log In to the System Through SSH?	16
11.5 O&M and Monitoring77	17
11.5.1 How Do I View the CPU, Memory, and Hard Disk Information of the Firewall?7	17
11.5.2 How Do I View the Interface Traffic of the Firewall?	17

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	
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

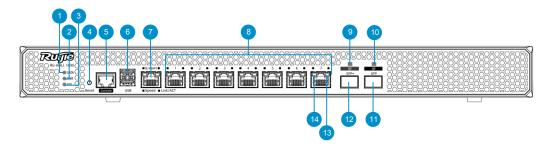


Table 1-1 Components on the Front Pan	Table 1-1	Components on the Front Panel
---------------------------------------	-----------	-------------------------------

No.	Component	Description
1	SATA hard disk status LED (SATA)	Steady green: A hard disk is connected.Blinking green: Data is being read or written.
2	Power module status LED (PWR)	 Steady green: The power supply is normal. Off: The power supply is cut off or fails.

No.	Component	Description	
3	System status LED (SYS)	 Blinking green: The device is powered on and being initialized. Steady green: Initialization is complete. Steady red: An alarm is generated. 	
4	Reset button	 Restarting the device: Press the button for less than 3 seconds. Restoring factory settings: Press the button for more than 5 seconds. When you perform either of the preceding operations, device status information is collected. After the device restarts, you can access the web UI of the firewall, choose System > One-Click Collection, and download the information. 	
5	Console port	 It is used to connect to the console for device maintenance and diagnosis. Note: 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	 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	 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 <u>Table 1-5</u> .	
12	10GE SFP+ port	Port 0F. For details about optical modules that support this port, see <u>Table 1-5</u> .	
13	Link/ACT status LEDs (square) of 10/100/1000BASE-T ports	 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	 Steady orange: Gbit/s port speed Off: 100/10 Mbit/s port speed

2. Rear Panel

Figure 1-2 Rear Panel

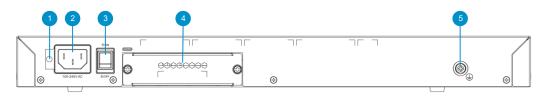


Table 1-2 Components on the Rear Panel

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

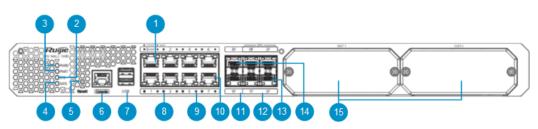
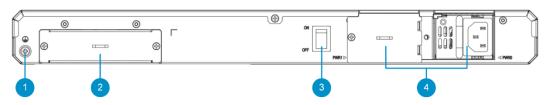


Table 1-3	Components on	the Front Panel
	e e inpenie i i e i i	

No.	Component	Description	
1	MGMT port	It is used to access the device management page upon first login.	
2	System status LED (SYS)	 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)	 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	 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: 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	 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	Solid orange: Gbps port speedOff: 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	Solid green: The port is connected.Blinking green: The port is receiving or sending data.	
12	10GE SFP + port LEDs	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



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.

Table 1-4 Components on the Rear Panel

1.4 Specifications

1.4.1 RG-WALL 1600-Z3200-S Specifications

Table 1-	5 S	pecifications
	• •	poontoutiono

Model	RG-WALL 1600-Z3200-S			
Memory	4 GB DDR4 memory			
Boot ROM	3 MB			
еММС	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	 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. 			

	 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	1 x RJ45 MGMT port (reusing Ge0/0)					
Port	1 x RJ45 console port (RS-232)					
USB Port	x USB 2.0 ports					
Bypass Port	Not supported					
Expansion Module	Not supported					
Dimensions	440 mm × 200 mm x 43.6 mm (17.32 in. x 7.87 in. x 1.72 in.; without rubber pads)					
(W x D x H)						
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 1-6Specifications

Model	RG-WALL 1600-Z5100-S	
Memory	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	 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	 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	
	2 x expansion module slots (expansion modules not supported)	
Module Slot	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	440 mm x 300 mm x 43.6 mm (17.32 in. x 11.81 in. x 1.72 in.)	
(W x D x H)		
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	 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	 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

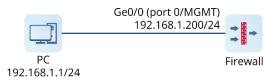
2.1.1 Logging In to the Device from the Web

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 <u>Table 2-1</u>. 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 <u>2.1.2 Logging In to the</u> <u>Device from the Console</u>.
- If you change the password and forget it, restore the initial password. For details, see <u>2.6 Password</u> <u>Restoration</u>.
- The management PC and firewall have been connected and can communicate with each other.
 - o Port 0/MGMT on the firewall is connected to the management PC through a network cable.

Product Cookbook



- 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.
 - o 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

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

Procedure

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

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

Internet 协议版本 4 (TCP/IPv4) Prop	erties >	<
General		
You can get IP settings assigned auto this capability. Otherwise, you need t for the appropriate IP settings.		
O <u>O</u> btain an IP address automatica	lly	
• Use the following IP address:		
IP address:	192.168.1.1	
Subnet mask:	255 . 255 . 255 . 0	
Default gateway:	192 . 168 . 1 . 200	
Obtain DNS server address auto	matically	
• Use the following DNS server ad	dresses:	
Preferred DNS server:	114 . 114 . 114 . 114	
<u>A</u> lternate DNS server:		
Ualidate settings upon exit	Ad <u>v</u> anced	
	OK Cancel	

(2) Log in to the web management page.

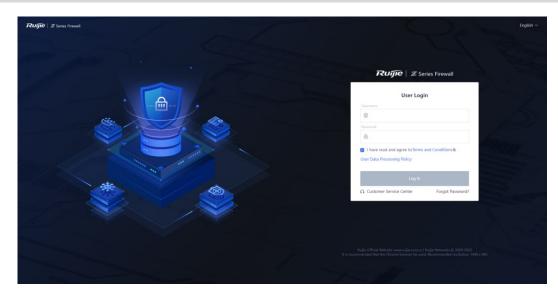
Note

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

- a Open a browser on the management PC.
- b Enter https://192.168.1.200 in the address bar and press Enter.

The login page is displayed.

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



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

Ruijie Z Series Firewall	습 Home	⊘ Monitor	Network	🗟 Policy 💿 System				M Network Discovery	Network Mgmt Quick Onb		Customer Service a
🛙 Interface 🗸 🗸	Physi	cal Interface									
Physical Interface Subinterface	⊖ En	able 🚫 Disable	e 🖸 Refresh								
Bridge Interface Aggregate Interface		Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mode	MTU	Operation
] Zone		Ge0/0			Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500	Edit
Routing >		Ge0/1			Routing	trust	IPv4: DHCP		-	1500	Edit
SSLVPN >		Ge0/2	-		Transparent	-	-	-	-	1500	C Edit
DNS		Ge0/3			Transparent					1500	C Edit
рнср >		Ge0/4	-		Transparent	-	-	-	-	1500	C Edit
Link Detection		Ge0/5	÷		Transparent	-	-		-	1500	C Edit
VRRP		Ge0/6			Transparent			÷	-	1500	C Edit
		Ge0/7	-		Routing	untrust	IPv4: DHCP	172.20.37.124/24	-	1500	C Edit
		TenGe0/0			Transparent				-	1500	C Edit
		Ge0/8			Transparent					1500	C Edit

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

K Back Edit Physical I	nterface			
Basic Info				
Interface Name	Ge0/1			
Description				
Connection Status	• Enable 🔿 Disable			
Mode	• Routing Mode 🛛 Tr	ransparent Mode	Off-Path Mode	
* Zone	untrust	~	⊕ Add Security Zone	
Interface Type	• WAN Interface O	AN Interface		
Address				
IP Туре	IPv4 IPv6			
Connection Type	• Static Address O D	HCP O PPPoe	E	
* IP/Mask	192.168.0.200/24			
* Next-Hop Address	192.168.0.254			
Default Route				
Line Bandwidth				
Uplink		Select ~		
Downlink		Select ~		
Access Management				
Permit	🗹 HTTPS 🛛 PING	✓ SSH		
Advanced				
ISP Address Library	ISP Address Library	~		
① MTU	1500			
MAC	00:d0:f8:22:37:0a		Restore Default MAC	
Link Detection	Link Detection	~		

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

ltem	Description	Remarks
Access Management	 Whether the interface supports HTTPS, ping, and SSH. HTTPS: Allows users to access the device using https://Interface IP address, such as https://192.168.0.200. PING: Allows users to ping the interface address. If this option is not selected, ping fails even if there is a reachable route. SSH: Allows users to access the device by creating an SSH connection with the interface IP address, such as ssh 192.168.0.200. 	The configuration takes effect when local defense is enabled on the device. [Example] Select HTTPS .

d Click Save.

Follow-up Procedure

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

Figure 2-1 Web Management Page Layout

Admin List						
ole ⓒ Create 🗑 Delete ⊘ Enab	le 🛇 Disable 🗴 Password Po	olicy 🖸 Refresh				Enter the keyword.
nőg > Account	Role	Verify Trusted H ost	IPv4 Host	IPv6 Trusted Host	Description	Operation
nagement Platform	Super Admin	Disabled				Edit
Library Upgrade	Security Admin	Disabled	-		-	Change Password Edit
aintenance > 📄 useradmin	User Admin	Disabled				Change Password Edit
🗌 auditadmin	Auditor	Disabled	-		-	Change Password Edit
abctes		Disabled				Change Password Edit Delete

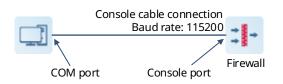
Area	Description
Mark and panel area	 This area displays the company logo, device name, and function panel. This area supports new network discovery, network-wide management, quick onboarding, policy configuration wizard, and customer service, helping users quickly complete deployment operations. This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

2.1.2 Logging In to the Device from the Console

Application Scenario

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

Network Topology



Tool Preparation

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



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 <u>Figure 2-2</u>.

If your PC does not have a COM port (such as the laptop), the USB-to-COM cable (as shown in <u>Figure 2-3</u>) 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 <u>Model 2</u> directly.

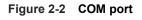




Figure 2-3 USB-to-COM Cable



- 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

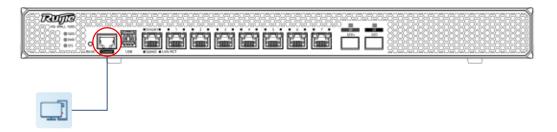
- Prepare a configuration cable and a PC that can be connected to a configuration cable. (For details, see **Tool Preparation**.)
- (2) Connect the configuration cable.

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

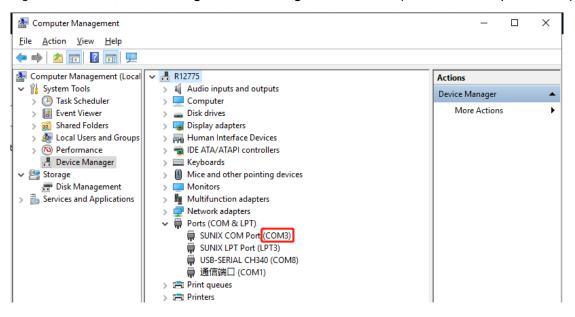
This section uses SecureCRT as an example. For details about other programs, see the corresponding operation manual.

a View identified COM ports on the PC.



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

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



b Run the SecureCRT software. The Quick Connect dialog box is displayed automatically. (If the dialog

box is not displayed, click *in* the menu bar.) In the dialog box, set the connection parameters and click **Connect**. The following table describes the connection parameters that you need to set.

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

Quick Connect			×
<u>Protocol:</u> P <u>o</u> rt: <u>B</u> aud rate: <u>D</u> ata bits: P <u>a</u> rity: <u>S</u> top bits:	Serial COM3 ~ 115200 ~ 8 ~ None ~ 1 ~	Flow Control	
Sho <u>w</u> quick c	onnect on startup	✓ Sa <u>v</u> e session ✓ Open in a <u>t</u> ab Connect Cance	el

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 <u>2.6 Password Restoration</u>.)

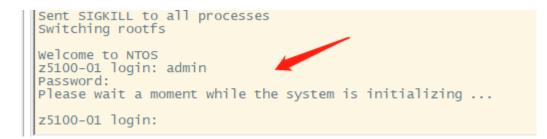
1 Note

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.

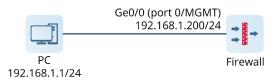


2.1.3 Logging In to the Device Using SSH

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.

K Back Edit Physical Interface	
Basic Info	
Interface Name Ge0/0	
Description	
Connection Status 🧿 Enable 🛛	Disable
Mode 🧿 Routing Mod	e 💿 Transparent Mode 💿 Off-Path Mode
* Zone trust	✓ O Add Security Zone
Interface Type 🔘 WAN Interfac	e O LAN Interface
Address	
IP Type IPv4 IPv6	
Connection Type 🧿 Static Address	s ODHCP OPPOE
* IP/Mask 192.168.1.200/	24
Line Bandwidth	
Uplink	Select V
Downlink	Select ~
Access Management	
Permit 🗹 HTTPS 🔽	PING 🗹 SSH
Advanced	
① MTU 1500	
MAC 00:d0:f8:22:37:	09 Restore Default MAC
	Save

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

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

The following uses the SecureCRT software as an example.

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

[📄 n	ot connected - Secu	reCRT						
	File	Edit View Opti	ons Transfer	Script	Tools	Window	Help		
	40	Connect	Alt+C	6	A 7	3 53 6	7 🕉	1 🔞 🖪	
	20	Quick Connect Connect in Tab/Tile.	Alt+Q						
	G	Connect in Tab/Tile.	Alt+B						
	3]	Reconnect	Enter						
		Reconnect All							

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

Quick Connect		\times
Protocol: Hostname:	SSH2 ~ 192.168.1.200	
Port:	22 Firewall: None	/
Username:		
Authentication Password PublicKey Keyboard I GSSAPI	interactive	
Show quick co	onnect on startup Save session	

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.

Web	SSH	Advanced S	Settings		
		Device Name	Z3200-s		
		* HTTPS Port	443		✓ Auto Redirection for HTTP
* [.ogin Timeo	ut Period (min)	1440		
* Allowed	Consecutive	e Login Failures	6		
	* Locko	ut Period (min)	3		
	Ve	rification Code	Enable	 Disable 	
			Save	Restore Defaults	

ltem	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 <u>7.1 Integrated</u> <u>Deployment on Ruijie Cloud</u> .	[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.	 Enter an integer in the range of 0 to 1440, in minutes. The default value is 30 minutes. [Example] 30
Allowed Consecutive Login Failures	Number of consecutive incorrect password attempts. If a user enters an incorrect password for a number of times exceeding the value specified by this parameter, the system automatically locks the user.	 Enter an integer in the range of 0 to 10. The default value is 6. [Example] 3
Lockout Period	Period of time within which the automatically locked user is not allowed to log in to the web management page.	 Enter an integer in the range of 0 to 30, in minutes. The default value is 3. [Example] 30
Verification Code	Whether a verification code is required for login to the web management page.	By default, the value is Enable . [Example] Enable

(3) Click Save.

2.3 Account Permission Settings

2.3.1 Administrator Permission Overview

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

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

Table 2-2 Permissions of the Default Roles

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.

Cre	eate 🔟 Delete 🥝 Enable (Change P	assword	\otimes			
	Account				ted Host	Description	Operation
	admin	Account	useradmin				Edit
	securityadmin	* 🕕 New	Enter the new password.			-	Change Password Edit
	useradmin	Password				-	Change Password Edit
	auditadmin	* Confirm Password	Enter the same password as above.				Change Password Edit

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

Password description:

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

Follow-up Procedure

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

< Back	Edit Admin Ad	count
	Basic Info	
	* Account	auditadmin
	* Enabled State	• Enable O Disable
	* Role	审计员 >
	Description	
	Advanced	
		To ensure account security, change the password when you enable the default administrator for the first time.
	* () Password	
	* Confirm Password	

• The default administrator account cannot be deleted.

2.3.3 Creating an Administrator

1. Creating an Administrator Role

Application Scenario

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

Procedure

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

Adm	n Role		
🕒 Cr	eate 🗊 Delete 🕻 Refresh	pub002.searchRoleName	
	Admin Role Name	Description	Operation
	Super Admin	-	Edit
	Security Admin	-	Edit
	User Admin	-	Edit
	Auditor	-	Edit

Basic Info				
* Admin Role Name				
Description				
Permission Settings				
	Permission	• Read-Write	O Read-Only	○ None
	> Monitor	0		
	> Network	0		
	> Object	0		
	> Policy	0		
	> System	0		
	> Quick Onboarding	0		
	> Policy Wizard	0		

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

Save	

ltem	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 Setting	Permission Settings					

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

n List						
eate 🗇 Delete 🔗 Enable	S Disable & Pa	assword Policy C Ref	resh			Enter the keyword.
Account	Role	Verify Trusted H ost	IPv4 Host	IPv6 Trusted Host	Description	Operation
admin	Super Admin	Disabled	-	-	-	Edit
securityadmin	Security Admin	Disabled	-	-	-	Change Password Edit
useradmin	User Admin	Disabled	-	-	-	Change Password Edit
auditadmin	Auditor	Disabled	-	-	-	Change Password Edit
test	Auditor	Disabled		-	-	Change Password Edit Delete
	Account admin securityadmin useradmin auditadmin	Delete Enable Disable Pressure Account Role Role Role admin Super Admin Super Admin Super Admin securityadmin Security Admin Super Admin Super Admin useradmin User Admin Auditor Super Admin	Delete Enable Disable δ Password Policy C Ref Account Role Verify Trusted H ost Ost Ost admin Super Admin Disabled ost ost securityadmin Security Admin Disabled ost useradmin User Admin Disabled ost auditadmin Auditor Disabled ost	Delete Enable Disable Password Policy Refresh Account Rele Verify Trusted H ost IPv4 Host admin Super Admin Disabled - securityadmin Security Admin Disabled - useradmin User Admin Disabled - auditadmin Auditor Disabled -	Delete Enable Disable Password Policy Refresh Account Role Verify Trusted H ost IPv4 Host IPv6 Trusted Host admin Super Admin Disabled - - securityadmin Security Admin Disabled - - useradmin User Admin Disabled - - auditadmin Auditor Disabled - -	Recount Role Verify Trusted H ost IPv4 Host IPv6 Trusted Host Description admin Super Admin Disabled - - - securityadmin Security Admin Disabled - - - useradmin User Admin Disabled - - - auditadmin Auditor Disabled - - -

(3) Set parameters for the new administrator.

< Back Add Admin Ad	count	
Basic Info		
* Account	Enter	
* Enabled State	• Enable 🔿 Disable	
* Role	Select a role.	
Description	Enter the description.	
Advanced	11	
* 🛈 Password	Enter the password.	
* Confirm Password	Enter the same password as above.	
Configure Trusted Host		
Restrict Trusted Host Login		
() IPv4 Trusted Host 1	IP ~ 0.0.0/0	🗓 Delete
	• Add IPv4 Trusted Host	
 IPv6 Trusted Host 1 	IP ~ ::/0	🖻 Delete
	€ Add IPv6 Trusted Host	
① MAC Trusted Host 1	aa:aa:aa:aa:aa:aa	🗓 Delete
	Add MAC Trusted Host ■	
		Save

Item	Description	Remarks
Basic Info		
Account	Username of the created administrator.	 The username can contain letters, digits, and underscores (_), and must start with a letter. The value cannot be the same as an existing administrator username. [Example] Admin_security
Enabled State	Whether to enable the new administrator account.	[Example] Enable

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		1
Password	Password used by the new administrator to log in to the web UI.	 A password must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Chinese characters, spaces, and fullwidth 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 Trust	red 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 fullwidth 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	100		Day
Age			
Sub	mit	Cance	el

- (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

Change Password

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 shortcut menu.

ကြ Network Discovery	⊗ Network Mgmt	€ Quick Onboarding	e Policy V) Wizard	ြ Customer Servi	ce admin
					admin	
					Super Adm	in
8F		21.9	%	Chan	ge Password	Log Out

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

 \otimes

5				_
* Old Password	Enter the old	password.		
* ① New Password	Enter the new	password.		
* Confirm Password	Enter the same	e password as a	bove.	
	Confirm	Cancel		

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

New Password	Password after change.	 The new password must meet the following requirements: Contain 8 to 15 characters. Contain at least three types of the following: uppercase letters, lowercase letters, digits, and special characters, and cannot contain Chinese characters, spaces, or full-width characters. Cannot be the same as the username or the username in reverse order.
Confirm Password	Password after change that is entered again.	The value of Confirm Password must be the same as that of New Password .

(7) Click Confirm.

3. Changing the Password of Administrators Except the Super Admin

Application Scenario

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

Procedure

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

 (\times)

The Change Password dialog box is displayed.

Change Password

* Old Password	Enter the old password.
* ① New Password	Enter the new password.
* Confirm Password	Enter the same password as above.

Confirm	Cancel
---------	--------

(3) Set a new password for the administrator.

The new password must meet the following requirements:

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

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

- Cannot be the same as the username or the username in reverse order.
- (4) Click Confirm.

2.4 Configuration Backup and Restoration

2.4.1 Exporting the Configuration

Application Scenario

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

Procedure

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

Config Backup
Back Up Config
Manually Back Up Export Current Config
Restoration Config
Restoration Mode: • Overwrite Current Config O Merge Current Config
Mode 1: Restore from a backup file on the device.
running-cfg-20240123163318.tar.gz \vee Restore
Mode 2: Restore from a local backup file.
Select a configuration file. Browse Restore

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

Config Backup	
Back Up Config	
Annually Back Up	nt Config
Restoration Config	
Restoration Mode: • Overwrite Current Config	O Merge Current Config
Mode 1: Restore from a backup file on the d	evice.
running-cfg-20240123163318.tar.gz	✓ Restore
Mode 2: Restore from a local backup file.	
Select a configuration file.	Browse Restore

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.
 - o Select a restoration mode.

Config Backup
Back Up Config
Manually Back Up Export Current Config
Restoration Config
Restoration Mode: • Overwrite Current Config O Merge Current Config
Mode 1: Restore from a backup file on the device.
running-cfg-20240123163318.tar.gz \vee Restore
Mode 2: Restore from a local backup file.
Select a configuration file. Browse Restore

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

Back Up Config Manually Back Up Lypert Current Config					
Manually Back Up Export Current Config					
Restoration Config					
Restoration Mode: • Overwrite Current Config					
Mode 1: Restore from a backup file on the device.					
running-cfg-20240123163318.tar.gz V Restore					
Mode 2: Restore from a local backup file.					
Select a configuration 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.

Default	ts Restoration
	① When factory settings are restored, all existing configurations will be deleted. To retain existing configurations, clickExport Current Config first and then restore factory settings.
	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

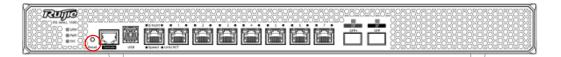
Application Scenario

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 <u>Figure 2-4</u>.

Figure 2-4 Reset Button on the Front Panel



Follow-up Procedure

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

Note

The Reset button provides the following functions:

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

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

2.6 Password Restoration

Application Scenario

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

Procedure

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

Ruíjie Z	Selles Filewall
User Lo	ogin
Username	
Password	
₽	
I have read and agree to Ter User Data Processing Policy	ms and Conditions&
Log I	n

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

Perform the Following Procedure

(\times)

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.

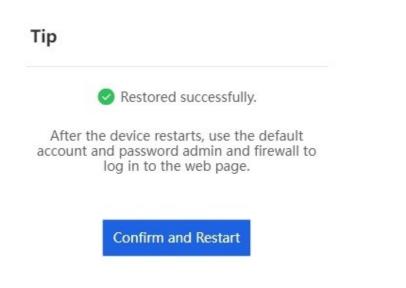
3. After login, click Restore Backup File. Then, the system prompts you to restart the device. After the device restarts, the Web login account and password are restored to admin and firewall, and the other configurations are retained. Please note that you need to use the original port and IP address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

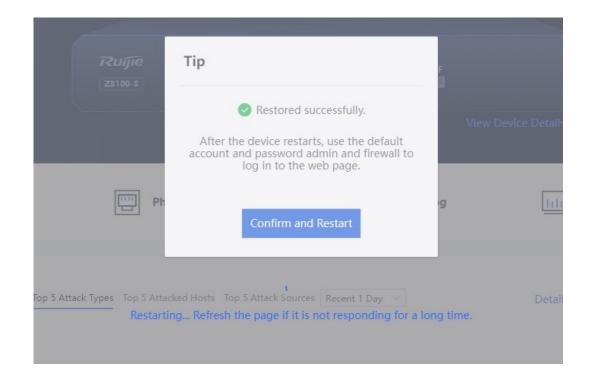
- a Hold down the Reset button for over 5s until the device is restored to the factory mode.
- b Connect the management PC to port 0/MGMT on the device panel through a network cable and set the IP address of the PC to one in the same network segment as that of port 0/MGMT (default address: 192.168.1.200), 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.

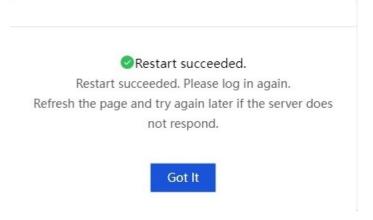
Restore Backup File
Backup files exist on the device. Select a handling method.
 Restore configuration from backup files. Device configuration before reset will be restored. (During restoration, the device will restart. Restore factory settings. (Backup files will be cleared.)
Confirm

Restore Backup Config









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

to ensure syst	em security, change your password upon login.
* New Password	Enter the new password.
	A password must contain at least three character categories,
	including uppercase and lowercase letters, digits, and specia characters.
	A password cannot contain any Chinese character, space, or
	full-width character.
	0 0
	a password cannot be the same as the username or the username in reverse order.
Confirm Password	Enter the same password as above.
	Password length range: 8–15 characters A password cannot be the same as the username or th username in reverse order.

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:

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

2.7.2 Configuring SNMP

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

Choose System > System Config > SNMP.

Ruffe Z Series Firewall	습 Home ⊘ Monitor ⊕ Ne	etwork 우 Object	@ Policy	⊜ System				Netwo	ጫ k Discovery	Ø Network Mgmt	1 Quick Onboardi
🔏 Admin 💦 🗧	SNMP										
System Config ~ System Time	Basic Config										
SNMP	SNMP (
Service Parameters	SNMP Version	v1/v2c v3									
Authorization Management	SNMP Read-Only Community String	Enter either an SNN	MP read-only								
Cloud Management Platform	SNMP Read-Write	Enter an SNMP rea	d-write comr								
🗒 Signature Library Upgrade	Community String										
System Maintenance >	Device Location	Enter the device lo									
	Contact Info	Enter contact infor									
	Trap Receiver										
	Trap Receiver1	Enter the receiver li	P address.	 Port 		① TRAP2 \ Type	Security Username	Enter the user	name.	🕒 Create	
		Save									
(2) Enable SI	NMP.										
SNMP											
	Basic Cor	nfia									
	SN	IMP 🔵	D								
		_									
	SNMP Vers	sion v	1/v2c		v3						
	SNMP Read-C	Dnly 🛛 🗄	nter e	ither a	an SNI	MP read-o	only				
	Community St	ring									
	community st	ing									
	SNMP Read-W	rite F	nter a	n SNN	/P rea	d-write co	omr				
			inter u		in rea						
	Community St	ring									
	Device Locat	tion 🛛 🗉	nter ti	ne dev	vice lo	cation.					
	Contact I	nfo E	inter c	ontac	t infor	mation.					

(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/v	/2c	1
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	1	1				
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
Туре	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).

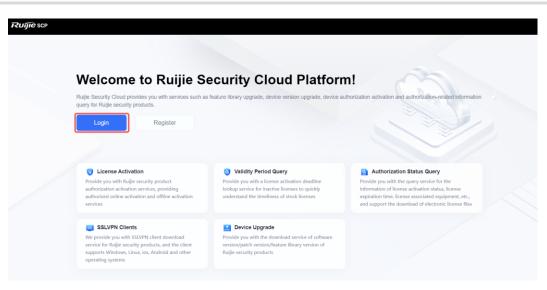
- a Enter <u>https://secloud1.ruijie.com.cn</u> in the browser and press **Enter**.
- b Click **Register** to access the registration page.
- c Enter the required user information to complete registration.

Tips Secure Cloud Platform a	account is used for device license activation, lice	nse change, and (other
	t can be bound to multiple devices and must be l rsonnel change, the account and password must		lf
accordingly .			
	Register		
* Country or region	Country or region	~	
* Time Zone	Time Zone	\sim	
* Email Address	Email Address		
* Password	Enter the password.		0
* Verification Code	Verification Code	Send Code	
	I have read and agree to Terms and Condition	onsandPrivacy Po	olicy.
	Sign up		

(2) Log in to the platform.

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

Click Login on the home page.



Account Please enter your username or email.	
Please enter your username or email.	
Password	
please enter Password	
Login	
I have read and agree to Terms and Conditions and Privacy Po	icy
Forgot password? Sign up	

- (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 dropdown list box. Click **Revise** to change the login password of the current user.

Ruíjie scp	A Home Security Operations	Device Operations	 Authorization Management 	Device Management	88 Version Management	[1****@qq.com
My account						(Personal Center Message Center
	Personal Information						G Log Out
	Account : 1*@qq.com @	Cancel Acc	ount				
	Password					ſ	Revise
	Regularly change to a high-strength passw	and to protect the account				Ľ	
	Email Email. 1'@qq.com <i>ଦ୍ଧ</i>						Revise
	Terms and Conditions And Privacy	Policy					
	Privacy Policy Release Time 2	023-09-08 00:00:00 Friday					

b Modify the email address.

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

Ruijie scp	A Home	Security Operations	Device Operations	Authorization Management	🖵 Device Management	B Version Management	***	1****@qq.com	
My account								 Personal Center Message Center 	J
	Persona	al Information Account : 1*@qq.com Ø	Cancel Acco	punt				G Log Out	
	Passwo Regularly c	rd hange to a high-strength password	to protect the account					Revise	
	Email Email: 1"@	qq.com 🐲						Revise	
	Terms an	d Conditions And Privacy P	olicy						
	4		23-09-08 00:00:00 Friday						

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.

Ruijie scp	A Home 😔 Security	Operations	Authorization Management	💭 Device Managemen	t 😰 Version Mana	igement 💿 Sy	stem Management		
Signature Library Ve App Identification Signatu	Product Type Select	a type. V Model	Select a model. V	oftware Version all	→ Ve	rsion Number Se	lect versionNumber 🤍	Query Reset	
Behavior Analysis Signat	No. File Name	Version Num	ber Version Descriptio	n Model	Software Version	releaseTime	File Size (MB)	MD5	Operation
Intrusion Prevention Sign	1 app_signatu	re.zip 20231222.16	5 20231222.1615	Universal	Universal	2023-12-22	0.69MB	4d98ddce4ef2d3	± Download
Virus Protection Signatur	2 app_signatu	re.zip 20231221.16	20231221.1601	Universal	Universal	2023-12-19	0.69MB	b3055177e9fbfdd	± Download
Virus Protection Signatur	3 app_signatu	re.zip 20231118.142	8 20231118.1428	Universal	Universal	2023-11-17	0.91MB	f404c8ec083e03	± Download
URL Signature Library	4 app_signatu	re.zip 20231110.166	0 20231110.1660	Universal	Universal	2023-11-13	0.67MB	8432da4d2bfed6	± Download
Threat Intelligence Signat	5 app_signatu	re.zip 20231103.110	3 20231103.1103	Universal	Universal	2023-11-03	1.10MB	5e9aea1db5e27e	± Download
Suttrate version ma V	6 app_signatu	re.zip 20231012.10	1 20231012.1011	Universal	Universal	2023-10-12	0.67MB	2b9d3a893a157f	± Download
	7 app_signatu	re.zip 20230611.16	9 20230611.1649	Universal	Universal	2023-09-21	0.51MB	7025ac553576d5	👱 Download
	8 app_signatu	re.zip 20230913.17	9 20230913.1719	Universal	Universal	2023-09-12	0.57MB	ac590bd0b7cbcf	👱 Download
	9 app_signatu	re.zip 20230912.10	3 20230912.1053	Universal	Universal	2023-09-11	0.57MB	1a2bc9792b3ed3	👱 Download
	10 app_signatu	re.zip 20230612.12	3 20230612.1213	Universal	Universal	2023-08-24	0.51MB	da1b2c7f9e9927	👱 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) Signature Library Threat Intelligence Signature Library URL Signature Library URL Signature Library							
Signature Library Type O Upgrade All (Upgrade all signature libraries online simultaneously) App Identification Signature Library	Virus Protection Signature Library (Deep Scan)	Virus Protection Signature Library (Quick Scan)					
Current Version/2023/222.1015 Last Upgrade Time- Latest Version/Unable to obtain the latest version. No SN record is found. Version State- Activation States Not Activated	Current Version- Lat ti Upgrade Time- Latest VersionUnable to obtain the latest version. No SN record is found. Version Statefile deep scan, function is not leaded admission StateNa Achivado	Current Version-20220619.0232 Last Upgrade Time: Latest Version-Unable to obtain the latest version. No SN record is found. Version State-Not Activated Activation StateNot Activated					
Online Upgrade Local Upgrade Rolling back	Online Upgrade Local Upgrade	Online Upgrade Local Upgrade	Consult				

Online upgrade

1 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.

ble Auto Upgrade		
ade Time:Daily 16 $\scriptstyle{\scriptstyle \lor}$ Hour 22 $\scriptstyle{\scriptstyle \lor}$ Minute		
ture Library: Select All App Identification Signature Library Svirus Protection Sign. ISP Address Library Threat Intelligence Signature Library	ature Library (Deep Scan) Virus Protection Signature Library (Quick Sca URL Signature Library & Behavior Analysis Signature Library	n) 😰 Intrusion Prevention Signature Library
pgrade All (Upgrade all signature libraries online simultaneously.)	View Protection Classifier Library (Dass Cost)	View Protection Stansture Ulterary (Duick Scon)
(Upgrade All Upgrade all signature libraries online simultaneously.) p Identification Signature Library	Virus Protection Signature Library (Deep Scan)	Virus Protection Signature Library (Quick Scan)
Ipgrade All Upgrade all signature libraries online simultaneously) p Identification Signature Library rent Version20231222.1615	Current Version:-	Current Version:20230619.0232
Ipgrade All Upgrade all signature libraries online simultaneously.) p Identification Signature Library rent Version20231222.1615 t Upgrade Time.		Current Version:20230619.0232 Last Upgrade Time-
Ipgrade All Upgrade all signature libraries online simultaneously.) p Identification Signature Library rrent Version:20231222.1015 Upgrade Time: est Version:Unable to obtain the latest version. No SN record is found.	Current Version:- Last Upgrade Time:-	Current Version:20230619.0232
ature Library Type Ipgrade All (Upgrade all signature libraries online simultaneously.) p Identification Signature Library rent Version20231222.1615 t Upgrade Time. est VersionUnable to obtain the latest version. No SN record is found. sion State- values Note Net Net Network	Current Version:- Last Upgrade Time- Latest Version:Unable to obtain the latest version. No SN record is found.	Current Version:20230619.0232 Last Upgrade Time: Latest Version:Unable to obtain the latest version. No SN record is found.

3. Behavior Analysis Signature Library Upgrade

Procedure

- Offline upgrade
- (1) Download a version file for the behavior analysis 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 > Behavior Analysis Signature Library, find the applicable version, and click Download in the Operation column to download the upgrade file to the local device.

Ruíjie scp	A Home	Security Operations	Device Operations	Authorization Management	Device Management	Stersion Manag	jement () Syst	tem Management		
Signature Library Ve	Desident	Type Select a type.	V Model Select	a model 🗸 Softw	are Version all	- Ver	sion Number Sele	ect versionNumber 🗸 🗸	Query Res	-
App Identification Signatu	Product	Select a type.	V Model Select	a model.	are version all	Ver	sion Number Sele	sci versionivumber 🗸	Query Res	et
Behavior Analysis Signat	No.	File Name	Version Number	Version Description	Model	Software Version	releaseTime	File Size (MB)	MD5	Operation
Intrusion Prevention Sign	1	content_signature_202312	221.0001.zip 20231221.0001		Universal	Universal	2023-12-25	0.00MB	e65ea9da00c8c7	坐 Download
Virus Protection Signatur										
Virus Protection Signatur										
URL Signature Library										
Threat Intelligence Signat										
Software Version Ma 🗸										

(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).

Signature Library 🛃 Select All 2 App Identification Signature Library 🛃 Virus Protection Signature Library (Deep Scan) 2 URL Signature Library 😨 Behavior Analysis Signature Library Save	Virus Protection Signature Library (Quick Scan) Intrusion Prevention Signature Library	ISP Address Library Threat Intelligence Signature Library
Signature Library Type		
O Upgrade All Upgrade all signature libraries online simultaneously.)		
App Identification Signature Library	Virus Protection Signature Library (Deep Scan)	Virus Protection Signature Library (Quick Scan)
Current Version:2030/105.1446 Last Upgrade Time/2024-01-11 Last Version:Utable to obtain the latest version. Version State:- Activation States-Activated	Current Vernion-2024/9102.0522 Last Upgrode Time-2024-91-02.155.09 Lastert Vernion/Inuble to batist the latest version. Version States- Advadion States-Advated	Current Version 2023/1219.1034 Last Upgrade Time2022-12-12 1156:14 Laster Version:Unable to obtain the latest version. Version States. Activation States.
Online Upgrade Local Upgrade Rolling back	Online Upgrade Local Upgrade	Online Upgrade Local Upgrade
Intrusion Prevention Signature Library	ISP Address Library	Threat Intelligence Signature Library
Current Version:2023/12/2.1655 Last Upgrade Time.2023-12.19 18:55:18 Lastart Version:Indulate to obtain the latest version. Version State:- Activation StateActivated	Gurrent Version:20221202 1005 Last Upgende Time- Lastest Version/Loste to obtain the latest version. Version State-	Current Version:202312/19.0716 Last Upginde Time2023-12-19 18-52-22 Lastert Version/Unable to obtain the latest version. Version State-Activated
Online Upgrade Local Upgrade Rolling back	Online Upgrade Local Upgrade	Online Upgrade Local Upgrade
URL Signature Library Connet Version:20231107.1551 Last Upgrade Time:2023-12-19 1851:06 Last Version State. Activation State Activated	Behavior Analysis Signature Library Corrent Venime-202312210001 Last Upgrade Time- Latest VenioncUnable to obtain the latest venion. Venion State-	
Online Upgrade Local Upgrade	Online Upgrade Local Upgrade	

• Online upgrade

Note

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

Signature Library (2) Selet All . 2) Appl Gerhaftano Signature Library (Deep Scan) 2) URL Signature Library (2) Behavior Analysis Signature Library Save	Virus Protection Signature Library (Quick Scan) Intrusion Prevention Signature Library	SP Address Library
Signature Library Type © Upprate Al Upprede all signature libraries online simultaneously.)		
App Identification Signature Library Current Venion/2004/196.5446 Last Upgravels Time/2024-0F-11 560.51 Last Venion/Losted to etailar the laster venion.	Virus Protection Signature Library (Deep Scan) Current Venion/2020/010.0522 Last Upgowale Time/2020-01-01 94:51:09 Laster Verion/Christie Loteisin de laster venion.	Virus Protection Signature Library (Quick Scan) Current Venion/2021/13/5154 Last Upgroufs Time/2023-12/515514 Last Venion/Links to tablin the last venion.
Venion State-Antonio Activities State-Antonio Online Signatio Local Upgrade Rolling Insta	Version State- Activation ShateActivated	Venion State-Artivitient Artivition State-Artivitient Online Stoprastic Local Liggrandi
Intrusion Prevention Signature Library Current Venion/2021/212.5655	15P Address Library Current Venion/2022/202.1005	Threat Intelligence Signature Library Current Venion/202112190716
Las Upprafe Time/222-12-19 155:16 Laster Venico-Duble to obtain the latest venico. Venico Statu- Activation Tatal-Activated	Last Upgende Time- Laster Version Unable to obtain the latest version. Version State-	Last Upprofile Time2023-17-19 15:52-22 Laster VenicionChable to obtain the latest venicion. Venicion Statute Activation Statute-Activated
Online Upprado Local Upprado Rolling Iaux	Colone Liggrade Local Liggrade Behavior Analysis Signature Library	Chilles Upgrade Local Upgrade
Current Wasion20231107.551 Last Upprade Time2023-T2-19-1851.06 Last Wision Unable to obtain the Intest vension. Vension State: Activation State/Activated	Current Wenion-20231221.0001 Last Upprode Time- Lathest Venion:Challe to obtain the latest sension. Venion State-	
Online Upgrade Local Upgrade	Online Upgrade	

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.
 - 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 > Intrusion Prevention Signature Library, find the applicable version, and click Download in the Operation column to download the version file to the local device.

Ruíjie scp	A Home	Security Operations Dev	ice Operations () Aut	norization Management	Device Management	BB Version Mana	gement () System	n Management		
Signature Library Ve	Product	Type Select a type.	Model Select a mo	idel. 🗸 Softwa	re Version all	Ver	sion Number Select	versionNumber 🗸	Query Reset	
App Identification Signatu	Troduct	The constants.	HOUSE CONSCIENCE	Join - Joint -		. 10			(dob)	
Behavior Analysis Signat	No.	File Name	Version Number	Version Description	Model	Software Version	releaseTime	File Size (MB)	MD5	Operation
Intrusion Prevention Sign	1	ips_full_sign_v20240102.1135.zip	20240102.1135	The upgrade package	Universal	>=R5	2024-01-02	1.22MB	f1f09476a32a3b9	👱 Download
Virus Protection Signatur	2	ips_full_sign_v20231229.1416.zip	20231229.1416	The upgrade package	Universal	>=R5	2023-12-29	1.22MB	c4d65f56e13147	\pm Download
Virus Protection Signatur	3	ips_full_sign_v20231219.1502.zip	20231219.1502	The upgrade package	Universal	>=R5	2023-12-19	1.21MB	f9b877063ba919	± Download
URL Signature Library	4	ips_full_sign_v20231212.1655.zip	20231212.1655	The upgrade package	Universal	>=R5	2023-12-12	1.20MB	a0ff1294a2d1db6	± Download
Software Version Ma V	5	ips_full_sign_v20231205.1629.zip	20231205.1629	The upgrade package	Universal	>=R5	2023-12-05	1.19MB	3a14d248815328	± Download
	6	ips_full_sign_v20231128.1702.zip	20231128.1702	The upgrade package	Universal	>=R5	2023-11-28	1.18MB	f0fca5be08ebe12	\pm Download
	7	ips_full_sign_v20231114.1631.zip	20231114.1631	The upgrade package	Universal	>=R5	2023-11-15	1.16MB	6a3fd5b30eafd3f	\pm Download
	8	ips_full_sign_v20231107.1530.zip	20231107.1530	The upgrade package	Universal	>=R5	2023-11-08	1.15MB	b7124756488c6e	± Download
	9	ips_full_sign_v20231031.1507.zip	20231031.1507	The upgrade package	Universal	NGFW_NTOS 1	2023-10-31	1.14MB	2669e1670e6964	± Download
	10	ips_full_sign_v20231024.1404.zip	20231024.1404	The upgrade package	Universal	NGFW_NTOS 1	2023-10-24	1.13MB	480dfc4210a83b	\pm Download

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

e Auto Upgrade le Time:Daily 16 v Hour 22 v Minute				
re Library: 2 Select All App Identification Signature Library Threat Intelligence Signature Library 2 URL Signature Library	ire Library (Deep Scan) 🛛 Virus Protection Signature Library (Quick Scan) 🖉 Behavior Analysis Signature Library	Intrusion Prevention Signature Library 🧧 ISP Address Library		
ture Library Type ograde All (Upgrade all signature libraries online simultaneously.)				
Identification Signature Library	Virus Protection Signature Library (Deep Scan)	Virus Protection Signature Library (Quick Scan)		
ent Version:20231222.1615	Current Version:-	Current Version:20230619.0232		
Upgrade Time:-	Last Upgrade Time:-	Last Upgrade Time:-		
t Version:Unable to obtain the latest version. No SN record is found.	Latest Version:Unable to obtain the latest version. No SN record is found.	Latest Version:Unable to obtain the latest version. No SN record is found.		
on State:-	Version State: The deep scan function is not enabled, and the virus protection	Version State:-		
ation State:Not Activated	signature library for deep scan is not loaded Activation State:Not Activated	Activation State:Not Activated		
nline Upgrade Local Upgrade Rolling back	Online Upgrade Local Upgrade	Online Upgrade Local Upgrade		
usion Prevention Signature Library	ISP Address Library	Threat Intelligence Signature Library		
ent Version:20231212.1655	Current Version:20221202.1005	Current Version:-		
Jpgrade Time:2023-12-28 18:47:25	Last Upgrade Time:-	Last Upgrade Time:2024-01-05 17:39:36		
	Latest Version:Unable to obtain the latest version. No SN record is found.	Latest Version:Unable to obtain the latest version. No SN record is found.		
t Version:Unable to obtain the latest version. No SN record is found.	Version State:-	Version State:-		
t Version:Unable to obtain the latest version. No SN record is found. on State:-	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 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		
	brary (Deep Scan) 👩 Virus Protection Signature Library (Quick Scan) 👩 Behavior Analysis Signature Library	Intrusion Prevention Signature Library 👩 ISP Address Library
App Identification Signature Library Current Version:20231222.1015 Last Upprade Time- Lasts 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- Laste Version State The See Scan Auction is not enabled, and the virus protection upgrature 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- Lates Version:Unable to obtain the latest version. No SN record is found. Version State: Activation State:Not Activated
Intrusion Prevention Signature Library Current Version 20231212.1655 Last Upgrade Time 2023-12-28 1047-25 Latest Version Unable to obtain the latest version. No SN record is found. Version State- Activation State Not Activated Continue Upgrade Local Upgrade Rolling back	ISP Address Library Current Venion.20221202.1005 Latel Upgrade Time- Latel Venion: Unable to obtain the latest venion. No SN record is found. Version State-	Threat Intelligence Signature Library Current Version- Last Upgrado Time 2024-01-05 17:85:86 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.

Ruíjie scp	Home	Security Operations	vice Operations () Aut	horization Management	🖵 Device Management	BB Version Mana	igement (i) Syste	m Management		
Signature Library Ve	Product 1	Type Select a type.	Model Select a mo	odel. v Softwa	re Version all	Ve	rsion Number Select	t versionNumber 🔍	Query Reset	
Behavior Analysis Signat	No.	File Name	Version Number	Version Description	Model	Software Version	releaseTime	File Size (MB)	MD5	Operation
Intrusion Prevention Sign	1	bash_20240112.1530_full_sig.a	cij 20240112.1530	hash_20240112.1530	Z3200-S	Universal	2024-01-12	8.91MB	6160b9a7e62ae3	± Download
Virus Protection Signatur	2	100 hash_20240112.0403_full_sig.	elj 20240112.0403	hash_20240112.0403	Z8620,Z8680	Universal	2024-01-12	76.35MB	82cf6841b4c0d8	± Download
Virus Protection Signatur	3	100 hash_20240112.0316_full_sig.a	cij 20240112.0316	hash_20240112.0316	Z3200-S	Universal	2024-01-12	8.98MB	c50814494865e3	业 Download
URL Signature Library	4	Mash_20240111.1502_full_sig.a	ij 20240111.1502	hash_20240111.1502	Z3200-S	Universal	2024-01-11	8.93MB	5f2e30c0370fa51	± Download
Software Version Ma ~	5	hash_20240111.1403_full_sig.a	ij 20240111.1403	hash_20240111.1403	Z8620,Z8680	Universal	2024-01-11	76.43MB	ccbd8d2f7c54e0	± Download
	6	Mash_20240111.0254_full_sig.a	ij 20240111.0254	hash_20240111.0254	Z3200-S	Universal	2024-01-11	9.04MB	0e51827fe8f4ada	± Download
	7	Mash_20240111.0003_full_sig.z	ij 20240111.0003	hash_20240111.0003	Z8620,Z8680	Universal	2024-01-11	76.40MB	271deb7bc1ab35	± Download
	8	🔝 hash_20240110.1440_full_sig.a	zij 20240110.1440	hash_20240110.1440	Z3200-S	Universal	2024-01-10	9.11MB	b4af4a92e93351	± Download
	9	1 hash_20240110.1003_full_sig	nj 20240110.1003	hash_20240110.1003	Z8620,Z8680	Universal	2024-01-10	76.45MB	6e749203a7ed2ff	± Download
	10	600 hash_20240110.0234_full_sig.a	tij 20240110.0234	hash_20240110.0234	Z3200-S	Universal	2024-01-10	9.10MB	cf2926f73bf6dc3	± 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		
Oupgrade All (Upgrade all signature libraries online simultaneously.)		
App Identification Signature Library	Virus Protection Signature Library (Deep Scan)	Virus Protection Signature Library (Quick Scan)
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	Current Version- Last Upgnde 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:Net Activated Online Upgrade Local Upgrade	Current Version:20230019.0232 Last Upgrade Time- Latest Version:Unable to obtain the latest version. No SN record is found. Version State: Activation State: Online Upgrade Local Upgrade
Intrusion Prevention Signature Library	ISP Address Library	Threat Intelligence Signature Library .
Current Version:20231212:1655 Last Upgrade Time:2023-12:2618:47:25 Latest Version:Unable to obtain the latest version. No SN record is found. Version State: Activation State: Not Activated	Current Version:20221202.1005 Last Upgrade Time- Latest Version:Unable to obtain the latest version. No SN record is found. Version State-	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 Rolling back	Online Upgrade Local Upgrade	Online Upgrade Local Upgrade
URL Signature Library	Behavior Analysis 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	Current Version:20231221.0001 Last Upgrade Time- Latest Version:Unable to obtain the latest version. No SN record is found. Version State-	

• Online upgrade

1 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.

gnature Library Upgrade nable Auto Upgrade		
pgrade Time:Daily 16 ~ Hour 22 ~ Minute gnature Library: Select All App Identification Signature Library 2 Virus Protection Signatur		Intrusion Prevention Signature Library IsP Address Library
Threat Intelligence Signature Library URL Signature Library Save	Behavior Analysis Signature Library	
ignature Library Type		
ignature Library Type O Upgrado All Upgrade all signature libraries online simultaneously) App Identification Signature Library	Virus Protection Signature Library (Deep Scan)	Virus Protection Signature Library (Quick Scan)
© 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:The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded	Virus Protection Signature Library (Quick Scan) Current Version:20230619.0232 Latt Upgrade Time- Latest Version:Unable to obtain the latest version. No SN record is found. Version State- Arthonicon State-Ved Activated

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).
 - 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 (Deep Scan), find the applicable version, and click Download in the Operation column to download the version file to the local device.

Ruijie scp	A Home	Security Operations	ice Operations 🕕 Aut	norization Management	Device Management	25 Version Mana	gement (i) System	m Management		
Signature Library Ve	Product 1	Type Select a type.	Model Select a mo	odel. v Softwar	e Version all	√ Ver	sion Number Select	versionNumber 🗸	Query Reset	
Behavior Analysis Signat	No.	File Name	Version Number	Version Description	Model	Software Version	releaseTime	File Size (MB)	MD5	Operation
Intrusion Prevention Sign	1	600 sdk_20240112.1119_full_sig.zip	20240112.1119	sdk_20240112.1119_f	Z8620,Z8680	Universal	2024-01-12	278.12MB	bc063dbcb4d7eb	± Download
Virus Protection Signatur	2	Sdk_20240112.1051_full_sig.zip	20240112.1051	sdk_20240111.2220_full_sig.zip	Z3200-S	Universal	2024-01-12	36.86MB	8061d97a695f60	± Download
Virus Protection Signatur	3	100 sdk_20240111.2220_full_sig.zip	20240111.2220	sdk_20240111.2220_f	Z8620,Z8680	Universal	2024-01-11	277.93MB	2d7edb00b5645b	业 Download
URL Signature Library	4	tu) sdk_20240111.2234_full_sig.zip	20240111.2234	sdk_20240111.2234_f	Z3200-S	Universal	2024-01-11	36.83MB	820e1390ba2d17	± Download
Software Version Ma	5	Msdk_20240111.1000_full_sig.zip	20240111.1000	sdk_20240111.1000_f	Z3200-S	Universal	2024-01-11	36.81MB	50983d9e6e7e35	± Download
	6	600 sdk_20240111.0945_full_sig.zip	20240111.0945	sdk_20240111.0945_f	Z8620,Z8680	Universal	2024-01-11	277.83MB	330b0ec1098e6a	± Download
	7	600 sdk_20240110.2142_full_sig.zip	20240110.2142	sdk_20240110.2142_f	Z3200-S	Universal	2024-01-10	36.80MB	b523cc4613f292	± Download
	8	🔟 sdk_20240110.2109_full_sig.zip	20240110.2109	sdk_20240110.2109_f	Z8620,Z8680	Universal	2024-01-10	277.64MB	613b7fc0226e7f0	± Download
	9	Comparent state in the second state of the sec	20240110.0928	sdk_20240110.0928_f	Z3200-S	Universal	2024-01-10	36.78MB	b26bd7ab9867d5	± Download
	10	msdk_20240110.0822_full_sig.zip	20240110.0822	sdk_20240110.0822_f	Z8620,Z8680	Universal	2024-01-10	277.46MB	4094c3e93a6082	业 Download

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

Signature Library Type O Upgrade All (Upgrade all signature libraries online simultaneously.)		
App Identification Signature Library	Virus Protection Signature Library (Deep Scan)	Virus Protection Signature Library (Quick Scan)
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	Current Version: Latt Upgrade Time: Latest Version:Unable to obtain the latest version. No SM record is found. Version Statc:The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded Activation State Net Activate Online Upgrade	Current Version:20230619.0232 Last Upgnade Time - Latest Version:Unable to obtain the latest version. No 5N record is found. Version State - Activation State - Not Activated Online Upgrade Local Upgrade
Intrusion Prevention Signature Library	ISP Address Library	Threat Intelligence Signature Library
Current Version-2023/12/2.1655 Last Upgrade Time-2023-12-28 1847-25 Lastet Version/Unable to obtain the latest version. No SN record is found. Version State. Activation State.Not Activated Online Upgrade Local Upgrade Rolling back	Current Version 20221 202 1005 Last Upgrade Time- Latest Version: Unable to obtain the latest version. No SN record is found. Version State- Online Upgrade Local Upgrade	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	Behavior Analysis Signature Library	
Current Version:-	Current Version:20231221.0001	

Online upgrade

1 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		
O Upgrade All (Upgrade all signature libraries online simultaneously.)		
App Identification Signature Library	Virus Protection Signature Library (Deep Scan)	Virus Protection Signature Library (Quick Scan)
Current Version:20231222.1615 Last Upgrade Time- Latest Version/Mable to obtain the latest version. No SN record is found. Version State- Activation States Tot Activated Online Upgrade Local Upgrade Rolling back	Current Version: Last Upgrade Time: Latest Version Xhale 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 leaded Activation State: Not Activated Online Upgrade Local Upgrade	Current Version:20220615.0232 Last Uggrade Time:- Latest Version:Unable to obtain the latest version. No SN record is found. Version State:- Activation State:- Activation State:- Decial Upgrade
Intrusion Prevention Signature Library	ISP Address Library	Threat Intelligence Signature Library
Current Version:20231212.1695 Last Upgrade Time:2023-1-228-18:47:25 Latest Version:Unable to obtain the latest version. No SN record is found. Version State: Activation State:Not Activated	Current Version:202212021005 Last Upgrade Time- Latest Version:Unable to obtain the latest version. No SN record is found. Version State-	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 Rolling back	Online Upgrade Local Upgrade	Online Upgrade Local Upgrade
URL Signature Library	Behavior Analysis Signature Library	
Current Version Last Upgrade Time 2024-01-04 04-25:17 Latest Version:Unable to obtain the latest version. No SN record is found. Version State-Not Activated	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.
 - 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 > URL Signature Library, find the applicable version, and click Download in the Operation column to download the version file to the local device.

Ruijie scp	A Home	Security Operations	wice Operations	orization Management	Device Management	盟 Version Mana	igement () Sy	stem Management		
Signature Library Ve A	Product T	ype Select a type.	Model Select a mo	del. v Softwar	e Version all	√ Ve	rsion Number Se	lect versionNumber 🗸 🗸	Query Reset	
Behavior Analysis Signat	No.	File Name	Version Number	Version Description	Model	Software Version	releaseTime	File Size (MB)	MD5	Operation
Intrusion Prevention Sign	1	600 url_db_i_full_20240102.0943.2	ip 20240102.0943	20240102.0943	Z3200-S	Universal	2024-01-02	7.49MB	54c55f531190a6	± Download
Virus Protection Signatur	2	url_db_i_full_20231107.1551.2	ip 20231107.1551	20231107.1551	Z3200-S	Universal	2023-11-07	7.49MB	59b58ed7275f66	± Download
Virus Protection Signatur	3	wl_db_i_full_20231010.1136.2	ip 20231010.1136	20231010.1136	Z3200-S	Universal	2023-10-10	7.49MB	0e5fbcbc03d5d7	± Download
URL Signature Library	4	wurl_db_i_full_20230901.0858.2	ip 20230901.0858	20230901.0858	Z3200-S	Universal	2023-08-31	6.39MB	c2dc63602e7dffe	± Download
Threat Intelligence Signat Software Version Ma v										

(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.

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

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	Virus Protection Signature Library (Deep Scan)	Virus Protection Signature Library (Quick Scan)
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	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 leaded Activation StateNot Activated Online Upgrade Local Upgrade	Current Version:20230619/0232 Last Upgrade Times- Latest Version Unable to obtain the latest version. No SN record is found. Version State Not Activated Online Upgrade Local Upgrade
Intrusion Prevention Signature Library Current Version.2023.122.1565 Last Upgrade Time.2023.12.2.8 18:47.25 Laster Version:Chable to obtain the latest version. No 5N record is found. Version State. Activation State. Colline Upgrade Local Upgrade Rolling back	ISP Address Library Current Venion:202212021005 Last Upgrade 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 Lastu Version-Unable to obtain the latest version. No 5N record is found. Version State- Activation State-Not Activated Online Upgrade Local Upgrade
URL Signature Library Current Version: Latt Upgrads Time 2024-01-04 04-29:17 Lattst Virsionichable to obtain the latest version. No 5N record is found. Version State- Activation State Net Activated Local Upgrade Local Upgrade	Behavior Analysis Signature Library Current Vension:20231221:0001 Last Upgrate Time: Last Vension State: Online Upgrate 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.

App interfection Signatu Behavior Analysis Signat No. File Name Version Number Version Description Model Software Version release Time File Size (MB) MC Interview Prevention Sign 1 1_0_3_28240112.0366_htt[sig.zip 20240112.0366 tl_0_3_20240112.0366 Universal Universal 2024-01-12 6.36MB 7db	
Intrusion Resention Sign 1 (j.03_20240112.0356_ful_sig.zip 20240112.0356 (j.03_20240112.0356 Universal Universal Universal 2024-01-12 6.36MB 7d	Query Reset
	05 Operation
Visus Protection Sgratur 2 6_03_20240111.1356_full_sig.zip 20240111.1356 6_03_20240111.1356 Universal Universal 202401-11 6.33MB 2d	5e3f5dbd345d 👱 Download
	1097a27b6743 👱 Download
Vivue Protection Signatur 3 II_03_20240110.2356_full_aig.zip 20240110.2356 II_03_20240110.2356 Universal Universal 2024-01-10 6.32MB 138	2d3bfc2f177d 👱 Download
	edc3a96e0d9a 👱 Download
Thread Intelligence: Signal 5 If _03_20240109 1956_ full_sig.zip 20240109 1956 If _03_20240109 1956 Universal Universal 2024-01-09 6.31MB 5fa Software Version Ma. v <t< th=""><th>ibf5a32c24958 👱 Download</th></t<>	ibf5a32c24958 👱 Download
	b15c49d7cc2 👱 Download
7 6_03_20240108.1156_full_sig.zip 20240108.1156 6_03_20240108.1156 Universal Universal 2024-01-08 6.31MB 170	cca6af100e8fb 👱 Download
8 ff_03_20240107.2156_full_sig.zip 20240107.2156 ff_03_20240107.2156 Universal Universal 2024-01-07 6.32M8 260	7467d83e2fb5 👱 Download
9 tf_03_20240107.0756_full_sig.zip 20240107.0756 tf_013_20240107.0756 Universal Universal 2024-01-07 6.35MB 720	7a43916ea78f 👱 Download
10 ti_03_20240106.1756_full_sig.zip 20240106.1756 ti_03_20240106.1756 Universal Universal 2024.01-06 6.33MB tb2	tdd00643c9db 👱 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.

iignature Library Type ⓒ Upgrade All (Upgrade all signature libraries online simultaneously.)		
App Identification Signature Library	Virus Protection Signature Library (Deep Scan)	Virus Protection Signature Library (Quick Scan)
Current Version:20231222.1615	Current Version:-	Current Version:20230619.0232
Last Upgrade Time:-	Last Upgrade Time:-	Last Upgrade Time:-
Latest Version:Unable to obtain the latest version. No SN record is found. Version State:-	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	Latest Version:Unable to obtain the latest version. No SN record is found.
version State:- Activation State:Not Activated	Version state: ine deep scan tunction is not enabled, and the virus protection signature library for deep scan is not loaded Activation State Not Activated	Version state- Activation State:Not Activated
Online Upgrade Local Upgrade Rolling back	Online Upgrade Local Upgrade	Online Upgrade Local Upgrade
Intrusion Prevention Signature Library	ISP Address Library	Threat Intelligence Signature Library
Current Version:20231212.1655	Current Version:20221202 1005	Current Version:-
Last Upgrade Time:2023-12-28 18:47:25	Last Upgrade Time:-	Last Upgrade Time:2024-01-05 17:39:36
Latest Version:Unable to obtain the latest version. No SN record is found.	Latest Version:Unable to obtain the latest version. No SN record is found.	Latest Version:Unable to obtain the latest version. No SN record is found.
Version State:-	Version State:-	Version State:-
Activation State:Not Activated		Activation State:Not Activated
Online Upgrade Local Upgrade Rolling back	Online Upgrade Local Upgrade	Online Upgrade

• Online upgrade

1 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.

p Identification Signature Library	Virus Protection Signature Library (Deep Scan)	Virus Protection Signature Library (Quick Scan)
rrent Version:20231222.1615	Current Version:-	Current Version:20230619.0232
t Upgrade Time:-	Last Upgrade Time:-	Last Upgrade Time:-
est Version:Unable to obtain the latest version. No SN record is found.	Latest Version:Unable to obtain the latest version. No SN record is found.	Latest Version:Unable to obtain the latest version. No SN record is found.
sion State:-	Version State: The deep scan function is not enabled, and the virus protection	Version State:-
ivation State:Not Activated	signature library for deep scan is not loaded	Activation State:Not Activated
	Activation State:Not Activated	
Online Upgrade Local Upgrade Rolling back	Online Upgrade Local Upgrade	Online Upgrade Local Upgrade
rusion Prevention Signature Library	ISP Address Library	Threat Intelligence Signature Library
rent Version:20231212 1655	Current Version:20221202.1005	Current Version-
Upgrade Time:2023-12-28 18:47:25	Last Upgrade Time:-	Last Upgrade Time:2024-01-05 17:39:36
est Version:Unable to obtain the latest version. No SN record is found.	Latest Version:Unable to obtain the latest version. No SN record is found.	Latest Version:Unable to obtain the latest version. No SN record is found.
sion State:-	Version State:-	Version State:-
ivation State:Not Activated		Activation State Not Activated

9. System Upgrade

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

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.

Ruijie scp	A Home	Security Operations	Device Operations	 Authorization Management 	Device Manageme	B Version Mana	gement 💿 :	System Management			_ 0 1****@qq.
Signature Library Ve 🗸	Product	Type Select a type. V	Model Sele	ct a model. V Software	Version all	 Version Nun 	nber Select ver	sionNumber 🗸	Query Reset		
Version Info	O Pi	ease select the software version t	hat is supported for upgrade by	ased on "Supported Software Version	s." Upgrading to other version	may result in a failure.					×
Patch Info	No.	File Name	Version Number	Version Description	eleaseTime Fi	e Size (MB) MDS	ō	Model	Software Version	Hardware Version	Operation
	1	NGFW_NTOS1.0R6P1_Z3	NGFW_NTOS 1.0R6P1	2	023-10-09 15	4.71MB df11	c9e1c8de2fd	Z3200-S	Universal	1.00;1.01	
	2	V5.2-NGFW_NTOS1.0R5_	NGFW_NTOS 1.0R5	2	023-06-16 15	4.64MB 573	6531783d0fb	Z3200-S	Universal	1.00;1.01;1.02;1.03	

(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.

Ruíjie Z Series Firewall	습 Home 🛛 Monitor	ork A≞ Object	Policy 🧿	System				🖗 Network Discovery	🔕 Network Mgmt	1 Quick Onboarding	Policy Wizard
🔏 Admin >	System Upgrade										
♦ System Config >											1
Fault Diagnosis >					m at https://secloud or refresh this page d					nload the latest	
Cloud Management Platform	Note: The file	name cannot contai	in any Chinese or f	ull-width characte	r. Before the upgrad	e, verify that the targ	get version matches	the device model.			
🗒 Signature Library Upgrade	Version Info										
🛞 System Maintenance 🛛 🗸	Current Version N	FW_NTOS 1.0R5, Re	elease(03151320)								
Device Info	Version Rollback Yo	can roll back toNG	FW_NTOS 1.0R4, F	elease(03151401)	1						
Device Positioning		ersion Rollback									
Config Backup	Online Upgrade										
System Upgrade	Recommended Version Fa	ed to connect to th	e server or obtain	the version.							
Restart	Local Upgrade										
Defaults Restoration											
		wnload Link:https://	-	_		1					
	Import	elect an upgrade fi	le.	Browse	Upgrade Now						
						,					

• Online upgrade

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.

Home 🛛 Monitor 🌐 N	letwork A≞ Object	Policy 🕲 Syst	m	Network Discovery	🔕 Network Mgmt	Quick Onboarding	Policy Wizard	Customer Service	Q admin
System Upgrade									
							1		
			. men, periorni are apgrade iota	any. Do not close of ren	con ano page da	ing the upgrade			
Note: The f	ile name cannot contai	n any Chinese or full-	idth character. Before the upgrade	e, verify that the target	version matches	the device model.			
Version Info									
Current Version	NGFW_NTOS 1.0R5, Re	lease(03151320)							
Version Rollback	You can roll back toNG	FW_NTOS 1.0R4, Rele	se(03151401)						
	Version Rollback								
Online Upgrade									
Personmended Version	Called to connect to th	a conver or obtain the	asten						
Recommended version	railed to connect to th	e server or obtain the	ersion.						
Local Upgrade									
Download	Download Link:https://	secloud1.ruijie.com.cr							
Import	Select an upgrade fi	e.	Browse Upgrade Now						
	System Upgrade Version pag process. Off Note: The f Version Info Current Version Version Rollback Online Upgrade Recommended Version Local Upgrade Download	System Upgrade (1) You can perform an upgrade onlin Wersion page and download the la process. Otherwise, the upgrade on Note: The file name cannot contal Version Info Current Version NGFW_NTOS 1.0RS, Re Version Rollback You can roll back to NG Wersion Rollback Online Upgrade Recommended Version Failed to connect to the Local Upgrade Download Download Linichttps://	System Upgrade	System Upgrade	Note: Windford Windford Wetwork Vectory System Upgrade (1) You can perform an upgrade online or visit Ruijie Secure Cloud Platform at http://sectoud1.ruijie.com.cn On the perform the upgrade locally. Do not close or refir process. Otherwise, the upgrade and fail. Note:: The file name cannot contain any Chinese or full-width character. Before the upgrade, verify that the target: Version Info Current Version NGFW_NTOS 1.0R5, Release(03151320) Version Rollback: You can roll back toNGFW_NTOS 1.0R4, Release(03151401) Version Rollback: Vousion Rollback Online Upgrade Recommended Version Local Upgrade Download Link:https://secloud1.ruijie.com.cn	Notifie Image: Stream Viework Prevent Viework Prevent Viework Method M	Notice Windling Windling We have Windling We have Windling Outlike Online windling Stystem Upgrade Image: Stystem Outlike Online windling Outlike Online windlike Onlike Online windlike Online windlike	Notice Image: Strate in the server or obtain the version. Local Upgrade	Notice Image: Worklow Image: Worklo

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.

A Caution

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

		oatch locally to complete the upgrade ny Chinese or full-width character. Be				
Note. The	The name cannot contain a	ny chinese of full-width character, be	tore the upgrade, verify th	at the target version match	es the device mou	ei.
Online Upgrade	(New patches will be installed a	at the specific time point. Some patches do	not support automatic upgrad	le and require manual upgrade.)		
Patch Info Sync	Daily 05 V Hour 37	7 🗸 Minute				
Auto Upgrade	(After this function is er	nabled, new patches that support automatic	c upgrade are automatically ins	talled.)		
Local Upgrade						
	Download Link:https://sec	:loud1.ruijie.com.cn				
		loud1.ruijie.com.cn Browse Upgr	rade			
Download	Download Link:https://sec	· ·	ade			

- 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.

Ruijie scp	A Home Security Op	erations	O Authorization Management	ent 💭 Device Management	28 Version Management	System Management			🤎 1****@
Signature Library Ve 🗸									
Software Version Ma 🔨	Product Type Select a t	ype. V Model Sel	ect a model. V	ware Version all	 Version N 	umber Select versionNumber	Query	Reset	
Version Info	Please select the patch	version that is supported for upgrade bas	ed on "Supported Software Versio	ns." Upgrading to other patch version	s may result in a failure.				
Patch Info	No. File Name	Version Number	Version Description	releaseTime File	Size (MB) MD5	Model	Software Version	Hardware Version	Operation

- 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.

downloa	ad the latest patch file. Then,	or visit Ruijie Secure Cloud Platform at install the patch locally to complete the ne cannot contain any Chinese or full-w	e upgrade. Do not close or	refresh this page	e during the	upgrade proces	s. Otherwise, the
		d at the specific time point. Some patches do i					
Patch Info Syr	nc Daily 05 \vee Hour	37 v Minute					
Auto Upgrad	de 🔹 (After this function is	enabled, new patches that support automatic	upgrade are automatically inst	alled.)			
Local Upgrad	de						
Downloa	ad Download Link:https://se	ecloud1.ruijie.com.cn					
Impo	Select a patch file.	Browse Upgra	ade				
C Refresh							
No.	Patch Name	system.upgradeType	Release Date	Descript ion	Source	Status	Installatio
			No Data				

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:
 - o Manually add the device SN and license code.

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

Ruijie scp	A Home Security Operations	perations () Authorization Management	🖵 Device Management	88 Version Management	System Management			
Authorization Activation	Device Authorization							
	License Activation	License Generation	×					
		Once a license file is generated, the vali	idity period begins. Activate the license	le.				
	License List	Manual Input Batch Import						
	If a submitted license code is not shown in the list Repage	No.1 * Device SN Enter	the device SN		ie T	ype Select a license typ		
	No. License Code	* License Code Enter	the license code.	Add License Code	nse	Validity Period	Activation Time	Operati
		Add Device SN and Authorization Cod	Se internet in the second s					
			Generate License File	Cancel				

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**.

Ruíjie scp	A Home								
Authorization Activation	Device A	uthorization							
		License Activation			ion	2	×		
	License L	ist			file is generated, the validity period s soon as possible.	d begins. Activate the license			
		Download	vn in the list Refresh the	O Manual Input	Batch Import		license 🗸	License Type Select a license	
	. N	No. License Code	License Name	Import Select a fi	e. Browse			License Validity Period	Activation
					Generate License File	Cancel			

- Offline activation
- 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.

Device Authorization	
License Activation	
License List	
± Batch Download	License Name Select license name. V License Status Select a license V License Type Select a license type. V
If a submitted license code is not shown in the list Refresh the page	Enter a device SN or license name
No. License Code License Name Device	N License Status License Type License Validity Period Activation Time Operation
	No Data

(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 <u>3.2.3</u> <u>2. Manual Activation</u>.

Ruijie Z Series Firewall	습 Home	S Monitor	Network	우 Object	Policy	⊕ System		M Network Discovery	🛞 Network Mgmt	1 Quick Onboarding	Policy Wizard	Customer Service	오 admin
Admin →	Author	rization Ma	nagement										
System Config ~ System Time		License Cor	-										
SNMP Service Parameters		 Before activating a device, register on and log in to Rujue Secure Cloud Platform athtps://secures.com.co. On the platform, access the Device Authorization page, and generate a license file. The account of the platform is used are activating and changing device licenses andmatte be kept confidential.) Select an activation mode based on device connection status.For threat intelligence, only online activation is supported. 									nie. The		
Authorization Management			e Online vate Now					You can choose Activate Man		ual activation.			
Cloud Management Platform			MACC93267266	Carry									
Signature Library Upgrade Image: System Maintenance >		License Infe		56 Copy							How to Obtain	Licence	
			nance License								How to Obtain	3G /3G	
		Available Perf	formance:3G(Basic	: Performance:1G	+Added New	Performance:20	 Performance to Be Added: 	ŁOG				30 /36	
				ns25(25 concurre	ent free license	e sessions + 0 cr	oncurrent purchased license sessi	ions)					
		🖨 Security	/ Capability Lice	nse									
		No.	Security Ca	pability Nam	e	D	Description	License T	ype		Status		
		1	App Ident	ification (APP)	ŀ		grade services for app id n signature libraries.	Formal Lic	ense	Activated (E 07)	xpiry Time:202	4-03-	
		2	Intrusion P	revention (IPS)) 11		grade services for IPS sig ture libraries.	Formal Lic	ense	Activated (E 07)	xpiry Time:202	4-03-	

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 <u>3.2.3</u> <u>1. Automatic Activation</u>.

Ruijie Z Series Firewall	Define © Monitor ⊕ Network & Object © Policy O System O
🔏 Admin >	I Authorization Management
🔅 System Config 🛛 🗸 🗸	
System Time	License Config
SNMP	 Before activating a device, repiter on and log in to Ruijie Secure Cloud Platform athtrps://secloud.log/inscience.com.co. On the platform, access the Device Authorization page, and generate a license file. The account of this platform is used for activating and changing device license and and the key confidential.)
Service Parameters	Select an activation mode based on device connection status. For threat intelligence, only online activation is supported.
Authorization Management	Activate Online You can choose to perform manual activation.
	Activate Now Activate Manually
Cloud Management Platform	
🗒 Signature Library Upgrade	Device SN:MACC932672666 Copy
	License Info How to Obtain License
	Performance License
	Available Performance:3G(Basic Performance:1G+Added New Performance:2G) Performance to Be Added:0G 3G/3G
	I SSL VPN License
	Max. Concurrent License Sessions25(25 concurrent free license sessions + 0 concurrent purchased license sessions)

3.2.3 License Activation Methods

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

🛕 Caution

The threat intelligence function supports online 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 (<u>https://secloud1.ruijie.com.cn</u>) and choose Authorization Management > Authorization Activation. On the page that is displayed, click License Activation and generate a license file.

Ruíjie scp	A Horne	Security Operations	Device Operations	0 4	Authorization Management	Device Management	B Version Management	System Management	t	
Authorization Activation	2 Device A	authorization								
			se Activation	se Gene	eration					
			0	Once a licer	nse file is generated, the validity					
	License L		4 💿 Ma	nual Input	 Batch Import 					
	Batch Download If a submitted license code is not sh page		e code is not shown in the list Refr No.1	5	* Device SN Enter the]	ן	e Type Select a license type. ~	
		No. License Code	Lic	L	* License Code Enter the	license code.	Add License Code		nse Validity Period Activation Time	Operati
					7	Generate License File	Cancel			

Procedure

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

				Network Discovery	Network Mgmt	Quick Onboarding	Policy Wizard	Customer Service	admin
Admin > Admin	horization Management								
🚸 System Config 🛛 🗸 🗸									
System Time	License Config								
SNMP	 Before activating a device, register on and log in account of this platform is used for activating and 	n to Ruijie Secure Cloud Platfo changing device licenses and	rm athttps://secloud1.ruijie.com must be kept confidential.)	n.cn. On the platform, ac	cess the Device Aut	thorization page, and	generate a license	file. The	
Service Parameters	2. Select an activation mode based on device con								
Authorization Management	Activate Online			You can choose	to perform mar	ual activation.			
	Activate Now			Activate Man	ually				
Cloud Management Platform									
👹 Signature Library Upgrade	Device SN:MACC932672666 Copy								
System Maintenance >	License Info						How to Obtair	License	
	Performance License								
	Available Performance:3G(Basic Performance:1G+	Added New Performance:2G)	Performance to Be Added:	0G				3G /3G	
	SSL VPN License								
	Max. Concurrent License Sessions25(25 concurren	t free license sessions + 0 cor	current purchased license sessio	ons)					

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 (<u>https://secloud1.ruijie.com.cn</u>) and choose **Authorization Management > Authorization Activation**. On the page that is displayed, click **License Activation**, and generate a license file.

RUIJIE SCP	A Home Security Operations Device C	perations 🛈 Authorization Management 🖓 Device Management 👔 Version Management 🍈 System Management	
Authorization Activation	Device Authorization		
	3 License Activation	License Generation ×	
		Once a license file is generated, the validity period begins. Activate the license on the device as soon as possible.	
	License List	O Manual Input O Batch Import	
	If a submitted license code is not shown in the list Refe page	No.1 5 Enter the device SN	e Type Select a license type. ~ Enter a device SN (
	No. License Code Lie	* License Code Enter the license code.	nse Validity Period Activation Time Operat
		Add Device SN and Authorization Code	
		7 Generate License File Cancel	

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

Generation succeeded.	×
Generation succe A license file is generated. Activate device as soon as possible. (For thre online activation is supp	the licenses on the eat intelligence, only
Download License File	Got It

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	Ianual License Activation Procedure								
1. Obtain Dev	ice Info								
Click Copy to a	obtain the device SN and use it on the cloud platform to generate a license file.								
Device SN: MA	СС93 Сору								
2. Export Lice	nse File								
Authorization	ure Cloud Platform athttps://secloud1.ruijie.com.cnOn the platform, access the Device page, and click Activate License. Then, enter the device SN obtained in step 1 and the license code hased, and export the license file.								
Ruijie Secure	e Cloud Platform								
3. Import Lice	ense File								
Import the lice	ense file obtained in step 2 and click Activate to complete the authorization.								
Upload	Select a license file. Browse Activate								
	Disable								

- (3) Copy the device SN and log in to 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.

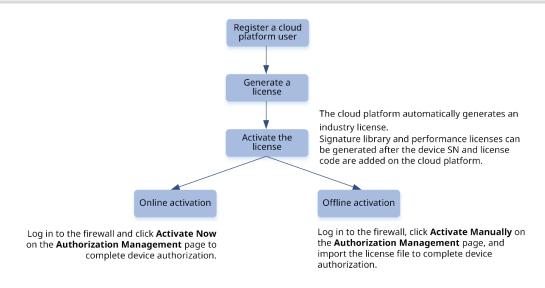
Follow-up Procedure

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 (<u>https://secloud1.ruijie.com.cn</u>) 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.

SYSLOG Server		
	arty log analysis platform for unified storage, analysis, and processing. I, it will occupy bandwidth and affect existing network services. Please o	DHCP logs can be displayed only after a DHCP server is configured and operate with caution.
Fast Syslog Forwarding		
Syslog Server1	Syslog Server2	
 Server IP Enter an IP address. Port 514 Standard Protocol Version rfc3164 trc5424 Logs to Be Sent to Syslog Server System Log Edit Template Session Log Edit Template Gett Template URL Log Edit Template Select a syslog type. 	Create	

ltem	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 SentTypes of logs to be sent to theto Syslog ServerSyslog 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 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.

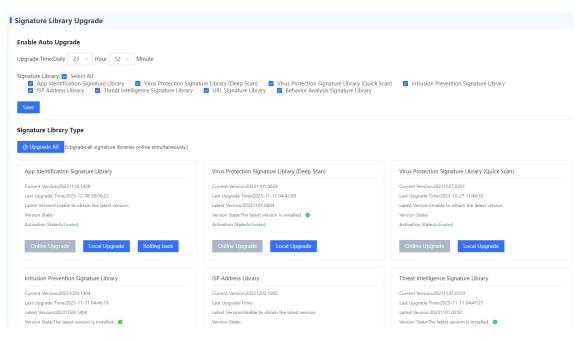
5.1 Configuring Automatic Upgrade

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.



The system displays information about the current signature libraries:

- Last Upgrade Time: displays the last time when a signature library is upgraded.
- Latest Version: displays the latest version information and functions and instructs you to upgrade a signature library.
- (2) In the Enable Auto Upgrade area, configure an automatic upgrade policy for signature libraries.

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

Signature Library Upgrade	
Enable Auto Upgrade	
Upgrade Time:Daily 23 \vee Hour 52 \vee Minute	
Signature Library: 😰 Select All 😰 App Identification Signature Library 😰 Virus Protection Signature Library (Deep Scan) 😰 Virus Protection Signature Library (Quick Scan) 😰 ISP Address Library 😰 Threat Intelligence Signature Library 😰 URL Signature Library 😰 Behavior Analysis Signature Library	Intrusion Prevention Signature Library

a Set the time for automatic upgrade.

You are advised to configure an off-peak period.

- b Select the type of signature library to be upgraded.
- (3) Click Save.

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.

Cuijie 27 Series Firewall	G Monitor System Object Policy OSystem		Network Discovery Network Mgmt Quick Oriboarding Policy Wizard Customer Service admin					
🎭 Admin 💦 🔗	Signature Library Upgrade							
System Config > Fault Diagnosis >	Enable Auto Upgrade							
b Cloud Management Platform	Upgrade Time:Daily 6 v Hour 4 v Minute							
Signature Library Upgrade	Signature Library Select All Zhang App Identification Signature Library Zhang Virus Protection Signature Library (D	Deep Scan) 👩 Virus Protection Signature Library (Quick Scan) 👩 Intrusion Prevention	n Signature Library 🗧 ISP Address Library 🚦 Threat Intelligence Signature Library					
	San							
	Signature Library Type							
	O Upgrade All (Upgrade all signature libraries online simultaneously.)							
	App Identification Signature Library	Virus Protection Signature Library (Deep Scan)	Virus Protection Signature Library (Quick Scan)					
	Current Version:20230217.1245	Current Version-	Current Version:20230309.0218					
	Last Upgrade Time:-	Last Upgrade Time-	Last Upgrade Time:-					
	Latest Version: Unable to obtain the latest version.	Latest Version:Unable to obtain the latest version.	Latest Version.Unable to obtain the latest version.					
	Version State:-	Version State:	Version State:-					
	Activation State:Activated	The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded	Activation State:Activated					
	Online Upgrade Local Upgrade system versionRollback	Online Upgrade de Local Upgrade	Online Upgrade Local Upgrade					
	Intrusion Prevention Signature Library	ISP Address Library	Threat Intelligence Signature Library					
	Current Version:20221026.1141	Current Version:20221202.1005	Current Version:20230308.1608					
	Last Upgrade Time:2023-03-13 11:53:03	Last Upgrade Time:-	Last Upgrade Time:-					
	Latest Version: Unable to obtain the latest version.	Latest Version:Unable to obtain the latest version.	Latest Version:Unable to obtain the latest version.					
	Version State-	Version State-	Version State-					
	Activation State:Activated		Activation State:Expired					
	Online Upgrade Local Upgrade system/versionRollback	Online Upgrade Local Upgrade	Online Upgrade Local 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.

App Identification Signature Library	Virus Protection Signature Library (Deep Scan)
Current Version:20230217.1245	Current Version:-
ast Upgrade Time:-	Last Upgrade Time:-
atest Version:Unable to obtain the latest version.	Latest Version:Unable to obtain the latest version.
/ersion State:-	Version State:
Activation State:Activated	The deep scan function is not enabled, and the virus protection signature library for deep
Online Upgrade Local Upgrade system.versionRollback	Online Upgrade d Local Upgrade
ntrusion Prevention Signature Library	ISP Address Library
Current Version:20221026.1141	Current Version:20221202.1005
.ast Upgrade Time:2023-03-13 11:53:03	Last Upgrade Time:-
atest Version:Unable to obtain the latest version.	Latest Version:Unable to obtain the latest version.
/ersion State:-	Version State:-
Activation State: Activated	

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 U	pgrade							\otimes
page an process	can visit Ruijie Secure Cloud Plat d download the latest upgrade f Otherwise, the upgrade may fai at the target version matches the	ile. Then, perform the I. Note: The file name	upgrade loc	ally. Do not	close or refresh	this page durir	ng the upgrade	
Download	Download Link:https://seclou	d1.ruijie.com.cn						
Import	Select an upgrade file.	Browse						
		Upgrade Now	Disable					

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

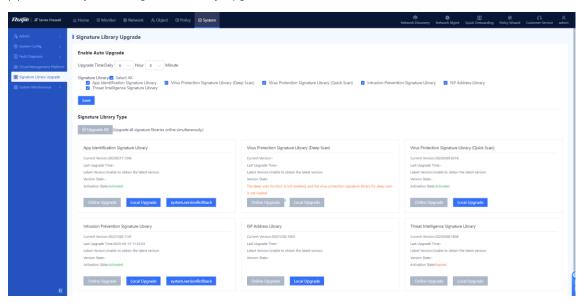
5.3 Online Automatic Upgrade

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.

op Identification Signature Library	Virus Protection Signature Library (Deep Scan)	Virus Protection Signature Library (Quick Scan)
urrent Version:20230217.1245	Current Version:-	Current Version:20230309.0218
ast Upgrade Time:-	Last Upgrade Time:-	Last Upgrade Time-
atest Version: Unable to obtain the latest version.	Latest Version:Unable to obtain the latest version.	Latest Version: Unable to obtain the latest version.
ersion State:-	Version State:	Version State:-
ctivation State:Activated	The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded	Activation State:Activated
Online Upgrade Local Upgrade system.versionRollb	Online Upgrade d Local Upgrade	Online Upgrade Local Upgrade
ntrusion Prevention Signature Library	ISP Address Library	Threat Intelligence Signature Library
urrent Version:20221026.1141	Current Version:20221202.1005	Current Version:20230308.1608
ast Upgrade Time:2023-03-13 11:53:03	Last Upgrade Time:-	Last Upgrade Time:-
atest Version: Unable to obtain the latest version.	Latest Version:Unable to obtain the latest version.	Latest Version: Unable to obtain the latest version.
ersion State:-	Version State:-	Version State:-
ctivation State Activated		Activation State:Expired

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.

Ruffe Z Series Firewall	🛆 Home 🕫 Monitor 🔀 Network Ag Object 😨 Policy 🗿 System 🖉 🎯 🔝 🔗	
🎭 Admin →	I System Upgrade	
♦ System Config >		
	(i) You can perform an upgrade online or visit Ruijie Secure Cloud Platform at https://secloud1.ruijie.com.cn On the platform, access the Software Version page and download the latest system upgrade file. Then, perform the upgrade locally. Do not close or refresh this page during the upgrade process. Otherwise, the upgrade may fail.	
D Cloud Management Platform	Note: The file name cannot contain any Chinese or full-width character. Before the upgrade, verify that the target version matches the device model.	
🗒 Signature Library Upgrade	Version Info	
🗑 System Maintenance 🛛 👻	Current Version V5.2-NGFW_NTOS 1.0R5, Release(03152203)	
Device Info	Versier Bellinet, Versier Konsten VCDV NTOC 1004 Release/03151401	
Device Positioning	Version Rollback You can roll back to NGFW_NTOS 1.0R4, Release(03151401) Version Rollback Version Rollback	
Config Backup		
System Upgrade	Online Upgrade	
Patch Installation	Recommended Version Failed to connect to the server or obtain the version.	
Restart	Local Upgrade	
Defaults Restoration	Download Link:https://secloud1.ruljie.com.cn	
	Import Select an upgrade file. Browse Upgrade Now	

- (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.

Ruijie Z Series Firewall	습 Home 🛛 Monitor 🌐 N	etwork A≞ Object	🗟 Policy	System	Retwork Discovery	⊗ Network Mgmt	€ Quick Onboarding	Ø Policy Wizard	ြ Customer Service	Q admin
Admin →	System Upgrade									
 ☞ Fault Diagnosis → ☞ Cloud Management Platform ☞ Signature Library Upgrade 	the Softwar this page d	e Version page and d iring the upgrade pro le name cannot cont	ownload the lat	test system upgrade e, the upgrade may f	orm at https://secloud1.ruijie file. Then, perform the upgra fail. .ter. Before the upgrade, verif	de locally. Do n	ot close or refresh			
System Maintenance Device Info Device Positioning Config Backup		NGFW_NTOS 1.0R4, F /ou can roll back to N Version Rollback						_		
System Upgrade Patch Installation	Online Upgrade				1					
Restart Defaults Restoration	Recommended Version	V5.2-NGFW_NTOS 1 Upgrade Now	.0R5, Release(0	3152203) Details						
	Local Upgrade	Download Link:https	://secloud1.ruiji	ie.com.cn						
	Import	Select an upgrade	file.	Browse	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.

A 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.

System Upgrade	
access the close or m Note: The	erform an upgrade online or visit Ruijie Secure Cloud Platform at (https://secloud1.ruijie.com.cn On the platform, e Software Version page and download the latest system upgrade file. Then, perform the upgrade locally. Do not efresh this page during the upgrade process. Otherwise, the upgrade may fail. file name cannot contain any Chinese or full-width character. Before the upgrade, verify that the target version he device model.
Version Info	
Current Version	V5.2-NGFW_NTOS 1.0R5, Release(03152203)
Version Rollback	You can roll back to NGFW_NTOS 1.0R4, Release(03170303) Version Rollback
Online Upgrade	
Recommended Version	Failed to connect to the server or obtain the version.
Local Upgrade	
Download	Download Link:https://secloud1.ruijie.com.cn
Import	Select an upgrade file. Browse Upgrade Now

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

System Upgrade		
the platform the upg fail. V Note: T target v Version In Current Versio	form an upgrade online or visit Ruijie Secure Clour n, access the Software Version page and download Version Rollback Do you want to perform version rollback now CK Cancel You can roll back to NGFW_NTOS 1.0R4, Release(0 Version Rollback	d the latest system upgrade file. Then, perform de process. Otherwise, the upgrade may \odot r. Before the upgrade, verify that the ?
Online Upgrade Recommended Version	Failed to connect to the server or obtain the versic	on.
Local Upgrade		

7 Configuration Examples for Typical Scenarios

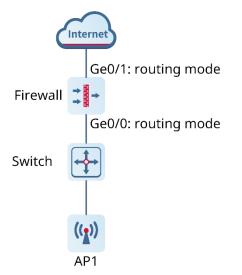
7.1 Integrated Deployment on Ruijie Cloud

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.

Ruffie Z Series Firewall							Netwo	nk Disco	very Network Mgmt	L Quick Onboarding	Policy V		က mer Service	ू admin
1 policies to be optimized 2 traffic exceptions to be handled	Ruffe Z2200-5	0/MGMT	2	3	4	6			e Details>>	32.		40.4% Memory	(1.69 Hard D	

ies Firewall			
① Unmanaged switches are not	displayed in the list. Some device models are not displayed in t	his phase, but will be discovered in the real topology phas	e. For details, see View Model ×
3 devices are discovered in total. Before starting the configuration, verify that the number of devices an	d cable connections are correct. Note: Unmanaged switches are not displa	yed in the list.	
	BXB Internet Firewall	1 1 Switch AP	
New Device (3)			
Device Model	SN	IP	MAC
Z3200-S Local Device	MACCMMMZ32005	192.168.1.200	00:D0:F8:22:36:AF
RAP1200(E)	CANLC2R001601	192.168.1.117	30:0D:9E:0C:1D:E2
NBS5100-48GT4SFP	G1RPAYR001597	192.168.1.162	10:82:3D:14:0B:E1
	Rediscover	Start	

(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.

Fre Z Series Firewall														
① To properly manage the network, create	a project so t	hat you can man	iage dev	ices on ti	he entire	network	c in this j	project.					×	
* Projec	ct Name :	test												
* Admin P	assword:													
Security	Defense:	Intrusion Preve	ention											
	н	Virus Protection Virus Protection Virus Protection Virus Protection Virus Protection Note that the security If the network connection Virus Protection Virus Protectio	license? polícies a	ire enabled	l in the di	rection fro	m LAN to	WAN on	the firewa	dl.	ation page.			
Configure the o	connection @	Electrical 🗆 C	Optical	I 📕 On	📃 Sel	ected	✓ Config	gured						
type of t	the port.:	0/MGMT	1	2	3 100	4	5	6	7	0F	8F			
Intranet li	Interface:	0/MGMT	1	2	3	4	5	6	7	0F	8F			
* LA7	N0/MGMT	192.168.1.200		7	255.2	55.255.0								
DHCP Addr	ress Pool:	192.168.1.1			192.1	58.1.254								

Ruffie Z Series Firewall		
	-	so that you can manage devices on the entire network in this project.
	Configure the connection type of the port.:	n 🗅 Electrical 🗀 Optical I 📕 On 🛄 Selected 🗸 Configured
		0/A/GMT 1 2 3 4 5 6 7 0F 0F
	* WAN Interface (Ge0/1)	O Dynamic (P(DHCP) O PPPoEDial O Static Address
	Advanced Settings	\$ >
	Intranet Interface :	
	* LAN0/MGMT	
	DHCP Address Pool:	192.168.1.1 - 192.168.1.254
	* Time Zone :	(GMT+9:00)Asia/Tokyo v
	* Time Server:	ntp.ntsc.ac.n ntp1.allyun.com
		Create Project and Connect to Network

ltem	Description	Remarks
WAN Interface	 Connects the firewall to the Internet. Generally, the WAN interface is directly connected to the fiber to the home (FTTH) Optical Network Unit (ONU) of the ISP. Three methods are available for a WAN interface to obtain an IP address: Dynamic IP (DHCP): Applicable when no professional network administrator is available. The user terminal automatically obtains an IP address to access the Internet 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 nexthop address must be configured. 	[Example] Ge0/1 Dynamic IP (DHCP)
LAN Interface	Connects to the LAN. The LAN interface IP address must be configured based on the predefined IP address planning.	[Example] 192.168.1.1/24

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

Ruffie Z Series Firewall		
	To properly manage the network, create a project so that you can manage devices on the entire network in this project. X	
	**WAN Interface (GeQ/7) O Dynamic (P(DHCP)) PPPoEDial) Static Address. Advanced Settings >	
	Intranet Interface:	
	* LAN0/MGMT 192.168.1.2 Synchronizing network wide Info DHCP Address Pool: 192.168.1.7 - 192.168.1.254	
	* Time Zone: (GMT+9:00JAda/Tolyo ~	
	* Time Server: ntp.ntsca.cn ntp.lailyun.com	
	Create Project and Connect to Network	

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

🚺 Note

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

ujie Z Series Firewall		Exit
	••••••••••••••••••••••••••••••••••••••	
	Log in Select the project type Prepare for configuration Configure VLANs	
	Please enter your Ruijle Cloud account to log in.	
	Please enter the username.	
	Please enter the password.	
	Login	
	Sign.up	

Note

If the firewall has been bound to the Ruijie Cloud platform, the following dialog box is displayed. Click **Go to Ruijie Cloud for Network Management** to go to the Ruijie Cloud platform and manage the device. Click **Return to EWEB Homepage** to return to the home page of the firewall. (5) After successful login, select a project type based on the actual networking scenario and click **Next**. The initial configuration delivered varies by the project type, so the project type must be set based on the actual service scenario.

∂ Z Series Firewall			
Log in		O Prepare for configuration	
	Pro	ject Type: Office	
Office	Hotel	Villa/Home	Factory/Warehouse
Restaurant	School	Retail/Shop	Residence
Customize			
		Next	

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

Ruffe Z Series Firewa						Exit
		Log in S	Select the project type Prepare f	or configuration Configure VLANs		
	3 devices are ready	y. Verify that the number of device:	s in the project is correct, and th Go to Ruijle CH	en click Go to Ruijie Cloud to proceed wi	th service network configuration	
	Model	SN	MAC	Name 4 Name the device	IP	Progress
Gateway	Firewall:Z3200-S	MACCMMMZ3200S	00D0.F822.36AF	Name	192.168.3.4	Ready
0/0	Switch:NBS5100-48GT4SFP AP:RAP1200(E)	G1RPAYR001597 CANLC2R001601	1082.3d14.0be1 300d.9e0c.1de2	Name	192.168.1.162 192.168.1.117	Ready Ready
Firewall 1/1 Switch 1/1 AP 1/1 A device is missing? Click here.						

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

Ruffe Z Series Firewall	≙ Home	⊕ Network , ዶ_ O	Dbject 🖾 Policy	/ 🕞 Syste	m					n k Discove	ry Network Mgmt	Quick Onboarding Po	Ø licy Wizard Custo		9 Imin
2	policies to be optimized traffic exceptions to be Idled		Ruíjie 23200-5	0/MGMT		2	3	4	6	OF Device	BF Details>>	30.1%) CPU	40.6% Memory	1.6% Hard Disk	

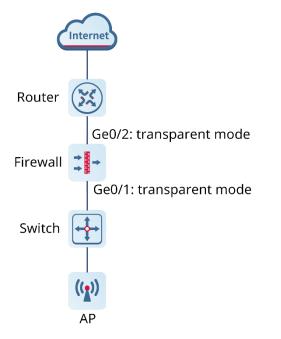
The following figure shows the **Overview** page of the master device.

Ruíjie Rcycc	test > Ruijie (Mantar) O			English	- 🛆 Remote O&M 🔮 Network (Configuration @Netw	ork Check <u>尚</u> Alert	⊡Log Out
옪 Overview	Device Info	Setup>	WI-FI					Setup>
③ Online Clients	Hostname: Ruijie	SN: CANLC2R001601						
⇔ wlan ∨	IP Address: 192.168.1.117 MAC Address: 30:0D:9E0C:1D:E2 RAP1200(E) Software Reveo(S 2.230.00.180	-	Primary Wi-Fi: @Ruijie-m1DE2 Security: No		Guest Wi-Fi: Security: No			
🕮 Firewall	RAP1200(E) Software ReyeeOS 2.230.00.180 Version:	1						
Switches								
🔅 Network	Net Status (Online Devices / Total)	_	_	_			Refresh ©	+ AP
	🥥 ———	Router	Firewall 1	Switch	ি 1/1			
	Internet	Router	Firewall	Switches	APs	Online Clients		
							Click RITA for h	elp.
«Collapse								Aik

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.

Reyce										
	Un-managed switche	s and some models will not be displaye	d in the list but be displayed in the topolo	gy. View More X						
	5 devices are detected. 1 devices should be added manually.									
	Please check the device quantity and cable connection t	before configuration. Note: Un-managed	switch will not be displayed in the list.	⑦ Can't find device?						
	Gateway Gateway -	Firewall 1 Firewall	Switch 1 Switch	1 1 AP Add Manually						
	My Network(4)			i						
	Model	SN	IP	MAC						
	NBR6210-E 1000	MACCHJQ621001	192.168.1.1	00:D1:F8:22:93:59						
	Z3200-S	MACCHJQZ32S31	192.168.1.5	00:d0:f8:22:36:ce						
	RAP2261(G)	G1RU70S000836	192.168.1.2	28.D0.F5.F5.9B.0E						
	NBS3200-48GT4XS-P	G1QH1AD000557	192.168.1.3	C0:88:E6:85:A8:C2						
	Show No.: 10 V Total Count: 4		H First	≪ Pre 1 Next ▶ Last № 1 GO						
	Add Manually									
		Detect again	Slart Config							
		@2000-2023 Ruijie Networks C	o., Ltd Online Service							

(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**.

Rujjie I #Reyee		
Uplink port Port for consecting to gatewary Frewart Downlink port Port for consecting to switch	Firewall Port Config Belect an optimize port Select a downlink port Port for Connecting is lipitham Guldware (splitter Put Geldez)	Destretes Connected Deconnected
	@2000-2023 Ruijie Networks Co., Ltd Online Service	

(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**.

Ruíjie I #Reyce		
Uplink port Port for connecting to gateway Freed Downlink port Port for connecting to switch	Firewall Port Config Select an uplink port Select a downlink port Port for Connecting to Downlinkans Select A downlink port OMGMT 1 2 3 4 5 5 7 0 6 8F (instruction Prevention I instruction Prevention I van Protection After this caption is checked, the LAN is WAN security defense is enabled by default. If the network connection is slow, you can disable security defense on the freewall policy configuration page.	Seacher Connected Disconnected
	@2000-2023 Ruije Networks Co., Ltd Chime Service	

Ruíjie I #Reyee		
Uplink port Por the consecting to gate wy Forward Downlink port Port for consecting to switch	Firewall Port Config The decide in uples and the downline port Port or Connectors is block downline port configuration. Preservat The reference connectors is block, you can deable security defense on the freeval policy configuration page.	Beecker Control Disconacion
	@2000-2023 Ruthe Networks Co., Ltd Online Service	

(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**.

Ruíjie I Reyce	
	Please create a project for the network so that you can manage devices on the project. X
	Project Name: nbr_web
	Management Password
	Odis Odis <td< th=""></td<>
	WAND(GR07): O DHCP O PPPoE O Static IP Address
	LAN Port
	LAN0/MGMIT(GI010): 192.168.1.1 / 255.255.2
	Create Project and Connect to Network
	@2009-2023 Ruije Networks Co., Ltd Online Service

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

Ruíjíe HReyce		Log Out
	Compared to the project type Prepare for configuration Configure VLANs	
	Please enter your Ruijie Cloud account to log in.	
	Please enter the username.	
	Please enter the password.	
	Login	
	Sign.up I have read and agreed to the Privacy Policy.	
	Local Configuration	
	@2000-2023 Ruije Networks Co., Ltd Online Service	-

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

Ruíjie I Reyce				
	•		0	O
	Log in	Select the project type	Prepare for configuration	Configure VLANs
		Proj	ect Type: Office	
	Office	Hotel	Villa/Home	Factory/Warehouse
	Restaurant	School	Retail/Shop	Residence
	Customize			
			_	
			Next	
		Lo	cal Configuration	
		@2000-2023 Ruijie	Networks Co., Ltd Online Service	

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

<i>líjíe</i> I ≢Rey	/cc					Log
		•		••••••		
		Log in	Select the project type Prepare	for configuration Configure VLANs		
	4devicesare ready.	. Verify that the number of device	s in the project is correct, and th	nen click Go to Ruijie Cloud to proceed w	ith service network configuration	on.
			Go to Ruijie Cl	loud		
	Model	SN	MAC	Name 4 Name the device	IP	Progress
Gateway	Gateway:NBR6210-E	MACCHJQ621001	00d1.f822.9359	Name	192.168.2.2	Ready
1/1	Firewall:Z3200-S	MACCHUQZ32531	00d0.f822.36cd	Name	192.168.1.5	Ready
	Switch:NBS3200-48GT4XS-P	G1QH1AD000557	c0b8.e6b5.a8c2	Name	192.168.1.3	Ready
Firewall 1/1 Switch 1/1 AP 1/1 device is issing? Click ere.	AP9A7221(d)	G19U705000836	2860/555.9kGe	Sterin.	192.168.1.2	Ready
			Local Configura	ition		
			@2000-2023 Ruijie Networks Co., I	Ltd Online Service		



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.

Product Cookbook

Policy ~									THE CHECK C	iscovery Network N	ngmit Quick C	noonong		69 Simulation Space
Config Wizard	Security Policy													ey sinulation space
ity Policy	Policy Group	≡	 Creat 	e 🛅 D	Oelete 🕝 Enat	ble 🚫 D	isable 😋 Refresh	More ~		Type All		~ Ente	r a keyword.	
Optimization	Add Policy	Group		Priority	Name	Туре	Src Security Zone	Src Address	Dest. Security Zone	Dest Address	Service	App	Tir	Operation
Life Cycle	Keyword					type	Sic. Security Lone	Sic. Address	Desc Security Lone	Dest. Address	Service	044		operation
an	All Groups	^	✓ Deta	ult Policy	Group									
earning	图 (2) Default			1	allow_trus	-	trust	any	untrust	any	any	any		Edit Delete
licy >					Default Po									
/ Defense >				2	Default Po	-	any	any	any	any	any	any		
t and Allowlist														
xy >														

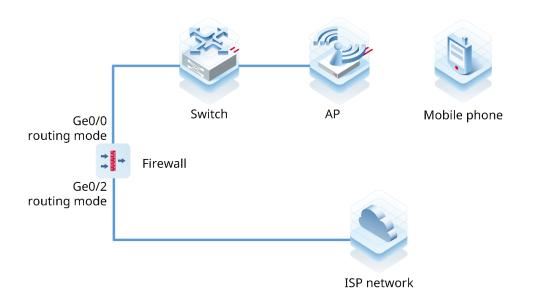
7.1.3 Deployment Using Ruijie Cloud App (Routing Mode)

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

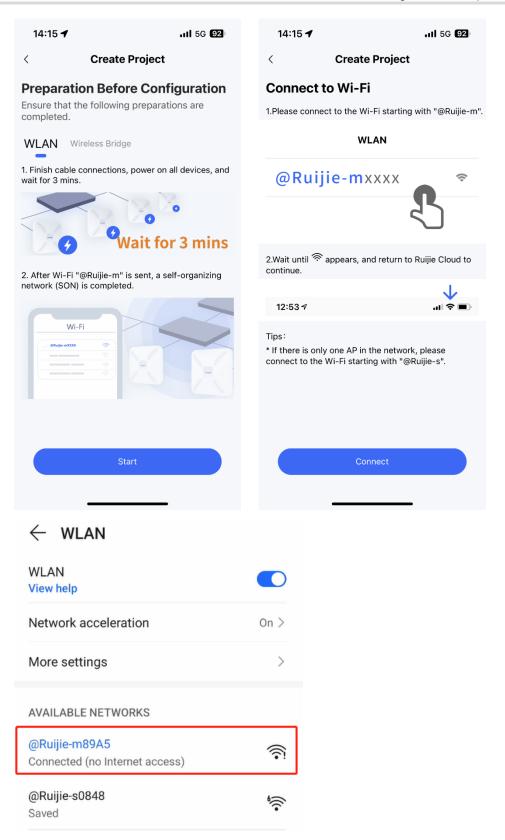
(1) After the network environment is established according to the preceding figure, start the Ruijie Cloud app and choose Project > Add a project.

14:14	0		1 50	g 93
Ruijie	Reyce		Ļ	Q
			G	
Scan		DEMO	Тоо	lkit
My 0	Received 1			Filter T
	+	Add a pro	oject	
[7]	$\widehat{\mathbf{v}}$	*	Ø	8
SaleForce	Product	Project	Community	20000

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

14:15 🗲		all 5G 92)
Ruijie Reyce		4 Q
E Scan	DEMO	C Toolkit
My 0 Received 1		Filter T
? Crea	ate a project	×
Have	Reyee APs?	
Reyes	Yes Connect to V	Vi-Fi
	<mark>No</mark> Scan or ente	r SN

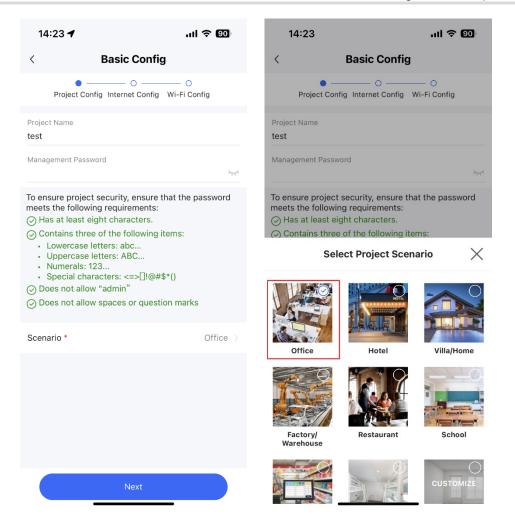
(3) Tap **Connect** to connect to the Wi-Fi signal of the Reyee AP.



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

14:22 🥑	al Ŷ 🗐	14:22 🕇	.ul
< Detect Device		< Detect Detect 3 Devices The devices that support S	;
(29s) Detecting Please wait.		Z324 NB55	/1
		Topo is inc	omplete?~
		Detect Again	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**.

14:23 .ul 🗢 💷
< Basic Config
O Project Config Internet Config Wi-Fi Config
Port Icon
Powered-on ports Selected: Not optional
Select an interface on the firewall for connecting to the ISP network. •
0/MGMT 1 2 3 4 5
Internet Connection*
DHCP ~
Network parameters are automatically assigned. You do not need to configure them.
Enable intrusion prevention
Next

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

14:23 .ul 후 90) ,	14:24 4 🔊 👀
< Basic Config		< Basic Config
Project Config Internet Config Wi-Fi Config Radio Country/Region Code China	~	Project Config Internet Config Wi-Fi Config Radio Country/Region Code China ~
2.4G/5G Smart Connect		2.4G/5G Smart Connect
SSID/Wi-Fi Name * Please enter the SSID		SSID/Wi-Fi Name * test
Encryption Mode 🕑 Do Not Encrypt 🔵 Encrypt	t	Encryption Mode 🕑 Do Not Encrypt 🔵 Encrypt
Encryption Type OPEN	>	Encryption Type C 59s Delivering
Save		Save

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

14:24	al Ŷ 💷	14:24 🕇	 5G 90
< A	dded Successfully	< Added S	uccessfully
	25		
	Please wait.		n delivering the
	Configuring Wi-Fi	the new Wi-Fi Ruijie Reyee Ap	Please connect to after returning to p for connectivity est.
	Configuring Device	👼 tes	t
T		🕂 No	Password
•	Configuring Network		
		Co	nnect
		_	

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

14:26 🕇		al ? 89	14:27 🔫	al 🗢 🛙	9
< test		¢ ≁ :	< D	evice Information	
 ▲ Office(BYOD) ⊘ Uptime 0d 01 			Online	firewall ∠ Model: Z3200-S IP: 192.168.1.200 MAC: 00:d0:f8:22:36:af SN: MACCMMMZ3200S Firmware Version: NGFW_NTOS 1.0R5, Release(03180701) CPU 25% Memory 33.8%	
	1/1 23200-5 1/1 NB55100		Port		3
	RAP1200(E)		All ports Port Ge0/0	Speed Mode	
Client List 2		p Detect	192.168.1.200, Ge0/1 192.168.3.4/24	1000M Routed Port	
G Workspa	ice	Q	Ge0/2	Disabled Transparent	
Basic	Advanced	Scenario	Ge 0/3	Disabled Transparent	
Q On-site					

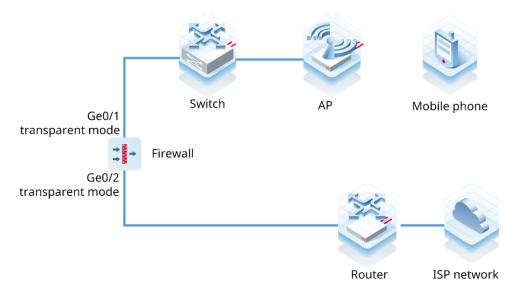
7.1.4 Deployment Using Ruijie Cloud App (Transparent Mode)

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.

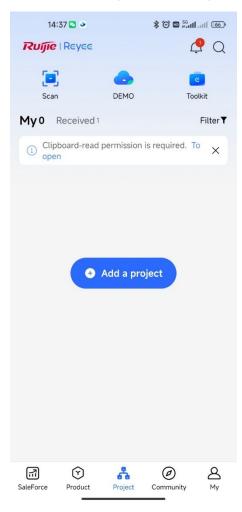
🚺 Note

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

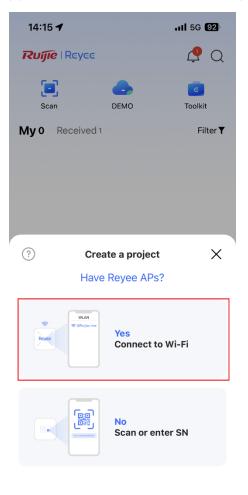


2. Procedure

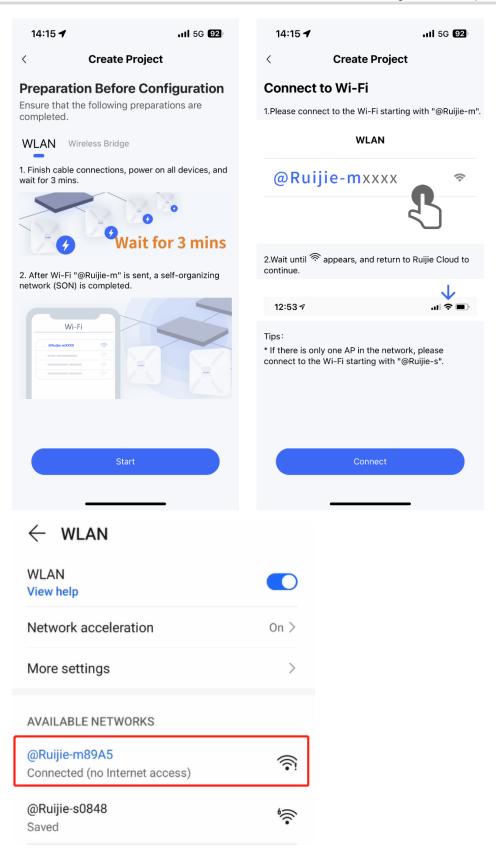
(1) After the network environment is established according to the preceding figure, start the Ruijie Cloud app and choose Project > Add a project.



(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.

14:22 🔿	ul 🗢 🔟	14:39 圆 🕥 🎐	60 % . ? © \$
< Detect Device		< Detect	Device
		Detect 6 Devices	
(29s) Detecting Please wait.		Add Manually	20-5
		NBS32	1
		Topo is inco	omplete?~
		Detect Again	Start Config

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

14:39 圆 🕒 🎐	🚳 🕱 III. III. 🏵 🛠
< Basi	ic Config
O Project Config Internet Cor	fig Configuration Wi-Fi Config
Project Name nbr_app Management Password	
ruijie@123	0
To ensure project security meets the following requi O Has at least eight char Contains three of the Lowercase letters: a Uppercase letters: A Numerals: 123 Special characters: O Does not allow "admin O Does not allow spaces	racters. following items: bc BC <=>[]!@#\$*() ,"
Scenario *	Office >
	Next

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



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



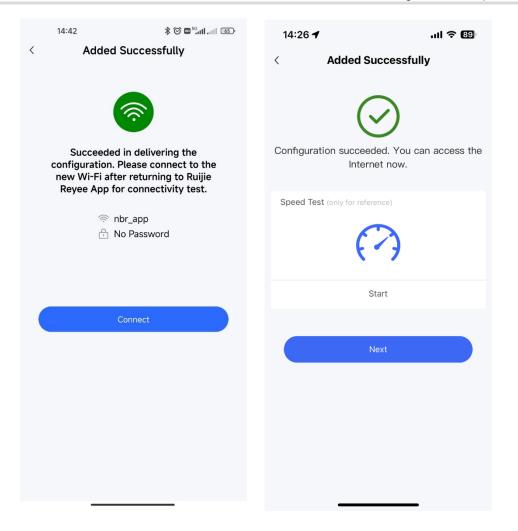
Select an interface on the firewall connected to downlink switch.*



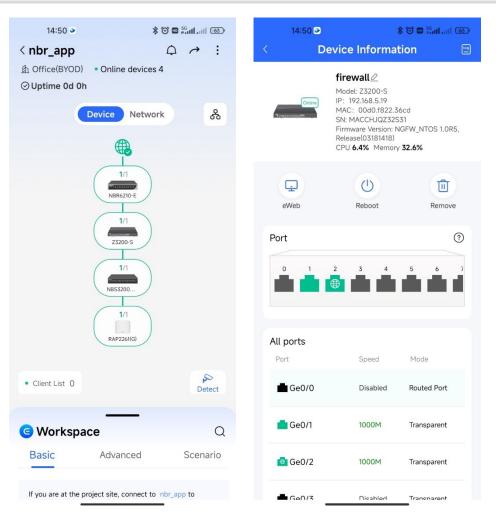
(7) Set the Wi-Fi name and password and tap Save.

14:40 🔟 🕙 🎐	8 O III 🕱 🚳
< Basic C	Config
Project Config Internet Config	Firewall O Configuration Wi-Fi Config
Radio Country/Region Code United States	~
2.4G/5G Smart Connect	
2.4G+5G	
SSID/Wi-Fi Name * nbr_app	
Encryption Mode 🥑 Do No	ot Encrypt 🔵 Encrypt
Encryption Type OPEN	>
Sav	ve 🚽

(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.ruijienetworks.com/ Choose Support > Download > Reyee and find the latest version of the Z-S series firewall under RG-WALL 1600-Z-S series cloud management firewalls.

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 .

A 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.

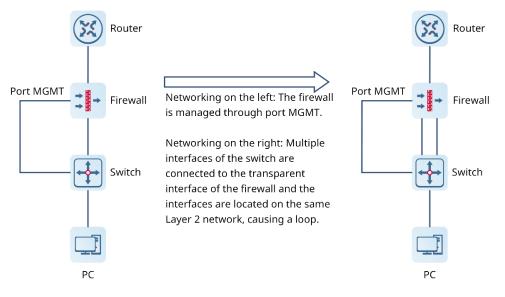
7.2.2 Deployment in Transparent Mode (Quick Deployment)

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



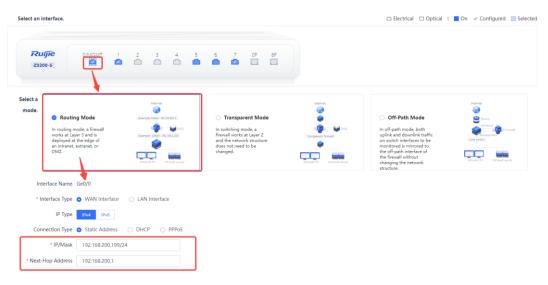
In this example, the firewall connects to the egress router through the WAN interface and connects to the core switch through the LAN interface. Port 0/MGMT (Ge0/0) of the firewall is used as the management interface to connect to the core switch (with management interface address set to 192.168.200.199 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.
 - 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.

RU Z3200			6 7 OF 8F			
elect a mode.	Routing Mode	Land Council (Col) (2010023) Council (Col) (2010024) Council (Council (Co	• Transparent Mode In switching mode, a find and the network structure does not need to be changed.	Intervet Comparent forest Fo	Off-Path Mode In off-path mode both of minated downink traffic monitored in mirored to the off-path interface of the fireval without changing the network structure.	Herener Constantion Constantion Herener Constantion Herener
Inter	rface Name Ge0/1					
	ection Type O Static Address	O DHCP				
	ection Type Static Address nterface.		5 <u>6</u> 7 Of 8F		으 Electrical	I 📕 On 🗸 Configured 📗 S
* Conne Select an in	ection Type Static Address nterface.		5 7 05 8F 7 0F 8F 7 0F 8F 7 0F 8F 1 0F 1 0F		Off-Path Mode In off-path mode, both uplik and downlink traffic on switch interfaces to be monitored is minimized as the firewall without changing the network	I On Configured S
* Conne Select an In 2320 Select a mode.	ection Type Static Address nterface.	2 3 4 Prove Completion (2010) Completion (2010)	Transparent Mode In switching mode, a firevall works at Layer 2 and the network structure does not need to be		Off-Path Mode In off-path mode, both uplink and downlink traffic on switch interfaces to be the off-path interface of the fireval without	bana
* Conne Select an Iri 2320 Select a mode.	ection Type Static Address nterface.	2 3 4 Competing (1,2)(3)(2) Competing (1,2)	Transparent Mode In switching mode, a firevall works at Layer 2 and the network structure does not need to be	Internet Second Tengenet Second Se	Off-Path Mode In off-path mode, both uplik and downlink traffic on switch interfaces to be monitored is minimized as the firewall without changing the network	bana

(2) (Optional) Check the connectivity.

Ruíjie	$\mid \mathbb{Z}$ Series Firewall	습 Home	S Monitor	Network	₽ Object	ତ Policy	System	M Network Discovery	⊗ Network Mgmt	£ Quick Onboarding	Ø Policy Wizard	নি Customer Service	Q admin
Quick	Onboarding W	izard											Exit
	🚫 Quick Onbo	arding			ⓒ Cor	nnectivity Ch	neck ·····	O Device C	oudification			O Finis h	
						Net	twork connectivity is normal Rease us to the next ster. Teter Again						Const
Previou	IS												Next

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

Quick Onboarding Wizard	Quick Onboarding	Connectivity Check	Device Cloudification	O Finish	Exit Wizard
Contraction of the second seco	e App to scan the QR e cloud for remote n Ruijie Reyee App. the QR code. nect to Ruijie Cloud.				
Note:You must set DNS bef		.com whether a correct DNS server is set. Otherwise, the configuration c upper-layer DHCP address pool configuration.)	cannot take effect. (If the outbound interface is configured	WRD DHCP or PPPoE, the DNS server	Q Court
		Previous Next			

Ruíjie	${\mathcal Z}$ Series Firewall	습 Home	G Monitor	Network	,₽= Object	Policy	System		M Network Discovery	⊗ Network Mgmt	1 Quick Onboarding	@ Policy Wizard	ြ Customer Service	Q admin
Quick	Onboarding W	lizard												Exit
	🚫 Quick Onbo	arding			🔗 Conn	ectivity Chec	k		🚫 Device	Cloudification			• Finis	
							\oslash)						
				You	By default, th	ne policy Full Li	AN-to-WAN connectiv	/ity is added to en	sure basic protection.					
								do not configur	_					
														0
							Finish							Consult
							Finish							

Configuration Verification

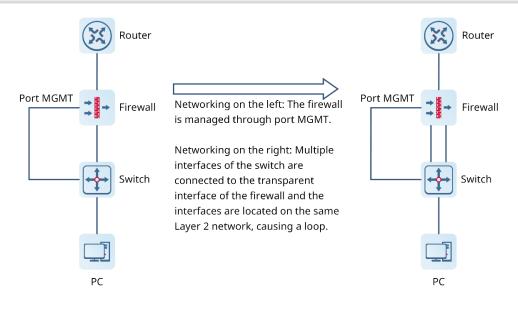
In transparent mode, the firewall can access the Internet without the need to modify the network environment, including the client IP address and gateway IP address.

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

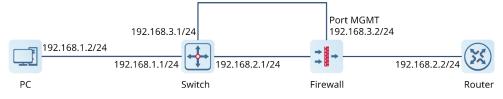
Network Requirements

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 I	nterface
Basic Info	
Interface Name	Ge0/0
Description	
Connection Status	• Enable 🔘 Disable
Mode	Routing Mode Transparent Mode Off-Path Mode
* Zone	untrust ∨ ⊕ Add Security Zone
Interface Type	• WAN Interface O LAN Interface
Address	
ІР Туре	ΙΡν4 ΙΡν6
Connection Type	• Static Address O DHCP O PPPoE
* IP/Mask	192.168.3.2/24
* Next-Hop Address	192.168.3.1
Default Route	
Line Bandwidth	
Uplink	Select V
Downlink	Select V

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

A Caution

The management interface cannot be converted to the transparent mode.

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

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

< Back Edit Physical	Interface	
Basic Info		
Interface Name	Ge0/2	
Description		
Connection Status	• Enable 🔿 Disable	
Mode	Routing Mode Transparent Mode	Off-Path Mode
* Bridge Interface	br0 v	④ Add Bridge Interface
* Zone	trust ~	④ Add Security Zone
Interface Type	O WAN Interface • LAN Interface	J
Advanced		
① MTU	1500	
MAC	00:d0:f8:22:37:0b	Restore Default MAC

c Configure attributes of Ge0/2 and click $\ensuremath{\textbf{Save}}$.

ltem	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 I	nterface	
Basic Info		
Interface Name	Ge0/3	
Description		
Connection Status	• Enable 🔿 Disable	
Mode	 Routing Mode Transparent Mode 	Off-Path Mode
* Bridge Interface	br0 v	Add Bridge Interface
* Zone	untrust ~	Add Security Zone
Interface Type	• WAN Interface O LAN Interface	
Advanced		
① MTU	1500	
MAC	00:d0:f8:22:37:0c	Restore Default MAC

The following figure shows the configuration result.

Ruífic Z Series Firew	vall	습 Home	Monitor	Network	우 Object 💿 Policy	System		(Network		Igmt Quick Onboardi	Ø ng Policy Wizard	ရှိ ဗို Customer Service adm
Interface	~	Physic	al Interface									
Physical Interface Subinterface		😔 Ena	ible 🚫 Disab	le 😋 Refres	h							
			Interface Nam	e Descrip	tion Ce Status	rfa Mode	Zone	Connection Type	IP	Aggregation Mo de	мти	Operation
			Ge0/0	-		Routing	trust	IPv4: Static IP	192.168.3.2/24	-	1500	C Edit
	>		Ge0/1	-		Routing	trust	IPv4: DHCP		-	1500	C Edit
	.		Ge0/2	-	m	Transparent	trust].		-	1500	C Edit
			Ge0/3	-	m	Transparent	untrust	-		-	1500	C Edit
	>		Ge0/4	-	m	Transparent	-	-		-	1500	C Edit
			Ge0/5	-		Transparent	-	-		-	1500	C Edit
			Ge0/6	-		Transparent	-	-		-	1500	C Edit
			Ge0/7	-		Routing	untrust	IPv4: DHCP	172.20.37.124/24	-	1500	C Edit
			TenGe0/0	-	m	Transparent	-	-	-	-	1500	C Edit
			Ge0/8	-	m	Transparent	-	-		-	1500	C Edit

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

Ruijie Z Series Firewall	습 Home 🛛 Ø Monitor	⊕ Network P= Object	Policy	(2) System	ကို 🛞 Network Discovery Network Mgmt
🕲 Security Policy 🛛 🗸	< Back Create Se	curity Policy			
Policy Config Wizard	Basic Info				
Security Policy Policy Optimization	* Name	all_trust_to_untrust			
Policy Life Cycle	Enabled State	Enable			
l Port Scan	* Policy Group	Default Policy Group	~	Add Group	
In Traffic Learning	* Adjacent Policy	allow_all		Before 🗸	
Standard NAT Policy	Description	Enter the security policy nar	me desc		
G Security Defense >	Src. and Dest.				
A Blocklist and Allowlist	Src. and Dest.				
🗑 Reputation Center	* Src. Security Zone	trust			
	* Src. Address	any			
	* Dest. Security	untrust			
	Zone				
	* Dest. Address	any			
	Service				
	Service	Select a service.			
	Арр				
	Арр	Select an application.			

(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.

Security Policy ~	Security Policy						Network	Discovery Net	work Mgmt	Quick Onboarding	Poincy Wizard	Customer Service
Policy Config Wizard Security Policy	Policy Group =	• Create	🛅 Delete 🥥 B	nable 🚫 Dis	able 🖸 Refresh	More ~		Туре	All		Enter a ke	
Policy Optimization Policy Life Cycle	Add Policy Group	🗆 Pr	riority Name	Туре	Src. Security Z one	Src. Addres	Dest. Security Zone	Dest. Addr ess	Service	Арр	Time Rang e	A Operation
Policy Life Cycle 命 Port Scan	Keyword Q All Groups	 Default 	t Policy Group									
Traffic Learning Se NAT Policy	81 (4) Default		1 port_scan	IPv4	any	any	any	PortScan	service_2	any	any	C Edit Delete
Security Defense >			2 allow_trus		trust	any	untrust	any	any	any	any	C Edit Delete
Blocklist and Allowlist			3 allow_all		any	any	any	any	any	any	any	C Edit Delete
SSL Proxy >			4 Default Po.		any	any	any	any	any	any	any	C Edit Delet

🛕 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.

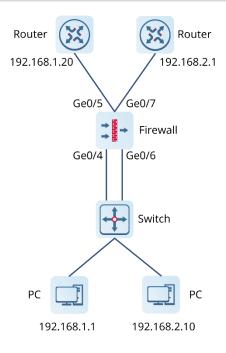
- You can successfully log in to the web management page to configure and manage the firewall.
- The PC on the same network segment as the management IP address can normally access the network.

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.

A 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**.

Ruijie Z Series Firewall	습 Home 🛛 Monitor	🔁 Network 🔑 Obj	iject 🖾 Policy	System		R Network Discovery	🛞 Network Mgmt	1 Quick Onboarding	Ø Policy Wizard	Customer Service	오 admin
Interface	Zone										
🖲 Zone	🕑 Create 📋 Delete	a D Refrach									
🖶 Routing >	U create	e Menesii									
III SSL VPN	Name		Description		Interface L	st	Refere	nce		Operation	
100 DNS	trust		Trust Zone.		Ge0/0,Ge0/1,G	ie0/2	4 Vie	w	E	dit Delete	
🔲 DHCP >	untrust		Untrust Zone.		Ge0/3,Ge0,	7	4 Vie	w	E	dit Delete	
Link Detection URRP	DMZ		Demilitarized Zo	ine.					E	dit Delete	

b Click Create and create security zone trust1.

< Back Add Security Z	one	
* Name	trust1	
Description		
Interface	To-be-selected (6) 🗌 Select All	Selected (0) Clear
	Enter the keyword.	Enter the keyword.
	Interface	
	Name	
	Ge0/4	
	Ge0/5	
	Ge0/6	
	Ge0/8	
	TenGe0/0	
		Save

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

A Caution

The security zone name must be unique.

(2) Create bridge interfaces.

a Choose Network > Interface > Bridge Interface.

Ruijie Z Series Firewall	🗅 Home 🛛 Monitor 🔀 🛚	etwork 😤 Object 🖾 Policy 🔅 !	System	M Network Discovery	⊗ Network Mgmt	1 Quick Onboarding	Ø Policy Wizard	Customer Service	्र admin
🖨 Interface 🗸 🗸	Bridge Interface								
Physical Interface Subinterface	Member interfaces are	nterfaces configured with the transparen	it mode.						
Bridge Interface Aggregate Interface	🕒 Create 🛅 Delete 🕻	Refresh 🛛 Enable 🛇 Disable							_
傻 Zone	Bridge Interface	Member Interface	Connection Type IP		Next-F	lop Address		Operation	
		Ge0/2, Ge0/3, Ge0/4							
iið SSL VPN >	br0	Ge0/5, Ge0/6, Ge0/8 TenGe0/0	DHCP -		-			O Edit Delete	
10 DNS									
■ DHCP >									

b Click Create and create bridge interface br1.

< Back Add Bridge In	terface
Basic Info	
* Interface Name	br1
Connection Status	• Enable O Disable
Member Interface	Select ~
Address	
Connection Type	○ Static Address • DHCP
Src. MAC Consistency	
Check	
 Src. MAC Consistency 	
Check	
Access Management	
Permit	□ HTTPS □ PING □ SSH
	Save

- c Configure parameters for the bridge $\mbox{br1}$ and $\mbox{click Save}.$
- d Repeat the preceding steps to create bridge interface **br2**.

Ruijie Z Series Firewall	☆ Home	Network & Object	t 🐨 Policy 🔅	🕄 System	۹ Network D		⊈ Quick Onboarding	Ø Policy Wizard	Customer Service	ې admii
E Interface V	Bridge Interface									
Physical Interface Subinterface	① Member interfac	es are interfaces configure	d with the transpar	ent mode.						
Bridge Interface Aggregate Interface	🕑 Create 📋 Delet	e 🖸 Refresh 🥝 Ena	ble 🚫 Disable							
Aggregate Interface	Bridge Interfa	ce Membe	er Interface	Connection Type	IP	Next-	Hop Address		Operation	
Bill Routing >	br0		Ge0/3, Ge0/4 Ge0/6, Ge0/8 /0	DHCP		-		•	D Edit Delete	
圓 DNS 剄 DHCP >	D br1			DHCP					Edit Delete	
Link Detection	D br2			DHCP	-	-			Edit Delete	
H VRRP										

- (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 I	nterface	
Basic Info		
Interface Name	Ge0/4	
Description		
Connection Status	• Enable 🔿 Disable	
Mode	Routing Mode Transparent Mode	Off-Path Mode
* Bridge Interface	br1 v	€ Add Bridge Interface
* Zone	trust1 ~	⊕ Add Security Zone
Interface Type	O WAN Interface O LAN Interface	
Advanced		
① MTU	1500	
MAC	00:d0:f8:22:37:0d	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**.

e C Refresh Description Network Interf ace Status							
Network Interf							
Network Interf							
ace Status	Mode	Zone	Connection Typ e		Aggregation M ode	мти	Operation
	Routing	trust	IPv4: Static IP	192.168.3.2/24	-	1500	Edit
	Routing	trust	IPv4: DHCP	-	-	1500	C Edit
	Transparent	trust	-	-	-	1500	C Edit
	Transparent	untrust	-	-	-	1500	Edit
- n	Transparent	trust1		-	-	1500	Edit
	Transparent	untrust1		-	-	1500	Edit
	Transparent	trust2		-	-	1500	C Edit
	Routing	untrust2		-	-	1500	C Edit
· .	Transparent	-		-	-	1500	C Edit
	Transparent					1500	C Edit
	· m	- Transparent	- Transparent -	- Transparent	- Transparent	- Transparent	- Transparent 1500

The following figure shows the configuration result.

A 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.

Ruffe Z Series Firewall	🖨 Home 🛛 Ø Monitor 🕀 №	Network 유 Object 중 Policy @	3 System	Retwork Discovery	Ketwork Mgmt Quick Onboarding	O Policy Wizard Customer Service adm
	Bridge Interface					
	() Member interfaces are	interfaces configured with the transpare	ent mode.			
Bridge Interface Aggregate Interface		Refresh 🛛 Enable 🚫 Disable				
	Bridge Interface	Member Interface	Connection Type	IP	Next-Hop Address	Operation
	Dr0	Ge0/2, Ge0/3, Ge0/8 TenGe0/0	DHCP			C Edit Delete
	D br1	Ge0/4, Ge0/5	DHCP	-	-	Edit Delete
	D br2	Ge0/6, Ge0/7	DHCP	-	-	Edit Delete

- (4) Create security policies 1 and 2 and associate zones trust1 and untrust1 with security policy 1 and zones trust2 and untrust2 with security policy 2.
 - a Choose **Policy > Security Policy**.
 - b Click **Create** and create security policy 1.

< Back Create Se	curity Policy	
Basic Info		
* Name	sec_1	
Enabled State	• Enable 🔿 Disable	
* Policy Group	Default Policy Group \sim	⊕ Add Group
* Adjacent Policy	allow_all \sim	Before 🗸
Description	Enter the security policy name desc	
Src. and Dest.		
* Src. Security Zone	trust1 ~	
* Src. Address	any \lor	
* Dest. Security	untrust1 ~	
Zone		
* Dest. Address	any \checkmark	

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**.

Ruíjie Z Series Firewall	습 Home 🛛 Monitor 🖶 I	Network	A≞ Object	Policy	System		I	Retwork Discovery	🔕 Network Mgmt	E Quick Onboarding	 Policy Wizard 	Customer Service
Security Policy ✓	Security Policy											Simulation Sp
Policy Config Wizard Security Policy	Policy Group 🔳	🕑 Crea	ate 📋 D	elete 🔗 I	Enable 🚫 Di	isable C Refresh	More ~	1	ype All		Enter a ke	eyword.
Policy Optimization Policy Life Cycle	Add Policy Group		Priority	Name	Туре	Src. Security Z one	Src. Addres s	Dest. Security Zone	Dest. Addr ess	Service	Арр Т	ime Operation
Policy Life Cycle 頃 Port Scan	Keyword Q	✓ Def	ault Policy	Group								
ITraffic Learning	图 (5) Default		1	sec_2	-	trust2	any	untrust2	any	any	any	a Edit Delete
Security Defense			2	sec_1	-	trust1	any	untrust1	any	any	any	a Edit Delete
A Blocklist and Allowlist			з	allow_trus		trust	any	untrust	any	any	any	a Edit Delete
⊜ SSL Praxy >			4	allow_all		any	any	any	any	any	any	a Delete
			5	Default Po.		any	any	any	any	any	any	a Edit Delet

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.

Product Cookbook

Policy Confin Wizard	ecurity Policy			_					🦗 rk Discovery	O Network Mgmt	L Quick Onboarding	Ø Policy Wizard C.	ය 오 istomer Service adm
Policy Config Wizard													的 Simulation Space
Security Policy	olicy Group 🛛 📼	Crea	ate 🚺 D	elete ⊘ E	nable	O Disable	C Refresh	More ~		Type All		Enter a keyw	rd. Q
Policy Optimization Policy Life Cycle	Add Policy Group		Priority	Name	Addr	Service	Арр	Time Rang e	Action	Content Sec urity	Hit Count	Hit Session	Operation
Port Scan	Keyword Q	∨ Def	ault Policy	Group									
Traffic Learning	All Groups ^		1	sec_2	ny	any	any	any	Perm		2612 Clear	View Details	Edit Delete
NAT Policy >			2	sec_1	ny	any	any	any	Perm		5076 Clear	View Details	Edit Delete
Blocklist and Allowlist Reputation Center			3	allow_trus	ny	any	any	any	Perm	L	0 Clear	View Details.	Edit Delete
SSL Proxy			4	allow_all	ny	any	any	any	Perm		0 Clear	View Details.	Edit Delete
			5	Default Po	ny	any	any	any	Den		0 Clear	View Details.	Edit Delete

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

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.

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

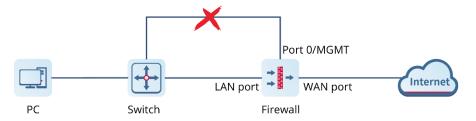
Application Scenario

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.

Bridge Interface

0	Member interfaces are interface	es configured with the transpare	ent mode.			
🕀 Cr	eate 📋 Delete 😋 Refres	h 😔 Enable 🚫 Disable				
	Bridge Interface	Member Interface	Connection Type	IP	Next-Hop Address	Operation
	br0	Ge0/2, Ge0/3, Ge0/8 TenGe0/0, Ge0/5	DHCP			Edit Delete

Note

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

- (2) Perform the corresponding operation on the bridge interface based on service requirements.
- If a new physical interface works in transparent mode, click **Refresh** to obtain the latest member interface information.
- Click **Delete** to delete the bridge interface.

🛕 Caution

- The default bridge interface **br0** of the firewall cannot be deleted.
- The bridge interface with a member interface cannot be deleted. You need to remove the member interfaces before you delete a bridge interface.
- Click Edit and configure the bridge interface. Click Create and create a new bridge interface.

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

Back Add Bridge Interface		
Basic Info		
* Interface Name		
Connection Status	• Enable 🔿 Disable	
Member Interface	Select ~	
Address		
Connection Type	 Static Address DHCP 	
Src. MAC Consistency		
Check		
① Src. MAC Consistency		
Check		
Access Management		
Permit	□ HTTPS □ PING □ SSH	

Item	Description	Remarks
Interface Name	Name of a bridge interface.	 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. [Example] br1
Connection Status	Whether to enable the bridge interface.	[Example] Enable

ltem	Description	Remarks
Member Interface Address	Member interface in the bridge interface. Members of the bridge interface are interfaces set to transparent mode. One bridge interface can contain multiple transparent interfaces, but each transparent interface can belong to only one bridge interface.	To add a member to the bridge interface, set Bridge Interface to the current bridge interface when you configure the corresponding member interface (such as physical interface or aggregate interface). [Example] Ge0/2
Connection Type	 Connection type of the bridge interface. The options are as follows: Static Address: Applicable when the network administrator specifies an IP address for the device based on the predefined IP address planning. This connection type requires the network administrator to possess 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. 	[Example] Static Address
IP/Mask	IP address and mask of the interface.	You need to set this parameter when Connection Type is set to Static Address . [Example] 192.168.20.1/24
Next-Hop Address	Next router address to reach the router with the destination address.	You need to set this parameter when Connection Type is set to Static Address . [Example] 192.168.20.2/24
Default Route	Whether to enable the default route.	[Example] Enable

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

🛕 Caution

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

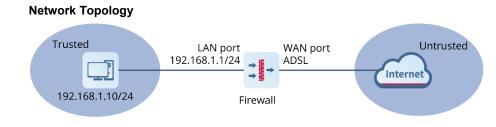
7.3.2 Single-Line Onboarding (Quick Deployment)

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.

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.



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.
 - o 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.

Select an i	interface.				🗅 Electrical 🗖 Optical I	On Configured Selected
		2 3 4 5 2 0 0 0	6 7 OF 8F			
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.	bernet Compared All (1993) Compared All (1993) Compared All (1994) Compared All (1994) C	• Transparent Mode In switching mode, a firewall works at Layer 2 and the network structure does not need to be changed.	bernet Comparent frame Transporter frame Transpo	Off-Path Mode In off-path mode, both uplink and downlink traffic on exitch interfaces to be monitored is mirrored to the firmeal without changing the network structure.	borner Constanting Constantin
Int	terface Name Ge0/0					
* li	nterface Type 🔘 WAN Interface	• LAN Interface				
	IP Туре IPv4 IPv6					
Con	nnection Type 🧿 Static Address					
	* IP/Mask 192.168.1.200/24					
* DHCP	Address Pool 192.168.1.1	-	192.168.1.254			

lect an interface.				🗅 Electrical 🗀 Optical I	■ On ✓ Configured 🎆 S
23200-5	2 3 4 5	5 6 7 OF 8F			
Plect a mode. P Routing Mode In routing mode, a firewall works at Layer 3 and is deployed at the edge of an instanct, extanct, or DMZ.	barret (Sarret) (SJ33823) (Sarret) (SJ53823) (Sarret) (SJ69:SJ3332) (SJ69:SJ332) (SJ69:SJ332) (SJ69:SJ322) (SJ69:SJ322) (SJ69:SJ322) (SJ69:SJ322) (SJ69:SJ322) (SJ69:SJ322) (SJ69:SJ322) (SJ69:SJ322) (SJ69:SJ322) (SJ69:SJ322) (SJ69:SJ322) (SJ69:SJ322) (SJ69:SJ322) (SJ69:SJ322) (SJ69:SJ69:SJ322) (SJ69:SJ69:SJ322) (SJ69:SJ69:SJ522) (SJ69:SJ69:SJ622) (SJ622) (SJ622)	Transparent Mode In switching mode, a firewall works at Layer 2 and the network structure does not need to be changed.	James Company	Off-Path Mode In off-path mode, both uplink and downlink traffic on switch interfaces to be monitored is mirrored to the firmwall without changing the network structure.	Parent Parent Parent Parent Correction Parent Pa
Interface Name Ge0/1 * Interface Type • WAN Interface	O LAN Interface				
IP Type IPv4 IPv6 Connection Type O Static Address	• DHCP O PPPoE				

🛕 Caution

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

(2) (Optional) Check the connectivity.

Ruijie	$\mid \mathbb{Z}$ Series Firewall	🖨 Home	S Monitor	Network	,≗ Object	2 Policy	System	R Network Discovery	⊗ Network Mgmt	1 Quick Onboarding	Ø Policy Wizard	G Customer Service	Q admin
Quic	c Onboarding W	izard											Exit
	Quick Onbo	arding			💽 Cor	nnectivity Ch	ieck ·····	O Device C	loudification			h	
						Net	the example of the second seco	ı.					Const
Previo	ıs												Next

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

Quick Onboarding Wizard	Quick Onboarding	Connectivity Check	Device Cloudification	O Finish	Exit Wizard
	ee App to scan the QR				
Note:You must set DNS bef		tworks.com Check whether a correct DNS server is set. Otherwise, the configuration eck the upper-layer DHCP address pool configuration.)	cannot take effect. (If the outbound interface is configured	J with DHCP or PPPoE, the DNS server	Const.
		Previous Next			

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 (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**.

Ruíjie Z Series Fire	wall	û Home		Network	,& Object	SPolicy	System	Metwork Discover	(Network Mgmt	Quick Onboarding	Policy Wizard	Customer Service	오 admir
	>	DHCP	Service List										
		DHCP Set	rver 💽										
	>		-										
	>	🕑 Crea	te 📋 Delete	e 🖸 Refresh					network.entire	eAgreem€ ∨	network.placeho	olderDHCP	
			Interface		network.pro	tocolTune	network.addressRangeOrPrefix	Default Gateway	Lease Time	DNS		Operation	
🔲 DHCP	\sim		interface		network.pro	tocorrype	network.addresskangeorPrenk	Default Gateway	Lease Time	DNS		operation	
DHCP Server			Ge0/0		Ipv4	1	192.168.1.1-192.168.1.254	192.168.1.200	1Hour0Minute	114.114.114.1	14	Edit Delete	
	t List												

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.)

Ruffe Z Series Firewall	습 Home 🛛 Ø Monitor	Metwork	₽ Object	ල Policy	System
☐ Interface >	< Back Create Sta	tic Routing			
 	Ib .	Type IPv4			
Static Routing	* Dest. IP Range/N	Mask			
Intelligent Routing	Next-Hop Add	dress			
Address Library Route	Inter	rface Select			\sim
	* 🕕 Pri	ority 5			
i SSL VPN > > i i i i i i i i i i i i i i i i i	Link Deteo	ction Link De	etection		\sim
戻 DHCP >	Descrip	otion			
link Detection					2
旧 VRRP					

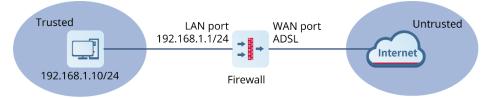
7.3.3 Single-Line Onboarding (Custom Deployment)

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



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

Configuration Points

Step	Description	Key Configuration
Configure interfaces.	 Select two interfaces on the device and set the interface type to WAN interface and LAN interface respectively. WAN interface: Used to connect to the Internet. LAN interface: Used to connect to the LAN. 	 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 Ian and IP address to 192.168.1.10.
Create a security policy.	Create a policy to control traffic between the LAN interface and WAN interface.	 Src. Security Zone: trust Src. Address: lan Dest. Security Zone: untrust Dest. Address: any
Configure NAT.	Configure source NAT to allow the LAN user to normally access the Internet.	 Src. Security Zone: trust Src. Address: lan Dest. Security Zone: untrust Dest. Address: any Src. Address Translated to: Outbound Interface Address

Procedure

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

< Back Edit Physical I	Edit Physical Interface					
Basic Info						
Interface Name	Ge0/7					
Description						
Connection Status	• Enable 🔿 Disable					
Mode	• Routing Mode 🔿 Transparent Mode 🔿 Off-Path Mode					
* Zone	untrust \lor \odot Add Security Zone					
Interface Type	WAN Interface LAN Interface					
Address						
ІР Туре	IPv4 IPv6					
Connection Type	○ Static Address ○ DHCP ● PPPoE					
* Account	admin					
* Password	•••••					

c Set parameters for the interface.

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

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

Line Bandwidth		
Uplink	Select v	
Downlink	Select ~	
Access Management		
Permit	🖌 HTTPS 🛛 PING 🗹 SSH	
Advanced		
ISP Address Library	ISP Address Library V	
① MTU	1500	
MAC	00:d0:f8:22:37:10	Restore Default MAC
Link Detection	Link Detection V	

e Click Save.

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

Ruffie Z Series Firewall	ය Ho	me 🛛 Monito	Network A	Object 🖙 Policy 🐵 Syst	em			m Network Discovery	🐼 Network Mgmt Quid	k Onboarding Policy Wizard	ନ ଥ Customer Service admi
	Phy	sical Interfac	e								
Physical Interface Subinterface	0	Enable 🚫 Dis	able 😋 Refresh								
	C	Interface Na	me Descriptio	n Network Interfac	e Mode	Zone	Connection Type	IP	Aggregation M	lode MTU	Operation
	0	Ge0/0			Routing	trust	IPv4: Static IP	192.168.1.200/24		1500	💽 Edit
	C	Ge0/1	-		Routing	trust	IPv4: DHCP	-	-	1500	C Edit
	C	Ge0/2			Transparent	trust				1500	C Edit
	0	Ge0/3			Transparent	untrust				1500	Edit
	0	Ge0/4		m	Routing	trust1				1500	Edit
		Ge0/5			Transparent	untrust1		-		1500	Edit
		Ge0/6			Routing	untrust	IPv4: DHCP	172.20.37.124/24		1500	Edit
	0	Ge0/7			Routing	untrust	IPv4: PPPOE	192.168.99.2/32	-	1500	Edit
	0	TenGe0/0	-	m	Transparent	-	-	-	-	1500	Edit
		Ge0/8			Transparent	-		-	-	1500	C 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 I	nterface
Basic Info	
Interface Name	Ge0/6
Description	
Connection Status	• Enable O Disable
Mode	• Routing Mode 🔿 Transparent Mode 🔿 Off-Path Mode
* Zone	trust v 🗢 Add Security Zone
Interface Type	○ WAN Interface ● LAN Interface
Address	
ІР Туре	IPv4 IPv6
Connection Type	• Static Address O DHCP O PPPoE
* IP/Mask	192.168.1.1/24

c Set parameters for the interface.

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

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

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

Ruffic Z Series Firewall	☆ Home	nk A₂ Object ເ⊴ Policy © System		🕅 😵 🖬 Network Discovery Network Mgmt Quick Onboard	ා ද ding Policy Wizard Customer Service admi
Interface ~ Physical Interface	IPv4 IPv6				
Subinterface	C Refresh				Enter a destination sub Q
Bridge Interface	Туре	Dest. IP Range/Mask	Next-Hop Address	Priority	Interface
Aggregate Interface	Static route	0.0.0/0	172.20.37.1	5	Ge0/7
嗄 Zone ⊟ Routing ~	Static route	0.0.0.0/0		5	ppp15
Static Routing	Direct route	172.20.37.0/24		-	Ge0/7
Intelligent Routing	Direct route	192.168.1.0/24			Ge0/0
Address Library Route	Direct route	192.168.99.1/32			ppp15
Routing Table					
BB SSL VPN >					
00 DNS					
🔲 DHCP >					
S Link Detection					
URRP VRRP					

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

Ruffe Z Series Firewall	🗅 Home 🛛 Monitor ⊕	Network A Object	ତ Policy 🔅 System	
[] Address	< Back Add IPv4 Add	lress Object		
🚱 Арр	Paula Infe			
URL Category	Basic Info			
写 Service	* Name			
🗄 Time Plan	Description			
🙊 ISP Address Library				
(P) User Authentication >				
E Certificate			ĥ	
Content Template >	IP Address/Range			
🕀 Security Rule Base	* ① IP Address/Range			
			4	

c Set parameters for the address object.

Set Name to Ian and IP Address/Range to 192.168.1.10.

- d Click Save.
- (4) Create a security policy.
 - a Choose Policy > Security Policy > Security Policy.
 - b Click **Create** and create a security policy.

< Back Create S	ecurity Policy	
Basic Info		
* Name	trust_to_untrust	
Enabled State		
* Policy Group	Default Policy Group	⊙ Add Group
* Adjacent Policy	Default Policy ~	Before v
Description	Enter the security policy name desc	
	Enter the occurry policy haine door	
Src. and Dest.		
* Src. Security Zone	trust ~	
* Src. Address	any \lor	
* Dest. Security	untrust \lor	
Zone		
* Dest. Address	any ~	
Service		
Service	any \lor	
Арр		
Арр	any \vee	
Time Range		
Time Range	Select ~	⊙ Add One-Off Time Plan ⊙ Add Cyclic Time Plan
Action Settings	Demit O Demi	
Action Option	• Permit O Deny	
Cont	ent Security (After being enabled, the fo	llowing configurations only take effect for IPv4 traffic.)
Intrusion Prevention	○ Enable O Not Enabled O Add I	ntrusion Prevention Template
Virus Protection	○ Enable • Not Enabled • Add •	/irus Protection Template
URL Filtering	O Enable O Not Enabled O Add U	JRL Filtering
Advanced	Settings	
		Save

c Set parameters for the policy.

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

Item	Description
Dest. Address	any
Service	any
Арр	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**.

Rujje Z Series Firewall	습 Home ⓒ Monitor
Security Policy	< Back Add NAT
Traffic Learning	NAT Type
State NAT Policy ✓	NAT Type SNAT O DNAT O SNAT and DNAT
NAT	Basic Info
NAT46	* Name rule_nat
NAT64	Enabled State O Disable
NAT66	Description Enter the description.
ALG Address Pool	Time Range any \checkmark \odot Add One-Off Time Plan \odot Add Cyclic Time Plan
NAT64 Prefix	Packet Before NAT
G Security Defense >	* Src. Security Zone trust \lor
ළ Blocklist and Allowlist	* Src. Address any \checkmark
Reputation Center SSL Proxy >	* Dest. Security untrust \checkmark
e sterioxy	Zone
	* Dest. Address any \checkmark
	* Service any \checkmark
	Packet After NAT
	Src. Address O Address Pool O Designated IP O Outbound Interface Address
	Translated to

c Set parameters for the NAT policy.

ltem	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

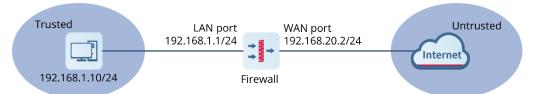
Set the IP address of the PC to 192.168.1.10/24, gateway address to 192.168.1.1, and DNS server addresses to 114.114.114 (primary) and 223.5.5.5 (secondary). (The address of the local DNS server must be used.) The PC can successfully ping the address 114.114.114.114.

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



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

Configuration Points

Step	Description	Key Configuration
Configure interfaces.	 Select two interfaces on the device and set the interface type to WAN interface and LAN interface respectively. WAN interface: Used to connect to the Internet. LAN interface: Used to connect to the LAN. 	 WAN interface: Set Connection Type to Static Address and configure the next-hop address. Add the interface to the security zone untrust. The system automatically generates a default route. LAN interface: Set the IP address to 192.168.1.1/24 and add the interface to the security zone trust. You can choose to enable some management functions on the interface.
Create an address object.	To facilitate management, configure the IP address of the LAN user as an address object.	Set the name to lan and IP address to 192.168.1.10.
Create a security policy.	Create a policy to control traffic between the LAN interface and WAN interface.	 Src. Security Zone: trust Src. Address: lan Dest. Security Zone: untrust Dest. Address: any
Configure NAT.	Configure source NAT to allow the LAN user to normally access the Internet.	 Src. Security Zone: trust Src. Address: lan Dest. Security Zone: untrust Dest. Address: any Src. Address Translated to: Outbound Interface Address

Procedure

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

Ruffe Z Series Firewall	습 Home I Monitor 🖶 Network 🔑 Object I 명 Policy ۞ System
🕒 Interface 🗸 🗸	< Back Edit Physical Interface
Physical Interface	Basic Info
Subinterface	
Bridge Interface	Interface Name Ge0/6
Aggregate Interface	Description
🛛 Zone	Connection Status 🧿 Enable 🛛 Disable
Here and the second sec	Mode 🝳 Routing Mode 🛛 Transparent Mode 🔷 Off-Path Mode
間 SSL VPN >	* Zone untrust v ③ Add Security Zone
ää DNS	
	Interface Type 🗿 WAN Interface 🔷 LAN Interface
link Detection	Address
B VRRP	IP Type IPv4 IPv6
	Connection Type 🧿 Static Address 🛛 DHCP 🔷 PPPoE
	* IP/Mask 192.168.20.2/24
	* Next-Hop Address 192.168.20.1
	Default Route

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.

UIJIC Z Series Firewall	🖨 Home	e 🛛 Monitor 🍕	Network ,A_ Object	Policy System				M Network Discovery	😵 Network Mgmt	Quick Onboarding	Policy Wizard	Customer Service	ر be e
Interface ~	Phys	ical Interface											
Physical Interface Subinterface	😔 Er	nable 🚫 Disable	C Refresh										
		Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregatio	on Mode MTU		Operation	n
		Ge0/0			Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500		Edit	it
		Ge0/1			Routing	trust	IPv4: DHCP	-	-	1500		C Edit	it
		Ge0/2	-		Transparent	trust	-	-	-	1500		C Edit	it
		Ge0/3	-		Transparent	untrust	-			1500		C Edit	it
		Ge0/4	-		Routing	trust1	-	-	-	1500		C Edit	it
		Ge0/5	-		Transparent	untrust1	-	-	-	1500		Edit	ít
		Ge0/6	-		Routing	untrust	IPv4: Static IP	192.168.20.2/24		1500		C Edit	ít
		Ge0/7			Routing	untrust	IPv4: DHCP	172.20.37.124/24		1500		Edit	ít
		TenGe0/0			Transparent		-	-	-	1500		Edit	it
		Ge0/8			Transparent					1500		Edit	it

- (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	dit Physical Interface							
Basic Info								
Interface Name	Ge0/1							
Description								
Connection Status	• Enable 🔿 Disable							
Mode	• Routing Mode 🛛 Transparent Mode 🔷 Off-Path Mode							
* Zone	trust \lor \odot Add Security Zone							
Interface Type	O WAN Interface IAN Interface							
Address								
IP Туре	ΙΡν4 ΙΡν6							
Connection Type	• Static Address O DHCP O PPPoE							
* IP/Mask	192.168.1.1/24							

c Set parameters for the interface.

ltem	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.

Ruijie Z Series Firewall	습 Home	S Monitor	Network	우 Object	I Policy	System		M Network Discovery	⊗ Network Mgmt	E Quick Onboarding	Ø Policy Wizard	Customer Service	오 admin
Interface >	IPv4	IPv6											
図 Zone 🖶 Routing 🛛 🗸	⊙ Cre	ate 🔟 Delete	e C Refres	h							Enter a d	estination sub	
Static Routing		Dest. IP Rang	e/Mask N	lext-Hop Add	ress	Interface	Priority	Link	Detection	Description		Operation	
Intelligent Routing		0.0.0.0/	0	192.168.20.1		Ge0/6	5		-			Edit Delete	
Address Library Route													
Routing Table													
00 SSL VPN →													
III DNS													
🔲 DHCP >													
Link Detection													
URRP VRRP													

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

Ruffe Z Series Firewall	습 Home 🛛 Ø Monito	or	,₽_ Object	ଞ Policy	ම System
匣 Address	< Back Add IPv	4 Address Ob	ject		
谷 App 딸 URL Category	Ва	sic Info			
Service		* Name Ian			
🗄 Time Plan	Des	cription			
ISP Address Library					
(2) User Authentication >					
臣 Certificate >					1
Content Template >	IP Address	/Range			
Security Rule Base	* () IP Address	/Range 192.16	8.1.10		
					1

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

< Back Create S	ecurity Policy	
Basic Info		
* Name	trust_to_untrust	
Enabled State	• Enable 🔿 Disable	
* Policy Group	Default Policy Group	⊙ Add Group
* Adjacent Policy	Default Policy ~	Before v
Description	Enter the security policy name desc	
Src. and Dest.		
* Src. Security Zone	trust \lor	
* Src. Address	any \vee	
* Dest. Security	untrust \vee	
Zone		
* Dest. Address	any \vee	
Service		
Service	any \vee	
Арр		
Арр	any ~	
Time Range		
Time Range	Select ~	⊙ Add One-Off Time Plan ⊙ Add Cyclic Time Plan
Action Settings		
Action Option	• Permit 🔿 Deny	
Cont	ent Security (After being enabled, the fo	llowing configurations only take effect for IPv4 traffic.)
Intrusion Prevention	○ Enable ● Not Enabled ⊕ Add I	ntrusion Prevention Template
Virus Protection	○ Enable ○ Not Enabled ④ Add \	/irus Protection Template
URL Filtering	○ Enable ○ Not Enabled ④ Add U	JRL Filtering
Advanced	Settings	
		Save

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		
Арр	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**.

Ruijie Z Series Firewall	습 Home ⓒ Monitor ④ Network 옷 Object 명 Policy ⑤ System
⁽²⁾ Security Policy →	< Back Add NAT
 Port Scan Traffic Learning 	NAT Type
Star Policy	NAT Type O SNAT O DNAT O SNAT and DNAT
NAT	Basic Info
	* Name rule_nat
	Enabled State 🧿 Enable 🔿 Disable
	Description Enter the description.
	Time Range any V ③ Add One-Off Time Plan ④ Add Cyclic Time Plan
	Packet Before NAT
G Security Defense >	* Src. Security Zone trust \lor
	* Src. Address any 🗸
🗟 Reputation Center	* Dest. Security untrust ~
	Zone
	* Dest. Address any \lor
	* Service any \checkmark
	Packet After NAT
	Src. Address 🔘 Address Pool 👘 Designated IP 🔹 Outbound Interface Address
	Translated to

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

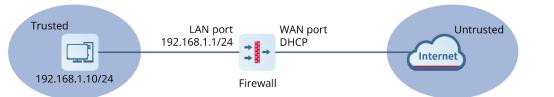
Set the IP address of the PC to 192.168.1.10/24, gateway address to 192.168.1.1, and DNS server addresses to 114.114.114 (primary) and 223.5.5.5 (secondary). (The address of the local DNS server must be used.) The PC can successfully ping the address 114.114.114.114.

3. Onboarding Through DHCP

Network Requirements

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

Network Topology



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

Configuration Points

Step	Description	Key Configuration
Configure interfaces.	 Select two interfaces on the device and set the interface type to WAN interface and LAN interface respectively. WAN interface: Used to connect to the Internet. LAN interface: Used to connect to the LAN. 	 WAN interface: Set Connection Type to DHCP. Add the interface to the security zone untrust. After the WAN interface obtains an IP address through DHCP, the system automatically generates a default route. LAN interface: Set the IP address to 192.168.1.1/24 and add the interface to the security zone trust. You can choose to enable some management functions on the interface.
Create an address object.	To facilitate management, configure the IP address of the LAN user as an address object.	Set the name to Ian and IP address to 192.168.1.10.
Create a security policy.	Create a policy to control traffic between the LAN interface and WAN interface and enable NAT.	 Src. Security Zone: trust Src. Address: lan Dest. Security Zone: untrust Dest. Address: any

Procedure

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

< Back	Edit Physical Interface					
	Basic Info					
	Interface Name	Ge0/7				
	Description					
	Connection Status	• Enable 🔿 Disable				
	Mode	• Routing Mode O Transparent Mode	Off-Path Mode			
	* Zone	untrust ~	⊕ Add Security Zone			
	Interface Type	• WAN Interface O LAN Interface				
	Address					
	IP Туре	ΙΡν4 ΙΡν6				
	Connection Type	○ Static Address	E			

c Set parameters for the interface.

ltem	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.

Physi	hysical Interface									
⊖ En	able 🚫 Disable	C Refresh								
	Interface Name	Description	Network Interfa ce Status	Mode	Zone	Connection Typ e	IP	Aggregation Mo de	мти	Operation
	Ge0/0	-		Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500	Edit
	Ge0/1	-	m	Routing	trust	IPv4: DHCP	-	-	1500	Edit
	Ge0/2	-	m	Transparent	trust	-	-	-	1500	Edit
	Ge0/3	-	m	Transparent	untrust	-	-	-	1500	Edit
	Ge0/4	-	m	Routing	trust1	-	-	-	1500	Edit
	Ge0/5	-	m	Transparent	untrust1	-	-	-	1500	Edit
	Ge0/6	-	m	Routing	trust	IPv4: Static IP	192.168.1.1/24	-	1500	Edit
	Ge0/7	-	m	Routing	untrust	IPv4: DHCP	172.20.37.124/24	-	1500	Edit
	TenGe0/0	-	m	Transparent	-	-	-	-	1500	Edit
	Ge0/8	-	m	Transparent	-	-	-	-	1500	Edit

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

< Back	Edit Physical Interface					
	Basic Info					
	Interface Name	Ge0/6				
	Description					
	Connection Status	• Enable 🔿 Disable				
	Mode	 Routing Mode O Transp 	oarent Mode	Off-Path Mode		
	* Zone	trust	~	⊕ Add Security Zone		
	Interface Type	○ WAN Interface	nterface			
	Address					
	IP Туре	ΙΡν4 ΙΡν6				
	Connection Type	• Static Address O DHCP	🔘 РРРо	E		
	* IP/Mask	192.168.1.1/24				

c Set parameters for the interface.

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

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

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

Ruíjie Z Series Firewall		윤 Object 영 Policy ⓒ System		🖗 🛞 Network Discovery Network Mg	Int Quick Onboarding	Ø € Policy Wizard Custome	a Q r Service adm
☐ Interface >	IPv4 IPv6						
愛 Zone 븝 Routing · ✓	C Refresh					Enter a destination	sub Q
Static Routing	Туре	Dest. IP Range/Mask	Next-Hop Address	Priori	ty	Interface	
Intelligent Routing Address Library Route	Static route	0.0.0.0/0	172.20.37.1	5	Ge0/7		
Routing Table	Direct route	172.20.37.0/24	-	-		Ge0/7	
iii SSL VPN →	Direct route	192.168.1.0/24	-	-		Ge0/0	
60 DNS							
同 DHCP >							
Link Detection							
H VRRP							

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

Ruijie Z Series Firewall	습 Home 🛛 Monitor 🔅	Network	,≏_ Object	🖾 Policy	System	
면 Address	< Back Add IPv4 Ac	ldress Obj	ject			
🚱 Арр						
URL Category	Basic Int	ro				
	* Narr	ne Ian				
🗄 Time Plan	Descriptic	on				
☑ ISP Address Library						
[®] User Authentication →						
딸 Certificate >					11	
Content Template >	IP Address/Rang	je				
🕀 Security Rule Base	* ① IP Address/Rang	ge 192.168	3.1.10			
					11	

- 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.

尼UJIE ℤ系列防火	/墙 ☆ ☆ ☆ ☆ ☆ ☆	全监控 🕀 网络配置 🙏 对象配置	仔 策略配置 (1) 系统管理	主 の G A 快速上线 策略向号 容服 admin
 8 安全策略 ~ 策略配置向导 	< 返回 新增安全省 基础信息	策略		
安全策略 策略优化 第100生命同期 ・ 第10日語 ・ ・ 近量学习 い 部 NAT策略 ン	* 名称	默认策略	2 ② 新聞編 2 ② 第 ~	
63 安全防护 > 為黑白名単	」 源与目的 "源安全区域			C vertes a
	* 源地址 * 目的安全区域 * 目的地址	untrust		
安全策略 策略优化	服务			
策略生命周期	应用			
母、安全防护 → 凡 黒白谷神	时间段 时间段 动作设置	any	 ・ ・ ・	
	内容安全	 ● 允许 ○ 拒绝 ○ 息用 ● 不息用 ◎ 新地入税加速 	RE	
Æ			977	

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
Арр	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 Se	ecurity Policy	
Basic Info		
* Name	trust_to_untrust	
Enabled State	• Enable 🔿 Disable	
* Policy Group	Default Policy Group	Add Group
* Adjacent Policy	Default Policy ~	Before v
Description	Enter the security policy name desc	
Src. and Dest.		
* Src. Security Zone	trust ~	
* Src. Address	any ~	
* Dest. Security	untrust ~	
Zone		
* Dest. Address	any \lor	
Service		
Service	any \vee	
Арр		
Арр	any ~	
Time Range		
Time Range	Select ~	⊙ Add One-Off Time Plan ⊙ Add Cyclic Time Plan
Action Settings		
Action Option	• Permit 🔿 Deny	
Cont	ent Security (After being enabled, the fo	llowing configurations only take effect for IPv4 traffic.)
Intrusion Prevention	-	ntrusion Prevention Template
Virus Protection		
URL Filtering	O Enable • Not Enabled • Add U	JRL Filtering
Advanced	Settings	
		Save

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

A 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**.

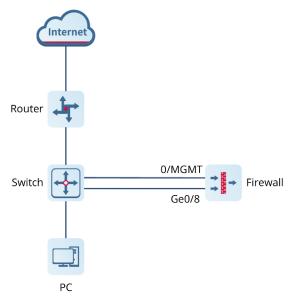
7.4.2 Deployment in Off-Path Mode (Quick Deployment)

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.





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.
 - 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.)

Select an ir	nterface.				🗅 Electrical 🗖 Optical	I 🔲 On 🗸 Configured 📃 Sele
RU 2320			6 7 OF 8F			
Select a mode.	Routing Mode In routing mode, a firewall works at Layer 3 and is deployed at the edge of an intramet, estanet, or DWZ.	Former Company (Add), SU(3813) Company (Add), SU(3812) Company (Add)	Transparent Mode In switching mode, a firewall works at Luyer 2 and the network structure does not need to be changed.	James Company front Transport front Transport front Transporta	Off-Path Mode In off-path mode, both uplinic and downink traffic on which instructs to be monitored is minored to the fineauli without the fineauli without	travel Control Con
	erface Name Ge0/0	AN Interface				
	IP Type IPv4 IPv6	0				
Conr	nection Type 🧿 Static Address	O DHCP O PPPoE				
	* IP/Mask 192.168.200.199/	24				
	Hop Address 192.168.200.1					

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

elect an in	nterface.												🗅 Electrical 🗖 Optical I	On 🗸 Configured	Sel
RU 2320	-	0/MGMT	1	2	3	4	5	6	7	OF	Ë				
elect a mode.	In routing works at L deployed	ing Mode mode, a firewall ayer 3 and is at the edge of t, extranet, or		for a	Internet	W omz		In fire an do	switching	is at Layer work struct	2	Denvel	 Off-Path Mode In off-path mode, both uplink and downlink traffic on switch interfaces to be monitored is mirrored to the off-path interfaces of the off-path interface of the network structure. 	Exercit Core subt Forum Core subt Forum	
Int	erface Name Zone														

Note

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

(2) (Optional) Check the connectivity.

Ruíjie	🛛 🎜 Series Firewall	습 Home	S Monitor	Network	은 Object	Policy	System	M Network Discovery	⊘ Network Mgmt	▲ Quick Onboarding	Ø Policy Wizard	റെ Customer Service	्र admin
Quic	k Onboarding W	/izard											Exit
	🚫 Quick Onbo	barding			(•) Cor	nnectivity Ch	neck	O Device C	loudification			O Finis h	
						Net	twork connectivity is normal Rease go to the next step: Detect Again						Cenut
Previo	us												Next

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

Quick Onboarding Wizard	Quick Onboarding	Connectivity Check	Device Cloudification	O Finish	Exit Wizard
Enable Ruijle Cloud-based Ma Ruijle Cloud-based Management (*) You can also use Ruijle Reyes cade and quickly connect to the co- management. (*) You can also use Ruije Reyes cade and quickly connect to the management. (*) The login/registration address Neterbor must are DNS before	App to scien the QR bound for remote upper Reyree App. to CR code. to the Ruijie Cloud. The for Ruijie Cloud is https://cloud.ruijieretenor connecting the device to Ruijie Cloud. Chee				
		Previous Next			

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

Note

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

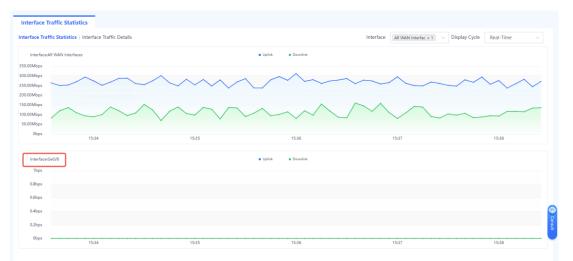
(5) Create a security policy.

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**.

ecurity Policy												59 Simulation Space
olicy Group 🛛 🚍	🕒 Creat	e 🔟 C	Delete 🕝 Enab	le 🚫 Dis	sable 🖸 Refresh	More ~		Туре	All		Enter a keywo	ord. Q
Add Policy Group Keyword Q		Priority	Name	Туре	Src. Security Z one	Src. Addres s	Dest. Security Zone	Dest. Addr ess	Service	Арр	Time Rang e	Operation
All Groups	∨ Defa	ult Policy	Group									
8 (4) Default		1	monitor_r	-	monitor	any	monitor	any	any	any	any	Delete
		2	allow_trus	-	trust	any	untrust	any	any	any	any	Edit Delete
		3	allow_all	-	any	any	any	any	any	any	any	Edit Delete
		4	Default Po	-	any	any	any	any	any	any	any	Edit Delete

Configuration Verification

Choose **Monitor > Traffic Monitoring > 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.

Ruíjie Z Series Fire	wall	습 Home	© Monitor ₫	🕒 Network 🛛 🔑 🛛	Object ເ영 Policy 영 Sy	stem		Network D	iscovery Network M	 gmt Quick Onboardin	⊘ ng Policy Wizard	Customer Service ac
Interface	~	Physi	cal Interface									
Physical Interface												
		⊖ En	able 🚫 Disable	C Refresh								
			Interface Name	Description	Network Interfa ce Status	Mode	Zone	Connection Typ e	IP	Aggregation Mo de	MTU	Operation
			Ge0/0	-		Routing	trust	IPv4: Static IP	192.168.1.200/24		1500	Edit
	>		Ge0/1	-		Routing	trust	IPv4: DHCP	-	-	1500	C Edit
	>		Ge0/2	-		Transparent	trust	-	-	-	1500	C Edit
			Ge0/3	-		Transparent	untrust	-	-	-	1500	C Edit
	>		Ge0/4	-		Routing	trust1	-	-	-	1500	C Edit
			Ge0/5	-		Transparent	untrust1			-	1500	C Edit
			Ge0/6	-		Routing	trust	IPv4: Static IP	192.168.1.1/24	-	1500	C Edit
			Ge0/7			Routing	untrust	IPv4: DHCP	172.20.37.124/24		1500	C Edit
			TenGe0/0			Transparent					1500	C Edit
			Ge0/8			Transparent					1500	Edit

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

< Back Edit Physical I	nterface	
Basic Info		
Interface Name	Ge0/8	
Description		
Connection Status	• Enable 🔿 Disable	
Mode	O Routing Mode O Transparent Mode	 Off-Path Mode
* Zone	monitor ~	Add Security Zone
	• Note: When configuring a security policy for the off-path mode, set both the source zone and destination zone to this monitor zone, and mirror both uplink and downlink traffic on switch interfaces to be monitored to the off-path interface of the firewall.Ge0/8	

- c Click Save.
- (2) Create a security policy.

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

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

olicy Group	=	_									
Silcy Gloup	=	Create Bat	ch Operation 🗸	More 🗸 😋 Refres	h 🔀 Custom	Field	Туре	All		Enter a keyw	ord. Q
 Add Policy Group 		Priority	Name	Src. Security Zone/I nterface	Src. Address	Src. Region	Dest. Security Zone/I nterface	Dest. Address	Dest. Region	Servi	Operation
Keyword		Default Policy	/ Group								
81 Groups 81 (7) Default	^ E) 1	sslvpn_c2s	untrust	ippool_test	any	any	res_test	any	any	Edit More ~
01 (1) 0 1011		2	4_To_2_in	4_To_2	any	any	any	any	any	any	Edit More ~
		3	BPS组	trust	any	any	untrust	any	any	any	Edit More ~
		4	defaulti	trust	any	any	untrust	any	any	any	Edit More ~
		5	allow_all	any	any	any	any	any	any	any	Edit More ~
		6	nat_test	untrust	any	any	any	any	any	nat_t	Edit More ~
		7	Default Po	nat_test any	any	any	any	any	any	any	Edit More ~

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.

Тір	\otimes
Are you sure you want to add	it in the simulation space?
The policy execution process can execution. The simulation helps you is in policies in advance and avoid risks	dentify vulnerabilities and issues
Do Not Show	r 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.

K Back Create S	ecurity Policy		
Basic Info			
* Name	monitor_sec_rule		
Enabled State	Enable		
* Policy Group	Default Policy Group	~	
* Priority	allow_all	~	Before 🗸
Description	Enter the security policy name desc		
Src. and Dest.			
Src. Security	monitor	~	
Zone/Interface			
* Src. Address	any	~	
Src. Region	any	~	
Dest. Security	monitor	~	
Zone/Interface			
* Dest. Address	any	~	
Dest. Region	any	~	
Service	any	~	
Action Option	• Permit O Deny		
	App、User、Effective Time $\ \lor$		
Content Security			
Intrusion Prevention	Disable		
Virus Protection	Disable		
URL Filtering	Disable		
Keyword Filtering	Disable		
Advanced	Settings		

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

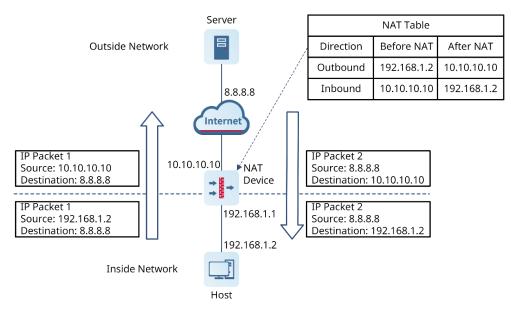
Network Address Translation (NAT) is to translate the source address (port) or destination address (port) in a packet into the desired address. NAT includes the following two steps:

- (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 <u>Figure 8-1</u>, 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

10.1.0.3/24 PC	59.108.29.140/24 Firewall	Internet
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].

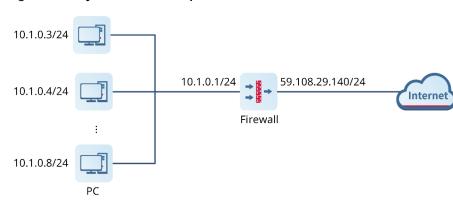


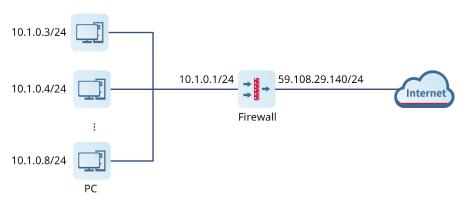
Figure 8-2 Dynamic NAT Example

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.





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.

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.

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

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.

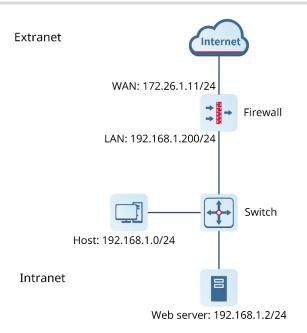
8.1.3 Configuring Destination Address Translation (One-to-One Port Mapping)

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:

Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mod e	МТU	Operation
Ge0/0	-		Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500	Edit
Ge0/1			Routing	untrust	IPv4: DHCP	-	-	1500	Edit

- (2) Configure 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).

Back Add S	Service						
	Basic Info						
* Ser	vice Name						
C	Description			11			
* Pro	otocol List						
	⊕ Create	🗓 Delete	C Refresh				
	P	rotocol	Src. Port	Dest. Port	Туре	Code	Operation
				No	Data		
	Total: 0						
					_		
					Save		

c Click Save.

(3) Configure the security policy.

The policy configuration is as follows:

2	allow_trus	-	trust	any	untrust	any	any	any	any	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
Basic Info	
* Name	WebServer
Enabled State	• Enable 🔿 Disable
Description	Enter the description.
Time Range	any \lor \odot Add One-Off Time Plan \odot Add Cyclic Time Plan
Packet Before NAT	
* Src. Security Zone	trust,untrust \sim
* Src. Address	any \lor
* Dest. Address	172.26.1.116 ~
* Service	18080 ~
Packet After NAT	
* ID	192.168.1.2
① Port	80 .

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

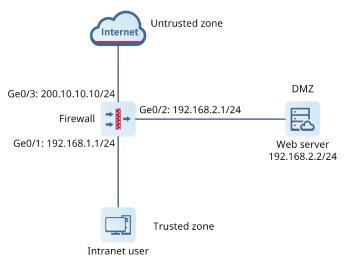
Users can visit http://172.26.1.116 from the Internet.

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 <u>7.3 Routing Mode</u>.

- (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	Serve	r_Mapping					
Description				li			
Protocol List							
	⊕ (Create 🔟 [Delete	Refresh			
		Protocol	Src. Port	Dest. Port	Туре	Code	Operation
		TCP	0-65535	50000	-	-	Edit Delete
	Total:	1					
		Confirm	n and Continu	e Adding	Confirm	Cancel	

- c Click Save.
- (3) Configure the security policy.

The policy configuration is as follows:

	Priority	Name	Туре	Src. Security Z one	Src. Addres s	Dest. Security Zone	Dest. Addr ess	Service	Арр	Time Rang e	Action	Content Sec urity	Hi	Operation
✓ Defa	ault Policy	Group												
	1	permit_loca	IPv4	trust	lan_users	untrust	any	any	any	any	Perm)	0	Edit Delete

(4) Configure port mapping.

Configure the destination address translation policy for extranet users.

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

Cuijie Z Series Firewall	🛆 Home	G Monitor	Network	,8₌ Objec	t 😨 Policy	System				N	etwork Discov	ery Networ		tk Onboarding Policy V	ကြ /card Customer Service ခ
Security Policy	NAT														
الله Port Scan الم) Traffic Learning	⊙ Crea	ite 🗊 Delete	🗄 Сору	🕗 Enabl	le 🛇 Disable	🖆 Import	Move	S Clear Hit	Record	Refresh					
B NAT Policy Y			Time Ra	NAT Ty		Packet Be	efore NAT			Packet	After NAT		Descript		
NAT NAT46		Name	nge	pe	Src. Security Zone	Dest. Security Zone	Src. Add ress	Dest. A ddress	Service	Src. Address	Dest. A ddress	Dest. Po rt	ion	Hit Count	Operation =-
NAT64 NAT66		nat_rule	any	SNAT	trust	untrust	any	any	any	Outbound Interface Address				4.36*10 ⁴ Clear	C Edit Delete
ALG															
Address Pool															
NAT64 Prefix															
Security Defense															
Blocklist and Allowlist															
Reputation Center															
SSL Praxy															

c Set the parameters related to destination address translation.

< Back Add NAT	
NAT Mode	
NAT Mode	○ SNAT ● DNAT ○ Twice Nat
Basic Info	
* Name	rule_1
Enabled State	• Enable O Disable
Description	Enter the description.
Time Range	any \sim \odot Add One-Off Time Plan \odot Add Cyclic Time Plan
Packet Before NAT	
* Src. Security Zone	untrust ~
* Src. Address	any ~
* Dest. Address	200.10.10.10 ~
* Service	Server_Mapping ~
Packet After NAT	
* IP	192.168.2.2
① Port	443
	Save

Item	Description					
Basic Info	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	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 O Twice Nat	
Basic Info		
* Name	rule_2	
Enabled State	Enable	
Description	Enter the description.	
Time Range	any \lor \ominus Add Or	ne-Off Time Plan 🛞 Add Cyclic Time Plan
Packet Before NAT		
* Src. Security Zone	trust \vee	
* Src. Address	any \vee	
* Dest. Address	200.10.10.10 ~	
* Service	Server_Mapping \lor	
Packet After NAT		
Src. Address Translated to	Address Pool ODesignated IP	Outbound Interface Address
* Designated IP	200.10.10.10	
* Dest. Address	192.168.2.2	
Translated to		
 Dest. Port Number 	443	
Translated to		

ltem	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 8-1Products 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.

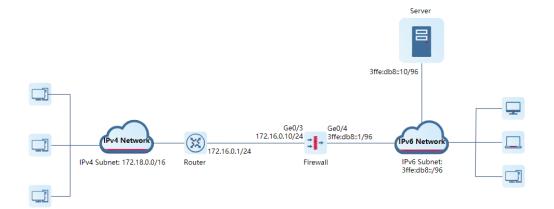


Table 8-2	Key Configuration Points in the Network Diagram
-----------	---

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	0.0.0255.255.255.255

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 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	dress IPv6 Address IPv4 Address Grou		IPv6 Address Grou	р
🛨 Create 🔟 De	lete 😋 Refresh			
Name	I	IP Address/Range	Address Group	Description
Pv4-all	(0.0.0255.255.255.255	-	-
IPv4net-dst		172.16.0.10	-	-
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.

IPv4 Address	IPv6 Address	IPv4 Address Group	IPv6 Address Group	
🕀 Create 🛅 D	elete 🕻 Refresh			
Name	1	IP Address/Range	Address Group Des	cription
IPv6net-ds	t S	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 N	AT64 Prefix
* Name	natpt-src
* () NAT64 Prefix	2ffe:db8::
Prefix Length	96 ~

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	4-to-IPv6 NAT		
Basic Info			
* Name	IPv4net-to-IPv6net		
Enabled State	💿 Enable 🛛 Disab	le	
Description	Enter the NAT policy of	description.	
Packet Before NAT			
* Src. Address	IPv4net-src	~	
* Dest. Address	IPv4net-dst	~	
* Service	any	~	
Packet After NAT			
① NAT Mode	Stateless NAT64	• Static NAT-PT	 Static NAT64
* NAT64 Prefix	natpt-src	 ✓ ⊕ Create I 	NAT64 Prefix
* Src. Address	2ffe:db8::10		
Translated to			
* Dest. Address	3ffe:db8::10	(\times)	
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 Secu	urity Policy	
Basic Info		
* Name	permit-natpt	
Enabled State	• Enable 🔿 Disable	
* Policy Group	Default Policy Group ~	⊕ Add Group
Description	Enter the security policy name desc	
Src. and Dest.		
* Src. Security Zone	any \vee	
* Src. Address	IPv4net-src \lor	
User/User Group	any \vee	
* Dest. Security	any \checkmark	
Zone		
* Dest. Address	IPv6net-dst v	
Service		
Service	Select a service. \sim	
Арр		
Арр	Select an application. \sim	
User/User Group		
User/User Group	Select a user.	
Time Range		
Time Range	Select ~	⊕ Add One-Off Time Plan ⊕ Add Cyclic Time Plan
Action Settings		
Action Option	• Permit 🔿 Deny	
Content	Security	
Intrusion Prevention		ion Prevention Template
Virus Protection		
URL Filtering	○ Enable	iltering
Advanced	Settings	
		Save

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.

\otimes **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.)

	Priority	Name	Src. Address	User/User Group	Dest. Security Zone	Dest. Address	Service	Арр	Time Range	Action	Content Security	Hit Count
∨ De	fault Policy	Group										
	11	permit-nat	IPv4net-src	any	any	IPv6net-dst	any	any	any	Permit		1 Clear
		_	permit-natot									

• 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.)

		Pac	ket Before NAT			Packet	After NAT		
Name	NAT Mode	Src. Address	Dest. Address	Service	NAT64 Prefix	Src. Address Translated to	Dest. Address Translated to	Dest. Port Numb er Translated to	Hit Count
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

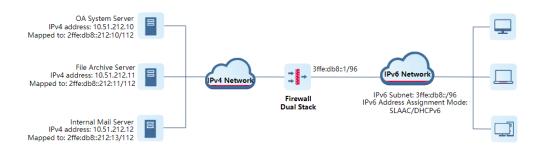
Table 8-3Products and Versions

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.



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

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	
🕀 Create 🛄 D	elete 🕄 Refresh			
Name		IP Address/Range	Address Group	Description
OA-server-	IPv6-mapping-a	2ffe:db8::212:10	-	-

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	
🕀 Create 🛅 De	lete 🕻 Refresh			
Name	I	P Address/Range	Address Group D	escription
OA-server-I	Pv4-address 1	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	Mapping-from-IPv4-to-IPv6						
* 🕕 NAT64 Prefix	2ffe:db8::						
Prefix Length	96 ~						

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 P	ool
* Name	Mapping-from-IPv6Subnet-to-IPv4 \otimes
Description	Enter the description.
* 🕕 IP Address/Range	172.16.10.100-172.16.10.139
	4

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	IPv6Subnet-Access-OA-server					
Enabled State	• Enable 🔿 Disable					
Description	Enter the NAT policy description.					
Packet Before NAT						
* Src. Address	IPv6-subnet-1 \lor					
* Dest. Address	OA-server-IPv6-mapping-address \vee					
* Service	any \checkmark					
Packet After NAT						
① NAT Mode	Dynamic NAT-PT O Dynamic NAT64					
* NAT64 Prefix	Mapping-from-IPv4-to- \lor \bigcirc Create NAT64 Prefix					
* Translate Src.	Mapping-from-IPv6Sut \lor $\textcircled{ dd Address Pool}$					
Address to Address						
in Address Pool						
SNAT Mode	○ NO-PAT ○ PAT					
* 🕕 Port Number	11001-12000					
Range						
* Dest. Address	10.51.212.10 ③					
Translated to						
	Save					

- 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 S	ecurity Policy
Basic Info	
* Name	permit-IPv6net-Access-OAserver
Enabled State	• Enable 🔿 Disable
* Policy Group	Default Policy Group \lor \odot Add Group
* Adjacent Policy	Default Policy \lor Before \lor
Description	Enter the security policy name desc
Src. and Dest.	
* Src. Security Zone	any ~
* Src. Address	IPv6-subnet-1 \lor
User/User Group	Select a user.
* Dest. Security	any ~
Zone	
* Dest. Address	OA-server-IPv4-address \lor
Service	
Service	Select a service.
Арр	
Арр	Select an application.
Time Range	
Time Range	any \lor \odot Add One-Off Time Plan \odot Add Cyclic Time Plan
Action Settings	
Action Option	• Permit O Deny
Content	Security
Intrusion Prevention	 Enable O Disable O Add Intrusion Prevention Template
Virus Protection	 Enable O Disable O Add Virus Protection Template
URL Filtering	 Enable O Disable O Add URL Filtering
Advanced	Settings
	Save

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.

S	ession Description				(\times)
	Basic Info				
	Session Creation Time:2023-09-07 13:20:55			efore Session it:47Second	
	Src. and Dest.				
	Src. Address:172.17.96.1	Dest	t. A	ddress:10.51.212.100	
	Src. Port:6	Dest	t. P	ort:6	
	NAT Src. Address:2ffe:db8::ac11:6001	NAT	De	est. Address:3ffe:db8::da64	
	NAT Src. Port:6	NAT	De	est. Port:6	
	More				
	Protocol:ICMP	App	:Ec	ho-request	
	Inbound Interface:Ge0/2	Out	οοι	ind Interface:Ge0/3	
	Forward Packets:5	Forv	var	d Bytes:500	
	Reverse Packets:5	Reve	erse	e Bytes:400	
	Security Policy:permit-access-IPv6Sever	Sess	ior	State:connection established	
	C	isable			

 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	dress	User/User Group	Dest. Security Zone	Dest. Address	Service	Арр	Time Range	Action	Content Security	Hit Count	Hit Session	Operation
∨ De	fault Policy (Group												
	5	permit-IPv	me	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.)

				Packet Before NAT			Packet After NAT					Description	Operati	
	Name	NAI Mode	Src. Address	Dest. Address	Service	NAT64 Prefix	SNAT Pool	SNAT Mode	Port Range	Dest. Address Translated to	Hit Count	Description	Operati	
		IPv6Subnet	Dynamic N AT-PT	IPv6-subne	OA-server-IP	any	Mapping-from -IPv4-to-IPv6	Mapping-from-IPv6Su bnet-to-IPv4	pat	11001-12000	10.51.212.10	1 Clear		C Edit

8.1.7 Configuration Example of Stateless NAT64 Networking

1. Applicable Products and Versions

Table 8-5 Products and Versions

D	evice Type	Device Model	Version
Fi	irewall	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.

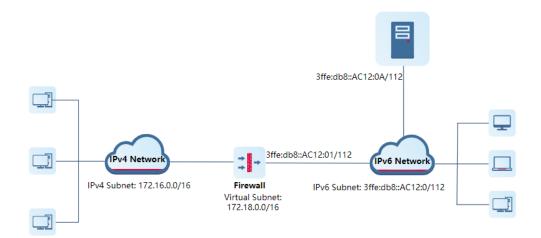


Table 8-6 Key Configuration Points in the Network Diagram

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	0.0.0255.255.255.255

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
 - 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 Stateless NAT64 Rule

🛕 Caution

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

a 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 							
Name	I	IP Address/Range	Address Group	Description			
IPv4-all	(0.0.0.0-255.255.255.255	-	-			
IPv4net-dst		172.18.0.0/16	-	-			
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 🔟 De	elete 🖸 Refresh			
Name	I	P Address/Range	Address Group	Description
IPv6net-dst	t 3	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	k Create NAT64 Prefix				
	* Name	nat64stl-src			
* 🚺 🕅	NAT64 Prefix	3ffe:db8::			
Ρ	refix Length	96 ~			

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	nat64-stl
Enabled State	• Enable 🔿 Disable
Description	Enter the NAT policy description.
Packet Before NAT	
* Src. Address	IPv4net-src ~
* Dest. Address	IPv4net-dst \lor
* Service	any ~
Packet After NAT	
① NAT Mode	• Stateless NAT64 O Static NAT-PT O Static NAT64
* NAT64 Prefix	nat64stl-src v 🕙 🛈 Create NAT64 Prefix
	IP Address NAT Tool
	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.

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 S	Security Policy					
Basic Info						
* Name	permit-IPv4-to-IPv6					
Enabled State	• Enable 🔿 Disable					
* Policy Group	Default Policy Group \lor \odot Add Group					
* Adjacent Policy	Default Policy \lor Before \lor					
Description	Enter the security policy name desc					
Src. and Dest.						
* Src. Security Zone	any					
* Src. Address						
User/User Group	Select a user.					
* Dest. Security						
Zone	*					
* Dest. Address	IPv6net-dst \lor					
Service						
Service	Select a service.					
Time Dange						
Time Range						
Time Range	e any \checkmark \odot Add One-Off Time Plan \odot Add Cyclic Time Plan					
Action Settings	;					
Action Option	n 💿 Permit i Deny					
Content	Security					
Intrusion Prevention	 Enable Disable Add Intrusion Prevention Template 					
Virus Protection	rotection 🔿 Enable 💿 Disable 🕀 Add Virus Protection Template					
URL Filtering	9 C Enable • Disable • Add URL Filtering					
Advanced	Settings					
	Save					

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 S	ecurity Policy
Basic Info	
* Name	permit-IPv6-to-IPv4
Enabled State	• Enable O Disable
* Policy Group	Default Policy Group \lor \odot Add Group
* Adjacent Policy	Default Policy \lor Before \lor
Description	Enter the security policy name desc
Src. and Dest.	
* Src. Security Zone	any \lor
* Src. Address	IPv6net-dst \lor
User/User Group	Select a user.
* Dest. Security	any \lor
Zone	
* Dest. Address	IPv4net-src ~
Service	
Service	Select a service.
Арр	
Арр	Select an application. \vee
Time Range	
Time Range	any \lor \odot Add One-Off Time Plan \odot Add Cyclic Time Plan
Action Settings	
Action Option	• Permit O 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	Settings
	Save

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.

50	ssion 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	
	WOIE	
	Protocol:ICMP	App:Echo-request
		App:Echo-request Outbound Interface:Ge0/3
	Protocol:ICMP	
	Protocol:ICMP Inbound Interface:Ge0/2	Outbound Interface:Ge0/3

 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	dress	User/User Group	Dest. Security Zone	Dest. Address	Service	Арр	Time Range	Action	Content Security	Hit Count	Hit Session	Operation
✓ Def	fault Policy (Group												
	6	permit-IPv	t-src	any	any	IPv6net-dst	any	any	any	Permit)	6 Clear	View Details	Edit Delete
			nermit-l	Pv4-to-IPv6										

• 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.)

• Cre		Delete 🖪 Copy	 Enable 	O Disable	Move	S Clear Hit Record	d 😋 Refresh				Enter a rule	name. C
	Packet Before NAT Packet After NAT											
	Name	NAT Mode	Src. Address	Dest. Address	Service	NAT64 Prefix	Src. Address Translated to	Dest. Address Translated to	Dest. Port Number Translated to	Hit Count	Description	Operation =-
	nat64-stl	Stateless NAT64	IPv4net-src	IPv4net-dst	any	nat64stl-src				4 Clear		C 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.

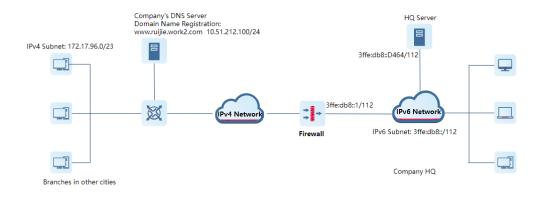


Table 8-8	Key Configuration Points in the Network Diagram

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	0.0.0255.255.255.255

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
 - 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 Static NAT64 Rule
 - a 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 🔟 De	lete C Refresh			
Name	I	P Address/Range	Address Group	Description
IPv4-all	(0.0.0.0-255.255.255.255	-	-
IPv4net-dst		10.51.212.100	-	-
IPv4net-src		172.17.96.0/23	-	-

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			
 Oreate ☑ Delete ☑ Refresh 						
Name	I	P Address/Range	Address Group	Description		
IPv6-webS	erver	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.

< Back Create NAT64 Prefix							
* Name	natpt-src						
* () NAT64 Prefix	2ffe:db8::						
Prefix Length	96 ~						

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 IPv4net-access-IPv6Server
Enabled State 💿 Enable i Disable
Description Enter the NAT policy description.
Packet Before NAT
* Src. Address IPv4net-src \lor
* Dest. Address IPv4net-dst \lor
* Service any \checkmark
Packet After NAT
NAT Mode Stateless NAT64 Static NAT-PT Static NAT64
* NAT64 Prefix natpt-src \lor \bigcirc Create NAT64 Prefix
* Dest. Address 3ffe:db8::D464
Translated to
Dest. Port Number Enter the port number after NAT.
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 S	ecurity Policy
Basic Info	
* Name	permit-access-IPv6Server
Enabled State	Enable
* Policy Group	Default Policy Group \lor \bigcirc Add Group
* Adjacent Policy	Default Policy \lor Before \lor
Description	Enter the security policy name desc
Src. and Dest.	
* Src. Security Zone	any \lor
* Src. Address	IPv4net-src \lor
User/User Group	Select a user.
* Dest. Security	any \lor
Zone	
* Dest. Address	IPv6-webServer v
Service	
Service	Select a service.
Арр	
Арр	Select an application. \sim
Time Range	
Time Range	any \checkmark \odot Add One-Off Time Plan \odot Add Cyclic Time Plan
Action Settings	
Action Option	• Permit O Deny
Conte	ent Security
Intrusion Prevention	 Enable • Disable • Add Intrusion Prevention Template
Virus Protection	 Enable • Disable • Add Virus Protection Template
URL Filtering	 Enable O Disable O Add URL Filtering
Advanced	Settings
	Save

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.

2	ession Description	X
	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

 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.)

	Priority	Name	ne Src. Address	User/User Group	Dest. Security Zone	Dest. Address	Service	Арр	Time Range	Action	Content Security	Hit Count	Operation
 Defa 	ault Policy	Group											
	7	permit-acc	IPv4net-src	any	any	IPv6-webSer	any	any	any	Permit)	7 Clear	Edit Delete
			permit-access-IPv6Serve	er 👘									

• 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			Descriptio	
			Src. Address	Dest. Address	Service	NAT64 Prefix	Src. Address Translated to	Dest. Address Translated to	Dest. Port Numb er Translated to	Hit Count	n	Operation ≡~	
	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

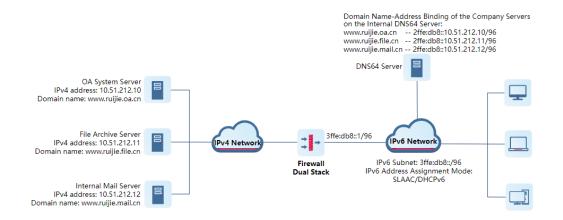
Table 8-9Products and Versions

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.



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:FFFFFFFFFF

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	,
⊕ Create 🔟 D	elete 🕻 Refresh			
Name		IP Address/Range	Address Group	Description
DNS64-pu	blic-IPv6-prefix	2ffe: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	
🕀 Create 🔟 De	lete 😋 Refresh			
Name	I	P Address/Range	Address Group Des	scription
IPv4Server	1	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	Create NAT64 Prefix					
* Name	DNS64-IPv6-prefix					
* 🕕 NAT64 Prefix	C 2ffe:db8::					
Prefix Length	96 v					

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 Po	ck Edit NAT Pool					
* Name	Mapping-from-IPv6Subnet-to-IPv4					
Description	Enter the description.					
* () IP Address/Range	172.16.10.100-172.16.10.139					

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 permit-IPv6net-access-IPv4Server
Enabled State 🧿 Enable 🔷 Disable
Description Enter the NAT policy description.
Packet Before NAT
* Src. Address IPv6-subnet-1 \sim
* Dest. Address DNS64-public-IPv6-prefix \sim
* Service any \checkmark
Packet After NAT
1) NAT Mode O Dynamic NAT-PT O Dynamic NAT64
* NAT64 Prefix DNS64-IPv6-prefix \lor \odot Create NAT64 Prefix
* Translate Src. Mapping-from-IPv6Sut \lor \oplus Add Address Pool
Address to Address
SNAT Mode O NO-PAT O PAT
* ① Port Number 11001-12000 ③
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 S	ecurity Policy
	Basic Info	
	* Name	permit-IPv6net-access-IPv4Server
E	nabled State	Enable Disable
*	Policy Group	Default Policy Group \lor \odot Add Group
* Ad	ljacent Policy	Default Policy \sim Before \sim
	Description	Enter the security policy name desc
Si	rc. and Dest.	
* Src. S	ecurity Zone	any ~
*	Src. Address	IPv6-subnet-1 \vee
User	r/User Group	Select a user.
* D	Dest. Security	any ~
	Zone	
* D	est. Address	IPv4Server V
	Service	
	Service	Select a service.
	Арр	
	Арр	Select an application. \checkmark
	Time Range	
	Time Range	any $\ \odot$ Add One-Off Time Plan $\ \odot$ Add Cyclic Time Plan
Act	ion Settings	
A	ction Option	• Permit O Deny
	Content	Security
Intrusio	n Prevention	○ Enable • Disable • Add Intrusion Prevention Template
Viru	us Protection	○ Enable O Disable O Add Virus Protection Template
I	URL Filtering	○ Enable • Disable • Add URL Filtering
	Advanced	Settings
		Save

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

 \otimes

::a33:d40a
1.212.10
0/2
n established
D)

 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.)

	Pri	ority	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		IРvб-subne	any	any	IPv4Server	any	any	any	Permit		4 Clear	Vie	C Edit Delete
			_	permit-IPv6net-acce	ss-IPv4Server										

• 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.)

			Packet Before NAT			F	acket After NA	т			
perm	Name hit-IPv6net-access-IPv4	NAT Mode	Src. Address	Dest. Address	Service	NAT64 Prefix	SNAT Pool	SNAT Mode	Port Range	Dest. Address Translated to	Hit Count
	permit-IPv6ne	Dynamic NAT64	IPv6-subnet-1	DNS64-public-IPv6-prefix	any	DNS64-IPv6- prefix	Mapping-from -IPv6Subnet-t o-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.

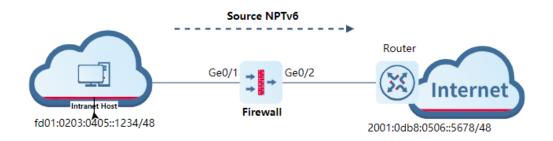


Table 8-12 Key Configuration Points in the Network Diagram

ltem	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

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
 - 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 NAT66-Source NPTv6 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					
 Generate I Delete Generate Create Create Create Create Cre								
Name	I	IP Address/Range						
src-before-	NATv6 1	fd01:203:405::/48						
IPv6-all	:	:						

b 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 NAT	66
NAT Mode	
NAT Mode	• Source NPTv6 O Destination NPTv6
Basic Info	
* Name	src-fd01-NPTv6
Enabled State	• Enable O Disable
Description	Enter the NAT policy description.
Packet Before NAT	
* Src. Address	src-before-NATv6 \lor
* Dest. Address	IPv6-all ~
* Service	any \lor
Packet After NAT	
* 🕕 NPT Info	2001:db8:1:: 48 ©
	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 S	ecurity Policy
	Basic Info	
	* Name	permit-src-before-NPTv6
E	nabled State	• Enable O Disable
*	Policy Group	Default Policy Group \lor \odot Add Group
* Ad	jacent Policy	Default Policy V Before V
	Description	Enter the security policy name desc
Si	c. and Dest.	
* Src. S	ecurity Zone	any \lor
*	Src. Address	src-before-NATv6 \lor
User	/User Group	Select a user.
* C	est. Security	any \lor
	Zone	
* [est. Address	IPv6-all ~
	Service	
	Service	Select a service.
	Арр	
	Арр	Select an application.
	Time Range	
	Time Range	any \lor \odot Add One-Off Time Plan \odot Add Cyclic Time Plan
Act	ion Settings	
A	ction Option	• Permit O Deny
	Content	Security
Intrusio	n Prevention	Enable Disable Add Intrusion Prevention Template
Viru	us Protection	○ Enable O Disable O Add Virus Protection Template
	URL Filtering	○ Enable
	Advanced	Settings
		Save

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

 \bigotimes

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.

Se	ession Description		(\times)
	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	
		Session State:connection established	

• 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.)

	Priority	Name	Src. Address	User/User Group	Dest. Security Zone	Dest. Address	Service	Арр	Time Range	Action	Content Security	Hit Co	ount
~ De	fault Policy	Group											
	9	permit-src	src-before	any	any	IPv6-all	any	any	any	Permit		1 Cl	lear
		_	permit-src-before-N	PTv6									

• 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.)

Name	NAT Mode	Packet Before NAT		Packet After NAT	Hit Count	Status	
Name	NAT Mode	Src. Address	Dest. Address	Service	NPT Info	Hit Count	Status
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

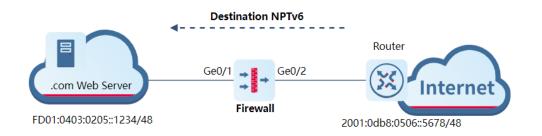
1. Applicable Products and Versions

Table 8-13	Products	and	Versions
		ana	101010110

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.



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

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
 - 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 NAT66-Destination NPTv6 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
🕒 Create 📋 🛙	Delete 🖸 Refresh		
Name		ID Address (Dawns	
Name		IP Address/Range	
dst-prefix-	after-NPTv6	fd01:403:205::/48	
dst-prefix-	before-NPTv6	2001:db8:102::/48	
IPv6-all		::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	

b 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 NAT	66		
NAT Mode			
NAT Mode	○ Source NPTv6	/6	
Basic Info			
* Name	dst-NPTv6-access-WebServer		
Enabled State	• Enable 🔿 Disable		
Description	Enter the NAT policy description.		
Packet Before NAT			
* Src. Address	IPv6-all ~		
* Dest. Address	dst-prefix-before-NPTv6 ~		
* Service	any \vee		
Packet After NAT			
* () NPT Info	fd01:403:205::	48 .	

- 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 C	reate S	ecurity Policy
Ва	asic Info	
	* Name	permit-IPv6-access-WebServer
Enabl	led State	• Enable O Disable
* Polic	cy Group	Default Policy Group \lor \odot Add Group
	nt Policy	Default Policy \checkmark Before \checkmark
	scription	Enter the security policy name desc
		Enter the security poincy name desc
Src. ai	nd Dest.	
* Src. Secur	rity Zone	any \checkmark
* Src.	Address	IPv6-all ~
User/Use	er Group	Select a user. V
* Dest.	Security	any \checkmark
	Zone	
* Dest.	Address	dst-prefix-after-NPTv6 \vee
	Service	
	Service	Select a service.
	Арр	
	Арр	Select an application.
	e Range	
Tim	ne Range	any \lor \odot Add One-Off Time Plan \oplus Add Cyclic Time Plan
Action	Settings	
Action	n Option	Permit O Deny
(Content 9	ecurity
Intrusion Pre	evention	 Enable • Disable • Add Intrusion Prevention Template
Virus Pr	rotection	 Enable • Disable • Add Virus Protection Template
URL	Filtering	Enable • Add URL Filtering
۵	dvanced	Settings
		Settings
		Save

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

(X)

6. Verification

Session Description

 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.

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					
More Protocol:IP	App:Echo-RequestV6				
	App:Echo-RequestV6 Outbound Interface:Ge0/2				
Protocol:IP					
Protocol:IP Inbound Interface:Ge0/3	Outbound Interface:Ge0/2				
Protocol:IP Inbound Interface:Ge0/3 Forward Packets:5	Outbound Interface:Ge0/2 Forward Bytes:300				

 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.)

	Priority	Name	Src. Address	User/User Group	Dest. Security Zone	Dest. Address	Service	Арр	Time Range	Action	Content Security	Hit Count
~ (efault Policy	Group										
	10	permit-IPv	IPv6-all	any	any	dst-prefix-aft	any	any	any	Permit		8 Clear
			permit-IPv6-acces	ss-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.)

Name	NAT Mode		Packet Before NAT		Packet After NAT	Hit Count	Status	
Name	NAT Mode	Src. Address	Dest. Address	Service	NPT Info	Hit Count	Status	
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.

Port N	Port Mapping												
🕒 Cre	eate 🕕 Delete	🗄 Сору 🥝	Enable	Disable 📵	Move 🔇 Cl	ear Hit Record	C Refresh			Enter a rule na	ame.		
	Name	Intranet Address	Intranet Port	Extranet Address	Extranet Port	Protocol	Src. Security Zone	Description	Hit Count	NAT Loopback	Operation	≡~	
							No Data						

(3) Configure port mapping.

< Back Add Port Ma	pping O Example	
Basic Info		
* Name	Enter the name.	
Description	Enter the description.	
Mapping Info		
* Intranet Address	Enter the intranet address.	
* Intranet Port	Example: 1 or 1-65535	
* Extranet Address	Enter the extranet address.	
* Extranet Port	Example: 1 or 1-65535	
* Protocol	Select a protocol.	
* Src. Security Zone	any \vee	
NAT Loopback	Onte: If the service provided by an i	intranet device needs to be accessed using a public IP address or domain name, NAT loopback needs to be enabled.
		Save

Item	Description	Remarks				
Basic Info	1	l				
Name	Name of a part mapping policy	[Example]				
Name	Name of a port mapping policy.	port_map				
Description	Description of a port mapping policy.	-				
Mapping Info	1	1				
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				
		Enter a single port number or port number range.				
Intranet Port	Intranet port number to be mapped to, which is the port number of the destination intranet server.	The number of configured intranet ports must be the same as that of the configured extranet ports.				
		[Example]				
		80 or 2-80				
Extranet	Extranet IP address used to receive requests	[Example]				
Address	from an extranet.	200.10.10.10				
		Enter a single port number or port number range.				
Extranet Port	Extranet port number used to receive requests from an extranet.	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.



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.

o 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.

o 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.

o Fraggle

Attack principle/characteristics: By making a simple modification of the smurf attack, fraggle uses UDP reply packets instead of ICMP packets (attack ports 7 (echo) or 19 (chargen)).

o 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.

o 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.

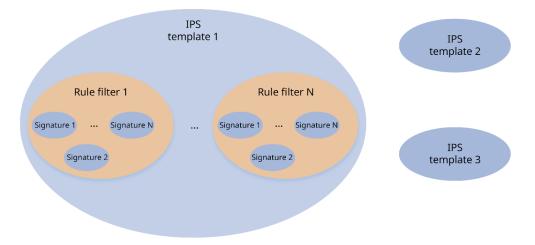
The IPS function of Z-S series firewalls is implemented using templates. Different templates can correspond to different signatures. You can customize the templates according to your needs. In addition, the device is delivered with a built-in "predefined template" that has been strictly verified.

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.

Ruffie Z Series Firewall	≙ Home	Network & Object Policy System	n 🚳 Network Discovery Network Mgm	Quick Onboarding Policy Wizard Customer Service admin
(I) Address	Custom Template	Predefined Template		
	C Refresh			
I URL Category	C Refresh			
👼 Service	Name	Description	Reference	Operation
📇 Time Plan	client	客户端防护	0	QView Details Copy View Filter Results
🙍 ISP Address Library	server	服务端防护	0	R View Details Copy View Filter Results
\textcircled{B} User Authentication \rightarrow				
E Certificate	mining	挖矿专项防护	0	RView Details Copy View Filter Results
Content Template 🛛 🗸				
Intrusion Prevention				
Virus Protection				
URL Filtering				
Security Rule Base				

• 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:

- o Default Action: All traffic that hits the signature is processed using the actions of the signature.
- o Alarm: Alarms are reported for all traffic that hits the signature, ignoring the actions of the signature.
- o 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	0	Enable	0	Not Enabled	mining	Action:	Default A $ \smallsetminus $	Add Intrusion Prevention Template
Virus Protection	0	Enable	0	Not Enabled	default	Action:	Block \lor	Add Virus Protection Template
URL Filtering	0	Enable	0	Not Enabled	⊕ Add UR	L 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 <u>8.9</u> <u>Configuring SSL Proxy Policies</u>.

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 Se	curity (Af	ter being	enabled, t	he followi	ng config	urations or	ily ta	ke effect for IPv4 traffic.)
In	trusion Prevention 🧿	Enable	O No	t Enabled	mining	Action:	Default A	· ~	Add Intrusion Prevention Template
	Virus Protection 🧿	Enable	O No	t Enabled	default	Action:	Block	~	Add Virus Protection Template
	URL Filtering 🔘	Enable	 No 	t Enabled	⊕ Add UR	RL 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.

Ruffe Z Series Firewall	ය Home	nitor 🕀 Network	,₽= Object	Policy	⊖ System	Net	🖗 work Discovery	🕲 Network Mgmt	1 Quick Onboarding	Ø Policy Wizard	Customer Service	<u>م</u> admin
Security Policy	DoS/DDoS At	tack Defense										
 Port Scan Traffic Learning 	⊖ Create ∨	🛅 Delete 🥝 En	able 🚫 Dis	sable 🖪 Ba	asic Protocol Packet Cor	itrol C Refres	h			Enter a na	me or source	
	Against DoS/DDoS e Against DoS/DDoS	me Defens	e Type At	tack Src. Zone	e Src. Address	Dest. Address	Defense (Config	Descriptio	n	Operation	
DoS/DDoS Attack Defense						No Data						
ARP Attack Defense Local Defense												
Local Defense Threat Intelligence												
ു Blocklist and Allowlist												
Reputation Center												
SSL Proxy >												

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

The system displays the Add Src. Defense Against DoS/DDoS page.

< Back Add Src. Defense	e Against DoS/DDoS			
Basic Info				
* Name				
Enabled State	Enable Disable			
Description		6		
Protected Host Range				
* Attack Src. Zone	Select	✓ ④ Add	d Security Zone	
* Src. Address	Select the source address.			
* Dest. Address	Select the destination address.			
Defense Config				
Scan Attack Types	Select Defense Types			
	Selected Defense Types: SYN Flood Attack	Defense, L	JDP Flood Attack Defense,ICMP Flood Attack D	efense,ICMPv6 Flood Attack Defense
DoS/DDoS				
Action After Detecting Attacks	Log Block			
Advanced Defense				
Packet-based Attack	All			
	Teardrop Attack Defense		Control IP Packets with Source Routes	Control IP Packets with Record Routes
	Smurf Attack Defense		ICMP Redirect Attack Defense	ICMP Unreachable Attack Defense
	LAND Attack Defense		WinNuke Attack Defense	Fraggle Attack Defense
	Large ICMP Packet Attack Defense	1500		
Filtering out IPv6 Packets with	Select			
Specific EHs				
			Save	

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

ltem	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 Ra Range of the attac	ange ck source associated with the policy. The policy ta	kes 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	1	
Scan Attack Types	3	
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

ltem	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)	1
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 Defens	e	1
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.

Ruffe Z Series Firewall	☆ Home	Monitor	Network	,₽≟ Object	Policy	System	Netw	ጫ vork Discovery	🛞 Network Mgmt	L Quick Onboarding	Policy Wizard	ဂြ Customer Service	ې admin
Security Policy	DoS/DD	oS Attack	Defense										
Port Scan Traffic Learning		e 🗸 🖻 🛙	Delete Sena	able 🚫 Di	isable 🖪 B	lasic Protocol Packet Co	ntrol 🖸 Refresh				Enter a na	ime or source	
	Against DoS/DD se Against DoS/DI	ame	Defense	e Type A	ttack Src. Zon	e Src. Address	Dest. Address	Defense (onfig	Description		Operation	
DoS/DDoS Attack Defense							No Data						
ARP Attack Defense													
Local Defense Threat Intelligence													
அத Blocklist and Allowlist													
🐻 Reputation Center													
l SSL Proxy →													

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

The system displays the Add Dest. Defense Against DoS/DDoS page.

< Back Add Dest. Defen	se Against DoS/DDoS		
Basic Info			
* Name			
Enabled State	• Enable 🔿 Disable		
Description			
Protected Host Range			
* Attack Src. Zone	Select ~	Add Security Zone	
* Src. Address	Select the source address. $\qquad \lor$		
* Dest. Address	Select the destination address. $\qquad \qquad \!$		
Defense Config			
Dest. Defense Against	Selected Defense Types: SYN Flood Attack D	efense,UDP Flood Attack Defense,ICMP Flood Attack Defense	se,ICMPv6 Flood Attack Defense
DoS/DDoS			
Action After Detecting Attacks	✓ Log 🗌 Limit		
Advanced Defense			
Packet-based Attack	All		
	Teardrop Attack Defense	Control IP Packets with Source Routes	Control IP Packets with Record Routes
	Smurf Attack Defense	ICMP Redirect Attack Defense	ICMP Unreachable Attack Defense
	LAND Attack Defense	WinNuke Attack Defense	Fraggle Attack Defense
	Large ICMP Packet Attack Defense 150	00	
Filtering out IPv6 Packets with	Select ~		
Specific EHs			
		Save	

(3)	Sat the parameters related to DeS/DDeS attack defense poli	01/
(3)	Set the parameters related to DoS/DDoS attack defense poli	Cy.

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 Ra	nge	1
Range of the attac	k source associated with the policy. The policy t	akes 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	1	
Dest. Defense Aga	inst 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.

ltem	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.

Custom Template	te Predefined	Template Adva	anced Settings			
➔ Create	elete 🕄 Refresh					Enter the keyword.
Name		Description		Reference		Operation
			No	o Data		
Back Add Intrus	ision Prevention Te	mplate				
Basic	: Info					
* Template N						
Descrip * Rule F						
	Create					
		Object	Severity	Protocol	Threat Type	Operation
		00,000	Sereiny		incut type	operation
				No Data		
共 0						
≣ ∓ Advanced Setti	tings					
				Save		

(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.

 \otimes

Back Add I	Intrusion Preventic	on Template				
	Basic Info					
* Temp	plate Name					
[Description					
*	Rule Filter					
	⊕ Create 🔟 Dele	ete				
	Name	Object	Severity	Protocol	Threat Type	Operation
				No Data		
				No Data		
	共0祭					
≣ ∓ Advance	d Settings					
				Save		

Add Rule Filter

* Name			
* Object	All Server Client		
* Severity	All High Medium	🗌 Low 🗌 Tip	
Protocol	To-be-selected (5) Select All Enter the keyword. DNS HTTP TCP TLS UDP	Selected (0)	Clear
Threat Type	To-be-selected (93) Select All Enter the keyword. Brute Force DDOS Deserialization Event Monitor Information Leakage Injection Attack	Selected (0)	Clear
	Cancel	Confirm	

- Name: Customized. You are advised to configure a name that can describe the filter function.
- o Object: Objects to be protected.
- **Severity**: Defense severity. For example, if only **High** is selected, only the security rules with high severity can hit the filter.
- o Protocol: Protocols to be detected. The protocol traffic that is not specified does not hit the filter.
- **Threat Type**: Types of threats to be detected. The threat traffic that is not specified does not hit the filter. If you have no special protection requirements, select all.
- 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.

≣ ↑ Advanced	Advanced Settings									
	If a rule is excluded, the action of its signature has the highest priority.									
E	Excluded Rule Settings									
	Select or enter data. O Add									
	1 Added	Action	Clear							
	ImageMagick server request for fake vulnerability (CVE-2016-3718)(4325	Block Alert Permit Default Signature Action	۵							

- 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	Se	curity <mark>(Af</mark> t	er b	eing enabled, the following configurations only take effect for IPv4 traffic.)
Intrusion Prevention		Enable	0	Not Enabled ips Action: Default A 🗸 🕢 Add Intrusion Prevention Template
Virus Protection)	Enable	0	Not Enabled ③ Add Virus Protection Template
URL Filtering)	Enable	0	Not Enabled ③ Add URL Filtering

Ruffie Z Series Firewall		r 🕀 Network 🔑 Object 😨 Policy 💿 System	1	🖗 😵 Network Discovery Network Mgmt	Quick Onboarding	Policy Wizard	Customer Service add
P Address	Security Rule Ba	ase					
중 App 쯟 URL Category	🛛 Enable 🚫 Dis	able O Add Search Criteria				Enter an	ID or a name. Q
🚭 Service	Rule ID	Defense Name	Threat Type	Threat Subtype	Severity	Action	Operation
🖶 Time Plan 🔍 ISP Address Library	4259841	D-LINK DIR-615 cross-station request for			 Medium 	Alarm	View Details
図 ISP Address Library ② User Authentication >	4259842	Western Digital mycloud NAS CSRF vuln			• High	Block	View Details
문 Certificate >	4259843	Wiki Cross Site Request Forgery Attack (c	-		• High	Block	View Details
Content Template	4259844	Easy hosting control panel Cross Site Req	-		 Medium 	Alarm	View Details
Security Rule Base	4325377	ImageMagick server request for fake vul			 Medium 	Alarm	View Detail
	4325378	WordPress Print My Blog Plug-in Code Pr			• High	Block	View Detail
	4325379	Weblogic SSRF vulnerability (cve-2014-4	-	-	 Medium 	Alarm	View Detail
	4325380	Weblogic SSRF vulnerability (cve-2014-4	-	-	Medium	Alarm	View Detail
	4325381	Avtech DVR device server side Request F	-	-	Medium	Alarm	View Details
	4325382	VMware vrealize SSRF vulnerability(cve-2		-	 Medium 	Alarm	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.



(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.

IPv4 Allowlist	Pv6 Allowlist IPv4 Bloc	klist IPv6 Block	ilist Tempora	ry IPv4 Blocklist Tem	porary IPv6 Block	list
⊖ Create 🔟 Delete	C Refresh C Set Bloc	king Duration				Enter an
No. IP	Туре	Adding Time	Blocking D uration	Remaining Blocking Duration	Source D	escription
			No Da	ta		

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 <u>8.9</u> 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.

Ruífie Z Series Firewall		⊕ Network P= Object			M Network Discovery	🛞 Network Mgmt	L Quick Onboarding	Policy Wizard	Customer Service	ې admin
(문) Address	Custom Template	Predefined Templat	e							Q
図 URL Category 勇 Service	Oreate ☐ Delete	C Refresh						Enter the k		
🖶 Time Plan	Name Name	Protocol	Upload	Download	Descrip	otion	Reference		Operation	
🖉 ISP Address Library				No Data	1					
B User Authentication >										
🗄 Certificate >										
Content Template 🛛 🗸										
Intrusion Prevention										
Virus Protection										
URL Filtering										
Security Rule Base										
< Back Ac	dd Virus Pro	otection T	emplate							
	Basic Info	,								
* 1	Femplate Name	Enter the	e template nan	ne.						
	Description	Enter the	e template des	cription.						

* Templa	te Name Enter the templa	ate name.		
De	scription Enter the templa	ate description.		
Sca	an Mode			
Sc	an Mode 💿 Quick Scan	 Deep Scan 		
Prot	tocol			
	Protocol Type	Upload	Download	
	FTP	~	×	
	HTTP	✓	~	
	POP3		\checkmark	
	SMTP	✓		
≣ ∓ Advanced	Settings			
			5	Save

- 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.

Conten	t Sec	urity <mark>(Af</mark> t	ter be	ing enabled, the following configurations only take effect for IPv4 traffic.)	
	_		_	Not Enabled	
Virus Protection	0	Enable	0	Not Enabled test Action: Block Virus Protection Template	
URL Filtering	0	Enable	0	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.

Static ARP Entry List	Proxy ARP	Anti-ARP Spoofing	Anti-ARP Rate Limit			
🕒 Create 📋 Delete	C Refresh		IP	MAC	Interface	Select ~
IP		MAC	Interface	Status	Description	Operation
			No D	Data		

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

(2) Above the operation area, click Create.

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

< Back Add ARP			
* IP			
* MAC			Auto MAC Obtaining
* Interface	Select	~	Auto Interface Discovery
Description			
		1	

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

ltem	Description	Remarks
IP	IP address to be bound to the static ARP entry.	[Example] 192.168.10.3
MAC	MAC address to be bound to the static ARP entry.	 Two configuration methods are supported: Fill in the information manually. Click Auto MAC Obtaining. The device will search for the MAC address matching the IP address according to the available ARP entry information. If no address is found, the system displays "No address is matched." [Example] 11:22:33:44:55:66
Interface	Physical interface to be bound.	 Two configuration methods are supported: Fill in the information manually. Click Auto Interface Discovery. The device will configure the interface that may match the IP address according to the related information. If no interface is found, the system displays "No interface is matched." [Example] Ge0/1

(4) Click **Save** 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.

Static ARP Entry List	Proxy ARP	Anti-ARP Spoofing	Anti-ARP Rate Limit				
Proxy ARP							
↔ Create 🗓 Delete	C Refresh			IP Address/Range		Interface	Select
Start IP		End IP	•	Interface	Status		Operation
			N	o Data			

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

(2) Enable Proxy ARF	(2)	Enable	Proxy	ARF
----------------------	-----	--------	-------	-----

Static ARP Entry List	Proxy ARP	Anti-ARP Spoofing	Anti-ARP Rate Limit				
Proxy ARF							
🕀 Create 🗓 Delete	C Refresh			IP Address/Range		Interface	Select
Start IP		End IP		Interface	Status		Operation
			N	lo Data			

(3) Click Create.

The system displays the Create Proxy ARP page.

< Back Create Proxy A	ARP
* Start IP	
* End IP	
* Interface	Select ~

- (4) Fill in the start IP address and end IP address of proxy and select the proxy interface.
- (5) Click Save to complete the configuration of proxy ARP.

Follow-up Procedure

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

3. Configuring Anti-ARP Spoofing

Application Scenario

The firewall periodically sends gratuitous ARP broadcast packets to allow terminals on the same network segment to obtain the correct MAC address of the firewall, thus preventing attackers from forging the gateway.

Procedure

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

Static ARP Entry List	Proxy ARF	þ	Anti-ARP Spoofing	Anti-	ARP Rate Limit
Anti-A	RP Spoofing (
* ① Gateway MAC Broadcas	st Interval (s)	30			
			Save		

- (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.

Static ARP Entry List	Proxy ARP	Ant	ti-ARP Spoofing	Anti-ARP Rate Limit
* ARP Request I	Rate Limit (pps)	100		
* ARP Reply I	Rate Limit (pps)	100		
		Save		

(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.

Ruijie Z Series Firewall				우= Object 🚭	Policy ©				M Network Discovery	S Network Mgmt	E Quick Onboarding	Ø Policy Wizard	ဂြ Customer Service	ې mbe
(i) Security Policy >	Loca	l Defense												
n Port Scan	• 0	reate 🛅 🛙	Delete 🕝 Enable	S Disable	 Move 	Z Local Def	ense					Enter the	keyword.	
응합 NAT Policy >		Priority	Name	Src. Security	Zone	Src. Address	Dest. Address	Service	Action		Description		Operation	
Security Defense DoS/DDoS Attack Defense		1	limit_local	any		any	any	local_service,icmp,i	permit		o the local device, b to 1500 pps per ho		Edit Delete	
ARP Attack Defense		2	deny_all	any		any	any	any	deny	Block all tra	ffic to the local devic	e. 🔵	Edit Delete	
Threat Intelligence														
An Blocklist and Allowlist														
SSL Proxy >														

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

Local	Defense						
🕒 Cre	eate 📋 🛙	Delete 😔 Enable	🛇 Disable 🕕 Move	C Local Defense	е		
	Priority	Name	Src. Security Zone	Src. Address	Dest. Address	Service	Action
	1	limit_local	any	any	any	local_service,icmp,i	permit
	2	deny_all	any	any	any	any	deny

Local Defense	\otimes
 When local defense is of management cannot be configurations become with caution. 	e configured, and existing
Enable Local D	efense 🗾
Confirm	Cancel

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

Basic Info					
* Name					
Enabled State	• Enable O Disable				
Adjacent Policy	Select a policy. V Before		~		
Description					
Src. and Dest.	li li				
Src. Security Zone	any 🛞 🗸 🔿 Ad	d Secu	rity Zone		
Src. Address	To-be-selected (5)		Selected (1)	Clear	
	Select ~ Enter the keyword.		Enter the keyword.		
			any	Ū	
	200.10.10.10 200.10.10.10 lan_users 192.168.1.20				
	172.26.1.116 172.26.1.116				
	TrafficLearni 172.20.37.114				
	PortScan_de 172.20.37.54				
	Add Address O Add Address Group				
Dest. Address	To-be-selected (5)		Selected (1)	Clear	
	Select ~ Enter the keyword.		Enter the keyword.		
	✓ any		any	Ū.	
	200.10.10.10 200.10.10.10				
	lan_users 192.168.1.20				
	172.26.1.116 172.26.1.116				
	TrafficLearni 172.20.37.114				
	Add Address O Add Address Group				

Service

Service	To-be-selected (7	8)		5	Selected (1)	Clear
	Select v	Enter t	he keyword.		Enter the keyword.	
	Service/Group	Protocol		a	iny	Ē
	_	/Service	Port			
	any					
	service_22_T	TCP	22			
	service_443	TCP	443			
	service_2048	ТСР	2048			
	service_2009	ТСР	20099			
		Add Servi	ce Group			
Action Settings						
Action Option	💿 Permit i 🔿 D	eny				
IP-based Rate Limit						
IP-based Rate Limit	● Disable 🛛 E	nable				

(4) Set the parameters of local defense policy.

Name of the local defense policy.	Characters such as `~!#%^&*+\ {};:""/<>? an spaces are not allowed. [Example] policy_1
Whether the policy is enabled in the system.	[Example] Enable
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.	-
Security policy description.	Characters such as `~!#%^&*+\ {};:""/<>? are not allowed.
olicy with source security zone, source addre The policy takes effect when all the four items	
The policy checks the traffic from this zone.	any indicates traffic of all zones. [Example] any
The policy checks the traffic from this address set.	any indicates all addresses. [Example] any
The policy checks the traffic to this address set.	any indicates all addresses. [Example] any
	any indicates all services.
	Whether the policy is enabled in the system. 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. Security policy description. Security policy description. Policy with source security zone, source addres The policy checks the traffic from this zone. The policy checks the traffic from this address set. The policy checks the traffic from this

Action Option	Action taken on the traffic that hits the policy.	[Example] Permit
IP-based Rate	Limit	
IP-based Rate Limit	 Whether to restrict the number of packets that can pass per second in the traffic matching the policy. Disable: not restricted Enable: restricted. The Packets Allowed to Pass Through Each Host (pps) field needs to be set. 	[Example] Disable

(5) Click Save.

Follow-up Procedure

- To delete multiple policies in a batch, select the policies that you want to delete and click **Delete** in the above bar.
- To enable multiple policies in a batch, select the policies that you want to enable and click **Enable** in the above bar.
- To disable multiple policies in a batch, select the policies that you want to disable and click **Disable** in the above bar.
- To adjust the policy priority, click **Move**. The closer a policy is to the front, the higher its priority is in matching.
- Enter the policy names, policy associated objects, full or part of the policy description in the search box to search for the policies. Fuzzy search is supported.

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.

Uplink Packet Rate Limit	New Session Limit	Session Number Limit Policy
Uplink Packet Rate Limiting		
Global Per-IP Rate Limiting ①		
Global Per-IP/IPv6 Uplink Limit (pp	s) 0	Save
Rate Limiting on Designated IP		
 ⊕ Create Im Delete Im Delete	resh	
IP	Limi	t (pps)
		No Data

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

- b Click Save.
- Rate Limiting on Designated IP Addresses
 - a Click Create.

Uplink Packet Rate Limit	New Session Limit	Session Number Limit Policy	
Uplink Packet Rate Limiting)		
Global Per-IP Rate Limiting ①			
Global Per-IP/IPv6 Uplink Limit (pp	s) 0	Save	
Rate Limiting on Designated IP			
 ⊕ Create Image: Delete Image: Create Image: Creat	fresh		
□ IP	Lim	it (pps)	Operation
		No Data	

b Configure rate limiting on a designated IP address.

< Back Create Rate Limiting on Designated IP		
* IP	Enter a rate limiting ip.	
* Uplink Limit (pps)	Enter 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.

Uplink Packet Rate Limit	New Session Limit	Session Number Limit Policy
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.

Uplink Packet Rate Limit	New Session Limit	Session Number Limit Policy	
New Session Suppression			
Global New Session Limiting ①			
Global New Session Connections/		Save	
New Session Limiting on Design • Create • Create • Create • Create			Enter an IP address.
IP	New	v Session Number Limit/s	Operation
		No Data	Consult

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.

Uplink Packet Rate Limit	New Session Limit	Session Number Limit Policy	
New Session Suppression)		
Global New Session Limiting ①			
Global New Session Connections,	/s 0	Save	
New Session Limiting on Design	nated IP		
← Create ☐ Delete Create	afresh		Enter an IP address.
□ IP	Nev	v Session Number Limit/s	Operation
		No Data	Consult

b Configure new session limiting on designated IP addresses.

< Back	Create Rate Limiting on New Sessions of Designated IP		
	* IP	Enter a rate limiting ip.	
* New	Session Number Limit/s	Enter New Session Number Limit/s	

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.

Uplink Packet Rate Limit New Session Limit Session Number Limit Policy						
Session Number Limit Policy						

(3) Click Create.

Uplink Packet Rate Limit	New Session Lir	nit Session Num	ber Limit Policy						
Session Number Limit Policy									
🔁 Create 🚺 Delete 🧔	Enable Oisable	Move Refrest	Sclear Hit Record		Custom Field				Q
Priority Na	ame Src. Addre	ss Dest. Address S	ervice App	User	Time Range	Total	Session Limit	Per-IP Session Limit	Hi
					No Data				

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

Back Create Session Num	ber Limit Policy	
Basic Info		
* Name		
* Enabled State	• Enable 🔿 Disable	
Description		
Src. and Dest. Addresses		
* Src. Address	any \vee	
* Dest. Address	any \lor	
Service		
Service	any \sim	
Арр		
Арр	any	
User		
User/User Group	any \lor	
Time Range		
Time Range	Select ~	⊙ Add One-Off Time Plan ⊙ Add Cyclic Time Plan
Total Session Limit		
* (i) Total Session Limit	0	
Per-IP Session Limit		
* () Per-IP Session Limit	0	
Action Settings		
Action Option	🔿 Alarm 💿 Block	

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

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

(5) Click Save.

Follow-up Procedure

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

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.

1 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.

Intelligence Management	
Threat Intelligence	

(2) Click to enable the TI function.

	n ()	you want to enable defense.	
Basic Config to Security Zone Identification Threat Intelligence Defense ① Select the th	a n C	you want to enable defense.	
to Security Zone Identification Threat Intelligence Defense () Select the th	e	you want to enable defense.	
Threat Intelligence Defense		rou want to enable defense.	
Select the the select the sele		ou want to enable defense.	
	hreat intelligence types for which y	ou want to enable defense.	
🔽 AllType	e 🔿 Deny 🖸	Alarm	
✓ Trojan		Alarm	
Vorm		Alarm	
Malwar	re 🔿 Deny 🖸	Alarm	
CnC	🔿 Deny 🤇	Alarm	
GrayWa	-	Alarm	
Proxy	_ , _	Alarm	
Phishin	ng 🔿 Deny 🖸	Aidm	

(1) Set the parameters of TI.

Item	Description	Remarks
Function Status	 Current status of the TI function Unauthorized: The TI function license is not activated for the device, or the device cannot communicate with Ruijie Secure Cloud Platform. 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. 	The status is displayed automatically according to the current TI function status. [Example] Normal
Basic Config		
Auto Security Zone Identification	 Whether to identify the traffic inbound and outbound security zones automatically. After this function is enabled, the device automatically identifies the inbound and outbound security zones (ingress and egress) of traffic, and determines whether to perform threat signature matching for the traffic. If this function is disabled, you can manually specify the effective security zones for TI. 	[Example] Enabled
Effective Security Zone	After the effective security zone is specified, the system performs TI matching and processing (block or alarm) for the traffic only when the outbound security zone of the traffic is the same as the specified zone.	When Auto Security Zone Identification is disabled, this parameter needs to be configured. [Example] untrust
Threat Intelligence D	befense	
Туре	Select the TI type to defend against.	Select to enable defense. [Example] APT
Action	 Action to be taken on the traffic matching the TI: Deny: Block traffic and record a security log. Alarm: Not block traffic, but record a security log. 	[Example] Deny

(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.

telligence Management	Custom Threat Intelligence	Excluded Threat	Intelligence Search	
Create 🗇 Delete	aport 🚺 Export 🥥 Enable 🚫 I	Disable C Refresh		SearchiP or Domain Name
Name			Intelligence Quantity	Operation
test1			1	Edit Delete
test2			0	Edit Delete

(2) Click **Create** to enter the Create Custom Threat Intelligence Type page.

istom Threat Intelligence Type
EnterThreat Intelligence TypeName
• Enable 🔿 Disable
IP or Domain Name

(3) Set the parameters of custom TI.

ltem	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.	 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.

Intelligence Management	Custom Threat Intelligence Exclu	uded Threat Intelligence Search	
🕀 Create 📋 Delete 🚺 Impo	ort 🖸 Export 🥥 Enable 🚫 Disable	C Refresh	SearchIP or Domain Name
Name		Intelligence Quantity	Operation
test1		1	Edit De
test2		0	Edit De

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

Import			\otimes
	d CSV Template D d XLSX Template	ownload XLS Templat	e
Import	Select a file.		Browse
	ОК	Cancel	

(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		\otimes
	ad CSV Template Download XLS Temp ad XLSX Template	late
Import	Select a file.	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.

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

< Back EditException Type							
* Name	default						
 IP or Domain Name 	IP or Domain Name						

(3) Set the parameters of excluded threat.

ltem	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.

1 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.

Intelligence Manag	gement	Custom Threat Intelliger	nce E	xcluded Threat	Intelligence Search
Query Mode	 Keywor 	d 🔾 File			
Query Content	IP or Doma	in Name	Search		

(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.

Intelligence Mana	gement	Custom Threat Intellig	jence	Excluded Threat	Intelligence Search
Query Mode	 Keywor 	rd 🔾 File		_	
Query Content	www.a.com		Search		

(3) Click **Search** and wait for the system to return the query result.

Intelligence Mana	gement	Custom Threat Intelligence	Excluded Threat	Intelligence Search	
Query Mode	Keywor	rd 🔾 File			
	- ,	Searc	_		

- Importing a File for Batch Query
- (1) Choose Policy > Security Defense > Threat Intelligence > Intelligence Search.

Intelligence Mana	agement	Custom Threat Intelligen	ice	Excluded Threat	Intelligence Search
Query Mode	 Keywo 	rd 🔿 File			
Query Content	IP or Doma	in Name	Search		

- (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.

Product Cookbook

Intelligence Man	agement	Custom Threat Intelligence		Excluded Threat	Intelligence Search
Query Mode	🔿 Keywa	ord O File			
Select File	Select a fil	e. Br	rowse	Search	
	Download C	SV Template Download XLS Tem	plate	Download XLSX Ter	mplate

- (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**.

Intelligence Mana	agement	Custom Threat Intelliger	nce	Excluded Threat	Intelligence Search
Query Mode	🔿 Keywo	rd 💿 File			
Select File	test.csv		Browse	Search	
	Download CS	V Template Download XLS 1	Template	Download XLSX Ter	mplate

(6) Wait for the system to return the query result. The result is displayed in a list at the bottom of the page.

Intelligence Man	agement	Custom Threat Intelliger	nce	Excluded Threa	at	Intelligence Search
Query Mode	🔘 Keywo	rd 💿 File				
Select File	example.xl	sx	Browse	Search ①		
	Download CS	V Template Download XLS 1	Template	Download XLS>	(Tem	plate
Query Result						
	🚺 Export	Intelligence Source	All	``	/	Enter the keyword. Q
	Intelligence	e Int	elligence S	Source		Operation
	192.168.1.2	No	hit			View Details on Ruijie Secure Clou
	10.48.40.40	No	hit			View Details on Ruijie Secure Clou
	www.a.com	No	hit			View Details on Ruijie Secure Clou
	10 ~	/ Page Total:3				Go to 1 < 1 >

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.

Eq.	oort 😋 Refr	esh 🚺 Export All						Search Criteri	a Enter an IP a	ddress or a po	rt number. O
arch	Criteria: Time:	2023-12-13 00:00:00 2023-1	2-13 23:59:59 Seve	rity: High, Medium, Low × Cle	bar						
o.	Severity 🗘	Security Event 🗘	Log Type	Attack Type 🗘	Defense Rule 🗘	Time ‡	Src. Address 🗘	Dest. Address 🗘	() App 🗘	Action	Operation ≡~
	• High	EICAR-Test-File	Virus Protect ion	Malware	o	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 Protect ion	Malware	0	2023-12-13 11:16:11	2001:db8:1::2	2001:db8:3::2	HTTP-BROWSE	Permit	View Details
	• High	EICAR-Test-File	Virus Protect ion	Malware	0	2023-12-13 11:16:03	2001:db8:1::2	2001:db8:3::2	HTTP-BROWSE	Permit	View Details
ŀ	• High	EICAR-Test-File	Virus Protect ion	Malware	0	2023-12-13 11:15:44	2001:db8:1::2	2001:db8:3::2	HTTP-BROWSE	Permit	View Details
	• High	EICAR-Test-File	Virus Protect ion	Malware	0	2023-12-13 11:15:25	2001:db8:1::2	2001:db8:3::2	HTTP-BROWSE	Permit	View Details
	• High	EICAR-Test-File	Virus Protect ion	Malware	0	2023-12-13 11:15:06	2001:db8:1::2	2001:db8:3::2	HTTP-BROWSE	Permit	View Details
	• High	EICAR-Test-File	Virus Protect ion	Malware	o	2023-12-13 11:10:10	2001:db8:1::2	2001:db8:3::2	HTTP-BROWSE	Permit	View Details
	• High	EICAR-Test-File	Virus Protect ion	Malware	0	2023-12-13 11:09:51	2001:db8:1::2	2001:db8:3::2	HTTP-BROWSE	Permit	View Details
	• High	EICAR-Test-File	Virus Protect ion	Malware	0	2023-12-13 11:09:32	2001:db8:1::2	2001:db8:3::2	HTTP-BROWSE	Permit	View Details
0	• High	EICAR-Test-File	Virus Protect	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		\otimes
Custom-Custom Intelligence	→ Dest.	xclude
Src. Security Zone: trust	Dest. Security Zone: zone4	
	2	
Src. IP: 203.0.114.2	Dest. IP: 203.0.113.2	
Src. Port: 58281	Dest. Port: 80	
MAC: 52:54:00:d8:1b:81	App: ApplicationBeingIdentified	
User:		
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: Os	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 <u>9.3.2 Querying Security Logs</u>.

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 <u>8.6 Keyword Filtering</u>.

Procedure

- (1) Choose Object > Content Identification Lib. > Keyword Set.
- (2) Click Create.

Keyword Set				
🕒 Create 🛍 Delete 😋 Re	fresh			Enter the keyword.
Name	Text	Description	Reference	Operation
		No Da	ita	

(3) Configure a keyword set.

Back Add Keywo	ord Set
Basic Info	
* Name	Enter the value.
Description	Enter the value.
* Text	Enter the value.
	4
	Separate multiple keywords using line breaks.

C	-	
	d١	/e

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 <u>8.5</u> 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 <u>3 License</u> 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.

Predefined URL Category	Custom URL Category		
redefined URL Category ≡	Q URL Category Query	© Refresh	Enter the keyword. Q
BE Popular	Name	Description	Reference
IE Leisure	Portal-Navigation	Web portals and websites that provide content navigation, including governme	1 View
E Information	Search Engine	Web search engines, such as Google, and industry search engines	1 View
E Unsavory	Online Shopping	C2C, B2B, and B2C online shopping websites, online stores, online transaction	1 View
HE 17	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.

defined URL Category	Custom URL Category	
Create 🔟 Delete 🔍 UR	RL Category Query	
Name	URL	Descriptio
		No Data

(3) Enter URL category information.

Save

< Back Create Cu	ustom URL Category
Basic Info	
* Name	Enter Name
Description	Enter Description
1) URL	Enter URL

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

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

Follow-up Procedure

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

Custom U	IRL					
 Create 	📋 Delete	Q URL Category Query	URL Categor	y Query	\otimes	er the keyword.
	Name	URL	URL	Enter a URL, Search		Operation
				No data Disable		
10 ~ / F	Page Total:0					Go to 1 🔨 1 🗲

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 <u>8.12</u> Security Policy.

Precautions

- To detect HTTPS-based URLs, you need to configure an SSL proxy policy. For details about SSL proxy, see
 <u>8.9</u> 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.

Custom Ter	mplate Predefi	ined Template				
⊕ Create	Delete C Refree	sh			Ente	r the keyword. Q
	Name	URL Allowlist	URL Blocklist	Description	Reference	Operation
	test		10.51.213.60	test1	-	Edit Delete Copy

(3) Enter URL filtering template information.

< Back Create UI	RL Filtering				
	5				
Basic Info					
* Template Name	Enter Name				
Description	Enter Description				
Blocklist and					
Allowlist					
① URL Allowlist	Allowlists take precedence	over blocklists.	① URL Block	dist Allowlist	is take precedence over blocklists.
URL Filtering	Name	🔿 Permit 🕕	🔿 Alarm 🕕	O Block ()	
	> Popular	0			
	> Business-Economy	0			
	> IT	•			
	> Information	0			
	> Leisure	•			
	> Life	0			
	> Policy-Law	0			
	> Science-Art	0			
	> House	•			
	> Transportation	•			
	> Unsavory			•	
	Uncategorized	•			

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

Item	Description	Remarks
URL Allowlist	After a URL is added to an allowlist, the device directly permits traffic that accesses the URL. URL allowlists take precedence over URL blocklists. Note: Multiple URLs can be entered. A URL can contain the wildcard character (*). Enter one URL per line. Press Enter to separate lines. If a URL contains the pound sign (#), the sign and the string after the sign do not take effect for matching. For example, if www.test.com/#123 is configured, all the domain names that start with www.test.com/ will be matched. If a URL contains the characters http:// or https:// , these characters will be automatically removed during matching. If an IPv6 address is configured as a URL, the input format	[Example] www.abc1.com
URL Blocklist	should be [<i>IPv6 address</i>]. For example, [2001::1] . After a URL is added to a blocklist, the device directly blocks traffic that accesses the URL. The input format is the same as that for the URL allowlist.	[Example] www.abc2.com
URL Filtering		
URL Filtering	Set processing actions for different URL categories: Permit: Permit traffic that accesses the URLs of the specific categories. Alarm: Permit traffic that accesses the URLs of the specific categories and generate an alarm log. Block: Block traffic that accesses the URLs of the specific categories and generate an alarm log.	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 <u>8.12</u> <u>Security Policy</u>.

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 <u>3 License Activation</u>.

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.

Custom Template	Predefined Template					
C Refresh					Enter the keyword.	Q
Name	URL Allowlist	URL Blocklist	Description	Reference	Operation	
default	-		Default profile. Block unsav	-	Сору	

b Click a template name to view URL filtering details.

< Back URL Filte	ring Details				
Basic Info					
* Template Name	default				
Description	Default profile. Block uns	avory.			
Blocklist and Allowlist					
() URL Allowlist	Allowists take precedence	e over blocklists.	() URL Block	list Allowlis	ts take precedence over blocklists.
URL Filtering	Name	🔘 Permit 🕕	🔿 Alarm 🕕	O Block ()	
	> Popular	•			
	> IT	0			
	> Information	0			
	> Leisure	0			
	> Business-Economy	0			
	> Life	0			
	> Policy-Law	0			
	> Science-Art	0			
	> House	0			
	> Transportation	•			
	> Unsavory			•	
	Uncategorized	0			

- (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.

Custom Template	Predefined Template				
C Refresh					Enter the keyword.
Name	URL Allowlist	URL Blocklist	Description	Reference	Operation
default			Default profile. Block unsavory.		Сору

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 <u>8.12</u> <u>Security</u> <u>Policy</u>.

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

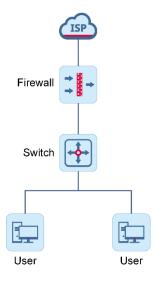
2. Service Demands

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.

Ruijie Z Series Firewall	🔓 Home 🛛 Ø Monitor ⊕ Netwo	rk 🔑 Object 🛛 영 Policy 🔞 System	m 🖗 🛞 Network Discovery Network Mgmt	€
匣 Address	App Custom App A	.pp Group		
App Content Identification Lib.	Арр Туре	C Refresh		google
Service	BE HTTP	Name	Type App Group	Reputation
🕑 Region	BE InstantMessaging-APP	Hume	type http://www.	Level
🖶 Time Plan	8 InstantMessenger	✓ HTTP	Default -	Low 0
ISP Address Library	8 InternetFileTransfer	 SearchEngines 	Default -	Low 0
B User Authentication >	81 IP-Voip	Google	Default -	Low 0
E Certificate	B≣ LearningEducation	 Web-Application 	Default -	Low 0
Content Template >	BE NetworkStorage	Google-Earth	Default -	Low 0
	DE Manue Mandia			

Ruijie Z Series Firewall		S Monitor	Network	& Object	🛛 Policy	System		Netwo	nk Discovery	🛞 Network Mgmt	Quick Onboarding	Policy Wizard	Customer Service	ې admin
1 Address	Арр	Custom A	рр Арр	Group										
Pp App	Арр Туре			C Refresh							ус	utube		۵
Service	BE Social	I-Media		Name			Туре		App Grou	þ		Reputa Level	ition Referen	nce
🗞 Region 🖶 Time Plan				✓ Social-N	Media		Def	fault	-			Low	0	
				YouT	ube		Def	fault	-			Low	2 View	N

• 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**.

Ruijie Z Series Firewall	습 Home 🛛 Monitor	rk 🔑 Object 🛛 🗟 Polic	y 🕲 System	M Network Discovery	⊗ Network Mgmt	1 Quick Onboarding	Policy Wizard	ဂ Customer Service	ې admin
[편] Address	Predefined URL Category	Custom URL Category							
	Predefined URL Category =	Q URL Category Query	Refresh			e-i	mail		
Keyword Set	B≣ IT	Name		Description			Reference		
URL Category		E-mail		Websites that provide e-mail service	25				
چ service ک Region									

To further confirm whether the website to be blocked is in this category, you can enter the website name.

Product Cookbook

Ruffe Z Series Firewall	☆ Home ⓒ Monitor ⊕ Network	은 Object 🛛 🖓 Po	olicy 🕸 System	(ጫ Network Discovery	⊗ Network Mgmt — Q	ick Onboarding Policy Wizard Customer Service	<u>ې</u> admin
[편] Address	Predefined URL Category	Custom URL Catego	ry				
Image: App Image: Content Identification Lib.	Predefined URL Category =	Q URL Category Qu	Jery C Refresh				
Keyword Set	BE Popular	URL Categor	v Query		\otimes	Reference	
URL Category	B Business-Economy	one categor	y query		i		
통 Service ይ Region	81 IT	URL	gmail.com	Search			
Time Plan	8E Leisure	Category	E-mail		.		
Q ISP Address Library	8≣ Life						
B User Authentication >	8 Policy-Law				•••		
📳 Certificate >	BE Science-Art						
Content Template	81 House						
Security Rule Base	B Transportation						
	8E Unsavory		Disable				Consult

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.

Ru	ijie Z Series Firew	all 🖒 Home	Ø Monitor	Metwork	은 Object	🖾 Poli	icy 😂 Syst	tem		Q Searc
8	Security Policy 🗠	Security Po	licy							
	Policy Config Wizard	Policy Group		≡	⊕ Create	Batch	Operation ~	More V 📿 Refree	sh 🗔 Custom	Field
	Security Policy				•	J				
	Policy Optimization	⊕ A	dd Policy Group	0	Pri	iority	Name	Src. Security Zone/I nterface	Src. Address	Src. Regi
	Policy Life Cycle	Keyword		Q	_			nterrace		
۵	Port Scan				 Default 	Policy G	roup			
60	Traffic Learning	All Groups		^		1	Long-Con	any	any	any
		間 (9) Default	t			2	sslvnn c2s		Inneal Tast1	

(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

Гір			\otimes
Are you sure	you want to add i	it in the simul	ation space?
simulation helps you		ies and issues in	
	Do Not Show	This Again	
	Simulation Space	Create]
simulation helps you	i identify vulnerabiliti void risks to services	ies and issues in in actual execu ^r This Again	n policies in advance

- (3) Configure the basic information of the security policy.
 - 0 Enter a policy name, for example, **BlockYoutube**.
 - Retain the default Enable state for Enabled State. 0
 - Set Policy Group to Default Policy Group. You can select a custom policy group as required. 0
 - Set **Priority** as required. A policy at the top of the list indicates a higher matching priority. 0

* Name	BlockYoutube		
Enabled State	Enable		
* Policy Group	Default Policy Group	~	⊕ Add Group
* Priority	Long-Connection	~	Before v
Description	BlockYoutube		

(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	any	~
Zone/Interface		
* Src. Address	any	\sim
Src. Region	any	~
Dest. Security	any	\sim
Zone/Interface		
* Dest. Address	any	~
Dest. Region	any	\sim
Service	any	~
Action Option	🔾 Permit 💿 Deny	
	App、User、Effective Time $ \smallsetminus $	

- (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.

 \otimes

To-be-selected (7207)	Selected (1)	Clear
Select V youtube	Enter app or app g	oup name.
 Social-Media YouTube 	YouTube	ī
Add App Group O Add Custom App		

- (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	any \checkmark	
Zone/Interface		
* Src. Address	any \vee	
Src. Region	any \lor	
Dest. Security	any ~	
Zone/Interface		
* Dest. Address	any \vee	
Dest. Region	any \lor	
Service	any \vee	
Арр	YouTube \lor	
User	any \vee	
Effective Time	any 🗸	⊕ Add One-Off Time Plan ⊕ Add Cyclic Time Plan
Action Option	🔿 Permit 💿 Deny	
	Fold A	
		Save

(9) After configuration, click Save.

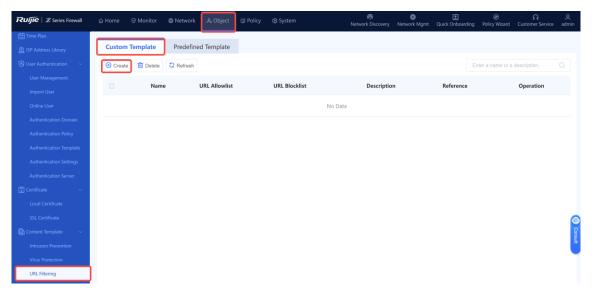
• Blocking a Custom Website Through URL Filtering

- (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.

Ruffe Z Series Firewall	습 Home 🛛 Monitor	🖶 Network	ہے Object	영 Policy 🛭 영 System	ක Network Discovery
먣 Address	Back Edit Cust	om URL Categ	Jory		
 App 	Basic Info				
Keyword Set	* Name	ruijie			J
URL Category	Description	Enter Description			
- Service	① URL	*.ruijie.com.cn			
🖉 Region		ruijie.com.cn *.ruijie.com			
🛗 Time Plan		ruijie.com			
🙊 ISP Address Library					
B User Authentication >					

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**.

Product Cookbook

Ruffe Z Series Firewall	습 Home 🛛 Ø Monito	r 🌐 Network	우_ Object 🛛 🖾 Policy	හි System		(ጫ Network Discovery	ଡ଼ Network Mgmt Qu
Address App Content Identification Lib Keyword Set URL Category Be Service Aegion Time Plan Sits P Address Library Ouser Authentication > Sits P Address 2 (2)	Back Create U Basic Info Template Name Description Blocklist and Allowlist URL Allowlist	RL Filtering ruije Enter Description Allowlists take prece	dence over blocklists.) URL Block	dist Allowlist	s take precedence o	ver blocklists.
Content Template Intrusion Prevention Virus Protection URL Filtering Advanced Settings Security Rule Base	URL Filtering	Name Custom Catego ruijie Popular Business-Econo IT Linformation	0	 ▲larm ● ● ●	Block ①		

- (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**.
 - 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.
 - Set **Src. and Dest.** parameters to any (more specific matching conditions can be configured in actual scenarios) and set **Action Option** to **Permit**.

Ruffe Z Series Firewall	습 Home	N
l Security Policy V	< Back Create Security Policy	
Policy Config Wizard	Basic Info	
Security Policy		
Policy Optimization	* Name Block_ruijie	
Policy Life Cycle	Enabled State Enable	
🚇 Port Scan	* Policy Group Unicy Group Object Obj	
httl Traffic Learning	* Priority BlockYoutube \lor Before \lor	
Traffic Control Policy		
다. NAT Policy >	Description Enter the security policy name descrip	
👜 Port Mapping	Src. and Dest.	
G Security Defense	Cre Coquette	

 Toggle on URL Filtering, set Custom Template to the created URL filtering profile, and set Action to Template Action.

Ruije Z Series Firewall	습 Home 🛛 🛛 Monitor	⊕ Network 🛛 🔑 Object	영 Policy 🔅 System		(ጫ Network Discovery	⊗ Network Mgmt Qui
	* Src. Address	any	~			
Security Policy	Src. Region	Select a URL filtering	template.			\otimes
Policy Optimization	Dest. Security Zone/Interface	Custom Template				
	* Dest. Address	• ruijie				
	Dest. Region	Predefined Template	_			
	Service	O default(Default profile. Bloc				
	Action Option					
			Cancel	Confirm		
			Cancer	Comm		
	Content Security					
	Intrusion Prevention	Disable				
	Virus Protection	Disable				
	URL Filtering	Enable Select a template.	Action: Template Actio	n ④ Add URL Filtering		
	Keyword Filtering	Disable				
	Advanced	Settings				

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.

Ruijie Z Series Firewall	습 Home 🛛 🕞 Monitor	@ Network 은 Object	@ Policy @ System	Q Se
먣 Address	App Custom	App App Group	-	
Pp App	Ocreate ☐ Dele	te C Refresh		
🕏 Service	Name	Category		
🖄 Region	Custom_1723	Custom_1		
🖽 Time Plan 🙊 ISP Address Library				
B User Authentication >				
III o ur i				

(2) Enter the custom application name and category name, and click Create to create an App Rule.

Add Custom App	p				\otimes
* Name	Custom_ Te	est			
Category	• Custom Type	○ Select from	existing categories.		
* Category Name	Custom_ Te	stGroup			
* App Rule					
	Protocol Type	Src. IP	Dest. IP	Dest. Port	Operation
			No D	ata	
	Co	nfirm and Continu	e Adding Confirm	n Cancel	

(3) Set Protocol Type and other parameters based on actual requirements, and click Confirm.

Create Custo	m App Rule	\otimes
Protocol Type	• TCP O UDP	
* ① Src. IP	0.0.0/0	
mber range: 0–65535 * ① Dest. IP ites any port	128.34.21.0/24	
* 🕕 Dest. Port	65535	
	Confirm	

(4) Click **Confirm**. The custom application is created.

Add Custom App)				\otimes
* Name	Custom_ Te	est			
Category	 Custom Type 	○ Select from e	existing categories.		
* Category Name	Custom_ Te	estGroup			
* App Rule					
	Protocol Type	Src. IP	Dest. IP	Dest. Port	Operation
	ТСР	0.0.0/0	128.34.21.0/24	65535	Edit Delete
	Со	nfirm and Continue	Adding Confirm	Cancel	

(5) Set App to the created custom application by referring to the process of creating a security policy.

Src. and Dest.		
Src. Security	any \checkmark	
Zone/Interface		
* Src. Address	any \vee	
Src. Region	any ~	
Dest. Security	any ~	
Zone/Interface		
* Dest. Address	any \vee	
Dest. Region	any \lor	
Service	any ~	
Арр	Custom_TestGroup ~	
User	any 🗸	
Effective Time	any ~	⊕ Add One-Off Time Plan ⊕ Add Cyclic Time Plan
Action Option	O Permit O Deny	
	Fold A	

7. Verification

Check the security policy to verify that the packets match the predefined security policy.

	Priority	Name	Src. Security Zone/I nterface	Src. Address	Src. Region	Dest. Security Zone/I nterface	Dest. Address	Dest. Region	Service	с
✓ Def	fault Policy	Group								
	1	BlockYout	any	any	any	any	any	any	any	

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 <u>8.12</u> Security Policy.

Procedure

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

Keyword Filtering			
OreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreateOreate<			
Name	Description	Reference	Operation
	1	No Data	

(3) Enter keyword filtering template information.

< Back Add Key	yword Fi	lter					
Basic In	nfo						
* Template Nar	me Ente	r the value.					
Descripti	on Ente	r the value.					
* Filter Ru	ule						
	🕀 Create	🔟 Delete					
		Name	Application Protoco	ol Keyword Set	Direction	Action	Operation
					No Data		
Т	īotal: 0						
				Sav	е		

ltem	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 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 <u>8.4.1</u> <u>Configuring a Keyword</u> .	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 <u>8.12</u> 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 <u>8.9 Configuring SSL Proxy Policies</u>.
- 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.

Analysis	Policy

① SSL proxy must be enabled to analyze HTTPS website content.							
③ Create ③ Delete ② Enable ③ Move S Clear Hit Record I C Custom Field C Refresh Enter a name or an analysis template.							
	Policy Name	Analysis Template	Description	Src. Address	User/User Grou p	Hit Count	Operation
	default_reco	default_reco	Analyze common services	any	any	0 Clear	View Delete
	default_all	Analyze All	Analyze all services	any	any	0 Clear	View Delete

(3) Configure an analysis policy.

Back Add Analysis F	Policy	
Basic Info		
* Name	Enter the value.	
Enabled State	• Enable 🔿 Disable	
Description	Enter the value.	
Src. Address		
Src. Address	Select the source address. $\qquad \sim$	
User		
User/User Group	any ~	
Analyze		
Action	 Analyze All Analyze by Template 	e 🔿 Not Analyze
Analysis Template	Template: Select a template. ④ Add Ana	lysis Template
ET Advanced Settings		
Src. Security Zone	Select the source security zone. \sim	
Dest. Security Zone	Select the destination security zone. \checkmark	
Dest. Address	Select the destination address. \sim	
Services and Apps		
Service	Select a service.	
Арр	Select an application.	
Time Range		
Time Range	Select ~	⊙ Add One-Off Time Plan ⊙ Add Cyclic Time Plan
		Save

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	1	1	
Action	 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 S	Settings	1	
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.	
Арр	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 <u>1. Configuring</u> <u>an Analysis Policy</u>.

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.

Analysis Template				
🕒 Create 🛅 Delete	C Refresh			Enter a name or a descriptic
Name	Туре	Description	Reference	Operation
default_reco	Predefine	Analyze common services	1 View	View Delete

(3) Configure an analysis template.

Toggle on or off **C** to enable or disable analysis for a specific type.

< Back Add Analy	ysis Template
Basic Info	
* Template Name	Enter the value.
Description	Enter the value.
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	Z Account, Title, Body, Attachment Name 🗌 Attachment Content
Weibo	
Analysis Content	Z Account, Title, Body, Attachment Name 🗌 Attachment Content
FTP	
Analysis Content	Uploaded/Downloaded File Name
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]
Description		Audit Template
Analysis Types		
URL	Users access web pages.	[Example]
		Enable
IM	Users log in to and log out from IM	[Example]
	software.	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 <u>9.3.4 Querying</u> <u>Behavior Analysis Log</u>.

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.

Advanced Settings		
* ① Maximum Decompressible HTTP Data Size	2048	Bytes
Save		

(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 <u>8.9.3</u> <u>1. Importing SSL Proxy Certificate</u>.

If you select **Protect Server** as the SSL proxy template type, import the server certificate first. For details about server certificate import, see <u>8.9.3</u> <u>2. Importing Server Certificate</u>.

Procedure

- (1) Choose Policy > SSL Proxy > SSL Proxy Template.
- (2) Click Create to enter the Create SSL Proxy Template page.

Ruijie Z Series Firewall	습 Home	G Monitor	Network	P= Object	Policy	System	M Network Discovery	🛞 Network Mgmt	1 Quick Onboarding	Ø Policy Wizard	Customer Service	Q admin
Security Policy	SSL Pro	xy Templa	te									
🖗 Port Scan	• Creat	e 🔟 Delete	e 🖸 Refresh							Enter the		
h Traffic Learning	Creat	Delete	G Refrest									
See NAT Policy >	1	Name	т	Гуре		Server Certificat	te	Des	cription		Operation	
Gecurity Defense >		default	保护	客户端		-	R	(认模板, 适用于用	户上网场景下的流量	代理	Edit Delete	
\mathcal{A}_{a} Blocklist and Allowlist												
Reputation Center												
🎒 SSL Proxy 🗸 🗸												
SSL Proxy Policy												
SSL Proxy Template												
SSL Proxy Allowlist												

(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	Enter the template name.			
Description	Enter the template description.			
Туре	• Protect Client 🛛 Protect Server			

ltem	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.
Туре	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.

Ruijie Z Series Firewall	습 Home 🛛 Monitor 🔀 Network	A≞ Object 😒	Policy 🕞 System	Retwork Discovery	🔕 Network Mgmt	E Quick Onboarding	Policy Wizard	Customer Service	کر admin
먵 Address	SSL Proxy Certificate Serve	er Certificate							
🛞 Арр	⊙ Create 🗇 Delete 🗗 Import	D Befreit						knaword	
図 URL Category	🕑 Create 📋 Delete 🛃 Import	C Refresh							
த Service	Name		Subject Info					Operation	
🛗 Time Plan								View Details	
👰 ISP Address Library	default_ca		C = CN, ST = Fujian, L = Fuzhou, O =	Ruijie, CN = Ruijie			Ċ	Download Delete	
B User Authentication >									
🖺 Certificate 🗸 🗸									
Local Certificate									
SSL Certificate									
Content Template >									
Security Rule Base									

Procedure

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

Ruffie Z Series Firewall	≙ Home ⊘ Monitor ⊕ Net	rork 유 Object	Policy 1	System	Retwork Discovery	🔞 Network Mgmt	Quick Onboarding	Policy Wizard	Customer Service	्र admin
E Address	SSL Proxy Certificate	Server Certificate								
🛞 Арр										
URL Category	🕑 Create 🛅 Delete 🛃 I	nport 🖸 Refres	1					Enter the	keyword.	
🚇 Service	Name			Subject Info					Operation	
🛗 Time Plan									View Details	
🙇 ISP Address Library	default_ca		C =	CN, ST = Fujian, L = Fuzhou, O =	Ruijie, CN = Ruijie				Download Delete	
Output Description										
🖺 Certificate 🗸 🗸										
Local Certificate										
SSL Certificate										
Content Template >										
Security Rule Base										

🚺 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 SS	L Proxy Certificate		\otimes
* Certificate Format	Select a certificate form	at. ~	
* Certificate File	Select a file.	Browse	
* Password	Enter the password.		
	ОК D	isable	
ltem	Description	Remarks	
		The sectificants	

Item	Description	Remarks
Certificate Format	Select the certificate format according to the suffix of the imported certificate file, and you can import certificates in PEM, P12, or CRT format.	 The certificate with the p12 or pem suffix already contains the key. You need to specify the password of the certificate when importing the certificate. The certificate with the crt suffix does not contain a key and a separate key file is required. When you import the certificate, specify the key file and password of the key file. [Example] P12
Certificate File	Imported SSL proxy certificate file.	Click Browse to select a certificate file to be uploaded from the local device.
Key File	Separate key file attached with the certificate.	The certificate file with the crt suffix does not contain a key. You need to upload the key file and specify the password for the key file when importing the certificate.
Password	Password of the key file.	 Certificate with the p12 or pem suffix: You need to specify the password of the certificate when importing the certificate. Certificate with the crt suffix: When you import the certificate, specify the key file and password of the key file.

Follow-up Procedure

• is used to configure whether to trust the SSL proxy certificate. When the icon is red, the certificate is not trusted; when the icon is green, the certificate is trusted. Click the icon to modify the credibility of the

certificate. Only one trusted SSL proxy certificate can exist on the device.

• Download the SSL proxy certificate, and import it into the client to make the client trust it.

SSL P	roxy Certificate Server Certificate		
🕀 Cre	ate 🔟 Delete 🖸 Import 😋 Refresh		Enter the keyword. Q
	Name	Subject Info	Operation

- 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.

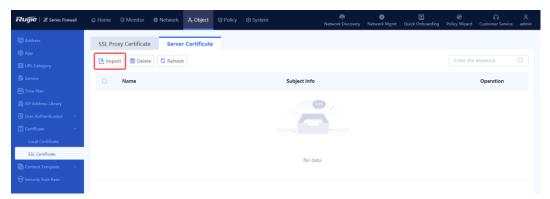
2. Importing Server Certificate

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 Ser	ver Certificate			(\otimes
* Certificate Format	Select a certificate	e format.	~		
* Certificate	Select a file.		Browse		
File					
* Password	Enter the password.				
	ОК	Disab	le		

ltem	Description	Remarks
Certificate Format	Select the certificate format according to the suffix of the imported certificate file, and you can import server certificates in PEM, P12, or CRT format.	 The certificate with the p12 or pem suffix already contains the key. You need to specify the password of the certificate when importing the certificate. The certificate with the crt suffix does not contain a key and a separate key file is required. When you import the certificate, specify the key file and password of the key file. [Example] P12
Certificate File	Imported server certificate file.	Click Browse to select a certificate file to be uploaded from the local device.
Key File	Separate key file attached with the certificate.	The certificate file with the crt suffix does not contain a key. You need to upload the key file and specify the password for the key file when importing the certificate.
Password	Password of the key file.	 Certificate with the p12 or pem suffix: You need to specify the password of the certificate when importing the certificate. Certificate with the crt suffix: When you import the certificate, specify the key file and password of the key file.

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 <u>8.9.2</u> <u>Configuring an SSL Proxy Template</u>.

Procedure

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

SSL Proxy Policy							
🕒 Create 🕅 Delete 🥥 Enable 🛇) Disable 🔞 Move 🔇 Clear Hit R	Record T Custom	Field C Refresh				
Name Src. Security Zone	Src. Address Dest. Security Zo	Dest. Address	Service	Арр	Action	Decryption Config File	Hit Count
			Ģ	4			
			No data				

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

Back Create SSL Pro	oxy Policy
Basic Info	
* Name	Enter the policy name.
Enabled State	• Enable 🔿 Disable
Description	Enter the policy description.
Src. and Dest.	
* Src. Security Zone	Select the source security zone. \sim
* Src. Address	Select the source address. \sim
* Dest. Security Zone	Select the destination security zone. $\!$
* Dest. Address	Select the destination address. \sim
Service	
Service	Select a service. \checkmark
Арр	
Арр	Select an application. \sim
Decryption Settings	
Action Option	 Decrypt Not Decrypt

ltem	Description	Remarks
Basic Info	-	
Name	Name of the SSL proxy policy.	Characters such as `~!#%^&*+\/0::"/<>? and spaces are not allowed. [Example] SSLPolicy_1
Enabled State	Whether to enable the new SSL proxy policy.	[Example] Enabled

ltem	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
Арр	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.

Dom	ain Name Allowlist App Allowlist		
🕒 Cre	ate Delete Schable Scherresh		Enter the keyword. Q
	Name	Туре	Operation
	login.live.com	预定义	Delete
	*.googleapis.com	预定义	Delete
	*.windows.com	预定义	Delete
	*.microsoft.com	预定义	Delete
	*.weixin.qq.com	预定义	Delete
	ssl.ptlogin2.qq.com	预定义	Delete
	xui.ptlogin2.qq.com	预定义	Delete
	passport.baldu.com	预定义	Delete
	wappass.baidu.com	预定义	Delete
	nsclick.baidu.com	预定义	Delete

(3) Enter the domain name and click Save.

< Back	Create Domain Name Allowlist	
* () De	omain Name	Enter a domain name.

2. Application Allowlist

Application Scenario

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

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

Procedure

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

Doma	ain Name Allowlist App Allowlist		
🕑 Ed	iit 🔟 Delete 😋 Refresh		Enter the keyword. Q
	Name	Туре	Operation
	HttpGames	预定义	Delete
	IPVoip	预定义	Delete
	OnlineGames	预定义	Delete
	VideoCategory	预定义	Delete
	SoftwareUpdates	预定义	Delete
	OnlineBankingPayment	预定义	Delete
	VideoconFerencing	预定义	Delete

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

Back Edit App	Allowlist			
* App	To-be-selected (4328)	Select All Se	elected (0)	Clear
	Select v Enter an app or ap	p group nam	Enter an app or app grou	up nam
	▶ □ HTTP			
	▶ □ IPVoip			
	OnlineGames			
	OnlineShopping			
	P2PSoftWare			
	▶ □ InternetFinance			
	Add App Group			

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.

Port Scan			
9	Port scan helps you identify ports and services and quickly cree. Configure the port scan range first. You can immediately start t It is recommended that Class C addresses be scanned and a ma Start Port Scan Port Scan Range @ Not Configu	he scan after completing the configuration, or save th aximum of top 20,000 scan results be exported.	-
(i) The default port policy is all	permit. Select the ports to be denied.		
Add Manually	Create Policy		IP Select IP 🗸
□ IP ‡	Port (Only Describing Well-Known Ports) ≑	Status ≑	Operation
		0	

- (2) (Optional) If the port scan range is not configured, configure it first.
 - a Click Start Port Range.

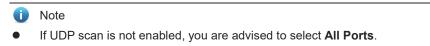
If the system displays "Configure the port scan range first.", click Configure.

	Tip
	• Configure the port scan range first.
	Configure
b	Select or add the IP address to be scanned.
	ter the IP address or range to be scanned in the Add Custom IP Address/Range input box, and click Add add it to the IP Address/Range area.

To quickly add IP addresses, click **Quick Import from Traffic Learning** or **Quick Import from Address Object**.

Set Address Range and Po	rt Range for Scan		ē
Ensure that the firewall is cor	ill take longer scanning time. Select only necessary ports ar nected to the device to be scanned and that scan traffic wil h CPU consumption. Start the scan when the system is idle	Il not be blocked by other security devices such as an I	PS.
Select or Add Addresses for S	can		
* Add Custom IP Address/Range	Enter an IP address, IP range, IP ad Add Ŧ	= Quick Import from Address Object	= Quick Import from Traffic Learning
IP Address/Range			
	Ν	lo Data	
elect or Add Ports for Scan			
	No Custom Ports Save a	Ind Scan Now Cancel	

c Select or add the port to be scanned.



Select or Add Ports for Scan

JDP Scan OYes Ports All Ports	NoCustom Ports			
 Common PortsSelect Custom Ports 	t Common Ports			
Add Custom Port Range	Example: 1 or 1-65535	Add ∓		
		Save	Save and Scan Now	Cancel

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

ltem	Description	Remarks
Ports	 Select the port to be scanned: All Ports: Scan all ports. 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. Select Common Ports to add common service ports. You can click Select Common Ports to select common service ports. Select Custom Ports to add the ports to be scanned. 	[Example] All Ports

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

Confirm the system prompt and click Scan Now.



 Port scan may take a long time and affect device performance.
 You are advised to select an off-peak period to perform

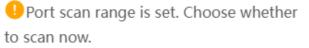
this operation.

Are you sure you want to scan now?



- (3) (Optional) If port scan policy has been configured:
 - a Click Start Port Scan.
 - b Click **Scan Now** to start port scan.

Tip

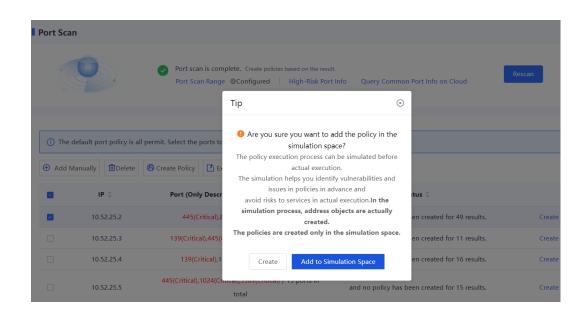


Port scan may take a long time and affect device performance. You are advised to select an off-peak period to perform this operation.



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

Port Sca	in			
	9	Port scan is complete. Create policies based on the result. Port Scan Range @Configured High-Risk Port Inf	o Query Common Port Info on Cloud	Rescan
(i) The	default port policy is al	I permit. Select the ports to be denied.		
🔁 Add M	Manually Delete	Create Policy		IP Select IP ~
•	IP ‡	Port (Only Describing Well-Known Ports) $\ \hat{\downarrow}$	Status 🌐	Operation
	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
	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
	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
	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
	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.

Security Policy												83 Simulation Sp
Policy Group	Ξ	🕒 Crea	te Bat	ch Operation \sim	More ~ C Refre	sh 📴 Custom	Field	Туре	All		Enter a keyv	word. (
 Add Policy G 			Priority	Name	Src. Security Zone/I nterface	Src. Address	Src. Region	Dest. Security Zone/I nterface	Dest. Address	Dest. Region	Servi	Operation
Keyword		∼ Defa	ult Polic	Group								
All Groups BE (2) Default	^		1	chptest	any	any	any	any	any	any	any	C Edit More ~
the cap a could be			2	Default Po	any	any	any	any	any	any	any	Edit More ~

 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

Port Sca	n			
	9	Port scan is complete. Create policies based on the result. Port Scan Range @Configured High-Risk Port Inf	o Query Common Port Info on Cloud	Rescan
① The ↔ Add M		ermit. Select the ports to be denied.		IP Select IP
	IP ‡	Port (Only Describing Well-Known Ports) 🌐	Status ≑	Operation
	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
	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
	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
	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
		139(Critical),445(Critical),2001(Critical) / 11 ports in		
	10.52.25.8	total	and no policy has been created for 11 results.	Create Policy View Details Delete

- 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.

Traffic Learnin	ng			
	Traffic learning provides policy op Enable Traffic Learning	imization suggestions based on learning results. Independent Traffic Learning Address @Not Configured	computing resources are used for analysis. Therefore, fo	rwarding performance is not affected.
Traffic Learning R	tesult Blocking Result			
Create Permit	Policy Create Deny Policy	🖸 Export 🛍 Delete		Enter the destination of Q
	Dest. IP	Port (Only Describing Well-Known Ports)	Src. IP	Operation
		No data		

- (2) (Optional) If the traffic learning address is not configured, configure it first.
 - a Click **Enable Traffic Learning** and click **Configure** in the prompt box to configure the traffic learning address.

Traffic Learning			
Traffic learning provides policy optimization	Tip	uting resources are used for analysis. Therefore, forwardi	ng performance is not affected.
	Configure a traffic learning address first.		
Traffic Learning Result Blocking Result	Configure		
Create Permit Policy Create Deny Policy	Delete C Refresh		Enter the destination of Q
Dest. IP	Port (Only Describing Well-Known Ports)	Src. IP	Operation

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.

Product Cookbook

Set Traffic Learning Addre	ss			⊗ ^{pe}	rformance is not affected.
 Set a destination IP address for number of addresses will take lon 					
select or Add Addresses					
* Add Custom IP Address/Range	Enter an IP address, IP range, IP ad	Add 🐨	⊒ Quick Import from Port Scan Config	En	
			⊒ Quick Import from Address Object		Operation
IP Address/Range	Delete Selected				
		No Data			
	Save	Save and Enable M Cancel			
		No data			

1 Note

To quickly add IP addresses, click **Quick Import from Port Scan Config** or **Quick Import from Address Object**.

- c Choose whether to enable traffic learning immediately according to service situation.
- When services are busy, click **Save** to save the traffic learning address configuration. You can enable traffic learning when services are idle.
- When services are idle, click **Save and Enable Now** to save the traffic learning address configuration and enable traffic learning immediately.
- (3) (Optional) If the traffic learning address has been configured, click **Enable Traffic Learning** to modify the traffic learning address or enable traffic learning immediately.

Traffic Learning			
Traffic learning provides policy optimizatio	Тір	while a set of the set o	Therefore, forwarding performance is not affected.
Enable Traffic Learning Traffi	Traffic learning address is set. Choose whether to enable traffic learning now.		
Traffic Learning Result Blocking Result	Enable Now Configure		
Create Permit Policy 🔀 Create Deny Policy 🚺 Expo	Cancel		
Dest. IP	Port (Only Describing Well-Known Ports)	Src. IP	Operation

Verification

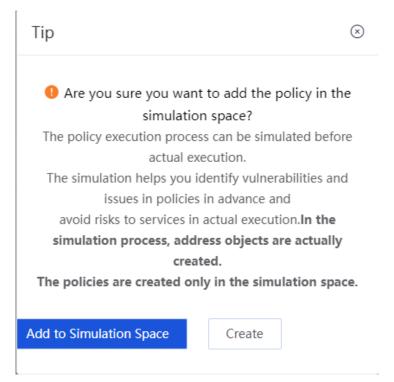
• To view the information about learned IP addresses and ports, click the **Traffic Learning Result** tab. To view the detailed access relationship, click **View Details**.

	Result Blocking Result	🚺 Export 🗴 🖬 Delete		Enter the destination of Q
	Dest. IP	Port (Only Describing Well-Known Ports)	Src. IP	Operation
	172.20.37.124	443	172.25.22.250 1	Create Permit Policy Create Deny Policy View Details Delete
	172.20.37.124	445(Critical)	172.18.162.108 1	Create Permit Policy Create Deny Policy View Details Delete
10 ~ / Pa	age 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**.

172.20.3	172.20.37.124445)							
🗟 Create P	Create Permit Policy Create Deny Policy 🔟 Delete Create Deny Policy C							
	Src. IP ≑	协议类型 ≑	Status ≑	Operation				
	172.18.162.108	ТСР	Unhandled	Create Permit Policy Create Deny Policy Delete				
10 ~	/ Page Total:1			Go to 1 < 1 >				

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



Insert it to	the specified location.	\otimes
* Policy Name Prefix	LnDeny	
* Policy Group	Default Policy Group \sim	
Policy	port_scan1_PortScan_policy_172.2C $\scriptstyle{\smallsetminus}$	
Before/After the Adjacent Policy	Before 🗸	
	OK Cancel	

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

	Priority	Name	ty	Dest. Addr ess	Service	Арр	Time Rang e	Action	Content Sec urity	Hit Count	Hit Session	Operation
✓ Det	fault Policy	Group										
	1	LnDeny_443		TrafficLear	any	any	any	Den		0 Clear	View Details	Edit Delete
	2	port_scan		PortScan	service_2	any	any	Perm		0 Clear	View Details	Edit Delete
	3	test		any	any	any	any	Perm		0 Clear	View Details	Edit Delete
	4	allow_all		any	any	any	any	Perm		0 Clear	View Details	Edit Delete

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

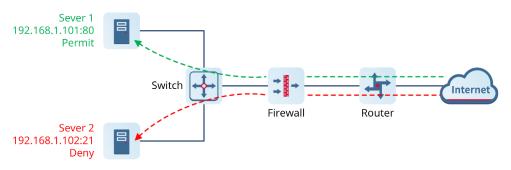
affected.
n oi Q

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	
C 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 C	Cyclic Time Plan				
	Basic Info				
	* Name				
C	Description	k			
* Effective T	ime Range 💿 Full Year 🛛 🔿 Specific Time	Range			
*	Cycle List				
	Cycle	Time Range	Operation		
	Cycle Mon.,Tues.,Wen.,Thur,Fri.	Time Range 10:00:00-23:59:59	Operation Edit Delete		
	Mon.,Tues.,Wen.,Thur.,Fri.				

In addition, Z-S series firewalls can also enforce different security policies for the type of application of traffic. For example, to prevent intranet and extranet users from accessing game apps anywhere, anytime, configure a security policy and associate it with game apps.

App Custom App Ap	pp Group				
Арр Туре	C Refresh			Enter a name.	Q
8E HTTP		_		Reputation	
8 IPVoip	Name	Туре	App Group	Level	Reference
1≣ OnlineGames	~ HTTP	Default		Low	0
8 OnlineShopping	 WebApplication 	Default	-	Low	0
BE P2PSoftWare	HTTP-BROWSE	Default	-	Low	0
BE InternetFinance	HTTP-PROXY	Default	-	Low	0
B≣ InstantMessenger	HTTP-GIF	Default		Low	0
III InstantMessaging-APP	MeituxiuxiuorMeiyan	Default		Low	0
B≣ VideoCategory	MSN	Default	-	Low	0
VideoStreamingMediaSoftware	Firefox	Default	-	Low	0
8≣ HttpVideos	Fast	Default	-	Low	0
8≣ Videos-APP	Wikipedia	Default		Low	0
8≣ VideoLIVE R≣ MusicRoAudio	Google	Default	-	Low	0
B InternetFileTransfer	 QQ Application 	Default		Low	0
NE ProtocolClass	QQ Space	Default	-	Low	0
⊞ InternetofThings	QQ Yedian	Default	-	Low	0
IE RemoteControl					

Through the flexible combination of IP address, port, user, device, time and other parameters, a variety of firewall policies meeting actual network security needs can be configured, so that the user's security policy can be effectively implemented.

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

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.

RUTTE Z Series Firewall	Network	, ዶ= Object - I Policy	System		M Network Discovery	Ø Network Mgmt	(Quick Onboarding	Ø Policy Wizard	G Customer Service	오 admin
Policy Config Wizard		Wele	come to the	Policy Config W	lizard.					Exit
Create Address Diject Divide addresses related to services and create objects to forditate policy configuration. You caninable fraffic Learningon this page to obtain traffic change information and policy optimization suggestions.	*	Create Police You can add or ad policies on this pay You can also perfor port scan to identi and generate recommended pol thus improving pol configuration efficiency.	Ey just ge. rm ify licles,	Sir Sir Sir sin act sin ide an ic ide an ic ic ide sin ic ide sin ic ide sin ic ide sin ic ide sin ic ide sin ic ide sin ic ide sin ic ide sin ic ide sin ic ide sin ic ide sin ide si ide si ide si ide si ide si i i ide si i i i i ide si i i i i i i i i i i i i i i i i i i	Conduct mulation e policy execution cess can be mulated before trut execution. The mulater before truth y culterabilities drawner and avoid is to services in tual execution.	*	Deliver p configura enable p	ation and olicies for defense on		Const

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.

Ruijie	Z Series Firewall	🛆 Home	Ø Monitor	Network	,₽_ Object	Policy	System	Metwork Discovery	🔕 Network Mgmt	Quick Onboarding	Policy Wizard	Customer Service	ي admin
Polic	y Config Wizard												Exit
							-						
	Create Addition	ess Object ···		····· O Create	Policy		Conduct Simulation	O Ex	ecute Policy			sh	
	Create Address Objec	t											
	 An address objective Divide addresse 				acilitate polic	y creation an	d management.						
	IPv4 Address	IPv6 Ad	dress										
							No IPv4 address object						
					After creating ac	ddress objects, j	you can perform port scan and enable traffic learning t	to facilitate policy creation	ın.				
							Create Address Ob						
	 Traffic learning 	helps you obt	ain traffic chan	ge, asset IP ad	dresses, and a	ctive port inf	formation and allows the system to provide mo	re precise defense p	plicies and policy	optimization sugg	estions.		0
	Enable Traffic Learni	ing											Consult

(2) Click Create Address Object.

ate 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
0
No IPv4 address object
After creating address objects, you can perform port scan and enable traffic learning to facilitate policy creation. Create Address Objects
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.
nable 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		\otimes
* Address Object Name	* () IP Address/Range	ŀ
Add IPv6 Address Object		\otimes
* Address Object Name	* () IP Address/Range	1

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

Item	Description	Remarks
IP Address/Range	IP address or range.	 Three configuration methods are supported: IP address: One or multiple IP addresses. Input an IP address per line. Press Enter to separate lines. Example 1: 192.168.20.3 Example 2: 1234::100 IP address range: A contiguous range of addresses. Connect the start IP address and end IP address with a hyphen (-). Example 1: 192.168.20.1-192.168.20.3 Example 2: 1234::100-2345::100 Network segment: IP address network segment Example 1: 192.168.1.0/24 or 192.168.1.0/255.255.255.0 Example 2: 1234::100/100

1 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.

Config Wizard													
Create Address Object			Create Policy			Conduct Simula	ion	O E	ecute Policy			O Finish	
reate Policy													
You can manually create police													
Tou can manually create point	cies or perforr	m port scan to g	guide policy creation.	Next, you can cho	ose to conduct simula	ation before exec	uting policies or directly	execute policies.					
View Simulation Result	cies or perforr	m port scan to ç	guide policy creation.	Next, you can cho	ose to conduct simula	ation before exec	uting policies or directly	execute policies.				Scan Port - Create Po	licy
	cies or perforr	m port scan to ç ⊕ Create			Refresh		uting policies or directly	execute policies.	All	~ E	Enter a keywo		
View Simulation Result	Ξ	Create			Refresh TC Custor	n Field	Dest. Security Zone/	Туре		✓ E	Enter a keywol		
View Simulation Result Policy Group		Create Price	Batch Operation ~	More V Q I Src. Security Zo	Refresh T Custor	n Field	Dest. Security Zone/	Туре				rd. C	

(2) Set parameters related to security policy.

Create Security Policy

a Configure basic information about security policy.

Basic Info			
* Name	Enter the security policy name.		
Enabled State	Enable		
* Policy Group	Select a policy group.	\sim	⊕ Add Group
* Priority	Select a policy.	\sim	Before v
Description	Enter the security policy name desc		

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

Src. and Dest.		
Src. Security	any	~
Zone/Interface		
* Src. Address	any	\sim
Src. Region	any	\sim
Dest. Security	any	\sim
Zone/Interface		
* Dest. Address	any	\sim
Dest. Region	any	\sim

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

ltem	Description	Remarks
Dest. Region	Destination region of the target data connection.	 Click the drop-down list, and select a destination region in the To-be-selected area. The selected region is automatically added to the Selected area. Click Add Custom Region to add a custom region object. [Example] any

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

Service	any	~
App	any	~
User	any	~

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

Effective Time	any	\sim	⊕ 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	0	Permit	0	Deny
---------------	---	--------	---	------

Action	Description
	If the action is set to Permit , the device performs check according to whether content security check is enabled:
Permit	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 Opt	tion		\otimes
Long-Lived Conne	ction Disable	9	
	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.

Set Simulation Duration							
Simulation Duration	1 Hour	~					
ОК	Cancel						

(3) Click OK.

The system automatically performs simulation run for the selected policies.

Create Address Object			Create Policy		• Cond	luct Simulation		O Execute P	olicy		O Finish	
mulation Run												
① The policy execution process car	n be simula	ited before a	ctual execution. Th	e simulation helps you iden	tify vulnerabilities	and issues in po	olicies in advance and avoi	d risks to services	in actual execution	L.		
						ng simulation						
			You can lea	ve this page temporarily and	I perform operatio	ns after the exe	cution result is generated.		Stop Simulation			
View Simulation Result	-	Tarenteen a	The second second		THE REAL PROPERTY.	a di Sama di					- 10	
		Ξ.		e Src. Security Zone/i	Src. Address	Src. Region	Dest. Security Zone/I nterface	Dest. Address	Dest. Region	Service	Operation	
												T

(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							
 Due to capacity lin 	Due to capacity limitations, only the details about the first 100,000 simulation results are recorded.						
Clean	ir Result						
Src. Address	Actual Execution Result	Simulation Result	Hit Count in Actual Exec ution	Hit Count in Simulation	Details		
The actual execution result is the same as the simulation result.							
10 v / Page Tota	al:0			Go	o 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.

Тір	\otimes

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	v This Again	
Sir	nulation Space	Create	

(3) Click Create.

The system displays the Create Security Policy page.

Basic Info		
* Name	Enter the security policy name.	
Enabled State	Enable	
* Policy Group	Select a policy group. \checkmark	
* Priority	Select a policy. \checkmark	Before 🗸
Description	Enter the security policy name desc	
Src. and Dest.		
Src. Security	any 🗸	
Zone/Interface		
* Src. Address	any ~	
Src. Region	any \checkmark	
Dest. Security	any ~	
Zone/Interface		
* Dest. Address	any \vee	
Dest. Region	any \vee	
Service	any \checkmark	
Арр	any ~	
User	any \checkmark	
Effective Time	any \lor	⊕ Add One-Off Time Plan ⊕ Add Cyclic Time
Action Option	• Permit 🔿 Deny	
	Fold A	
Content Security		
Intrusion Prevention	Disable	
Virus Protection	Disable	
URL Filtering	Disable	
Keyword Filtering	Disable	
Advanced	Settings	

(4) Set parameters of security policy.

ltem	Description	Remarks
Basic Info		
Name	Security policy name.	Characters such as `~!#%^&*+\/0::"/<>? 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.	 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/Interf ace	Source security zone or interface initiating the target data.	 Click the drop-down list, and select a source security zone or interface in the To-be-selected area. The selected item is automatically added to the Selected area. Click Add Security Zone to add a custom security zone. [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. Click Add Address or Add Address Group to create an address or address group object. [Example] any

ltem	Description	Remarks
Src. Region	Region initiating the target data connection.	 Click the drop-down list, and select a source region in the To-be-selected area. The selected region is automatically added to the Selected area. Click Add Custom Region to add a region. [Example] CN
Dest. Security Zone/Interf ace	Destination security zone or interface of the target data connection.	 Click the drop-down list, and select a destination security zone or interface in the To-be-selected area. The selected item is automatically added to the Selected area. Click Add Security Zone to add a custom security zone. [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.	 Click the drop-down list, and select a destination region in the To-be-selected area. The selected region is automatically added to the Selected area. Click Add Custom Region to create a custom region object. [Example] CN
Service	Service type of the target data connection request.	 Click the drop-down list, and select a service or service group in the To-be-selected area. The selected service or service group is automatically added to the Selected area. To add a custom service, click Add Service. [Example] any

ltem	Description	Remarks
Арр	Application type of the target data connection request.	 Click the drop-down list, and select an application or application group in the To-be-selected area. The selected application or application group is automatically added to the Selected area. To add a custom application, click Add Custom App. [Example] any
User	The traffic of specified users or user groups matches the policy.	 Click the drop-down list, and select a user or user group in the To-be-selected area. The selected user or user group is automatically added to the Selected area. Click Add User 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.	 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] Intrusion Prevention: Enable Virus Protection: Enable URL Filtering: Not Enabled Keyword Filtering: Enable

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

(5) Click Save.

Follow-up Procedure

- When the security policy, virus protection policy, or intrusion prevention policy is hit, a security log is recorded.
 You can choose 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.

Security Policy												69 Simulation	Space
Policy Group	Ξ	⊖ Creat	e Ba	tch Operation \sim	More ~	C Refresh	Custo	om Field	Type All		✓ Enter a key	yword.	
😌 Add Policy Group			Priority	Name	Use	r Effect	tive Time	Action	Content Security	Hit Count	Hit Session	Operation	
Keyword		✓ Defa	ult Polic	y Group									
All Groups	^		1	chptest	any		any	Permit)	0 Clear	View	Edit More	
Mar (17)			2	Default Po	any		any	Deny)	139 Clear	r View	Edit More ~	

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.

Product Cookbook

Policy Group	=					Custom Fie			Y Enter a	keyword.
		🕀 Crea	te Bat	ch Operation ~	More 🗸 😋 Refresh	Custom Fie	ld Type	All	Enter a	keyword.
🕣 Add Policy Group			Priority	Name	Src. Security Zone/I nterface	Src. Address	Src. Region	Dest. Security Zone/I nterface	Dest. Address	Operation
Keyword		✓ Defa	ault Policy	Group	interface			interface		
All Groups	^									Edit More ~
罰 (2) Default			1	chptest	any	any	any	any	any	Edit More ~
			2	Default Po	any	any	any	any	any	Move to Specific Location
										Move Up One Row
										Move Down One Row
										Тор
										Delete

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.

Policy Optimization			
Policy analysis intelligently idea	ntifies policy issues to provide policy optimization suggestions.	Analyze Policy Last analysis time:2023-03-10 11.23:43	
Issue Policies Ignored Policies			
Ignore C Refresh		Select the issue level. \sim Select the issue type.	 Enter a policy name.
Ssue Level	Issue Type 💠	描述	Operation
Issue Level			Operation



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

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

ssue Policies Ignored Policies Ignore Ignored Refresh		Select the issue level. Select the issue type.	cy name. Q
Issue Level	Issue Type 🌐	Description	Operation
4_To_2_out			Ignore Handle
Minor Issue	Never Matched	The policy never matches a packet.	
〜 default组			Ignore Handle
Minor Issue	Never Matched	The policy never matches a packet.	
✓ allow_all			Ignore Handle
Major Issue	Any Permission	The policy allows data packets to be forwarded from any source to any destination and is improper.	

🚺 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.

H	landle	Issue Poli	су										
	Policy N	lame:4_To_2	out										
	Policy Iss	sues : Neve	r Matched										
	Questio	n Descriptio	on										
	🖻 Desc	cription			1	Impact				🔠 So	lution		
	The polic	cy never mate	hes a packet.		1	Redundant policies occupy the memory of the device and affect device forwarding performance				ect You an condit	You are advised to delete the policy or modify matching conditions of the policy		
											Issue	No./Total:1/	1 Previous Nex
	Optimiz	e Policy									lssue	No./Total:1/	1 Previous Nex
	·		To-be-optin	nized		Optimizati	ion suggestion:	fou are advised	to delete the poli	:y or modify m			
	·		To-be-optin Name	nized Source	First Creation		ion suggestion: ¹ Src. Security Z one	íou are advised Src. Addres s	I to delete the poli Dest. Security Zone	:y or modify m Dest. Addr ess			

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 L	ife Cycle					
🚺 Expo	rt 🖸 Refresh				Eq. Search Criteria	nter the policy name. Q
	Change Time ≑	Change Strategy \Leftrightarrow	Change Type 💠	Account \Rightarrow	User IP 💠	Operation
	2023-03-13 11:43:54	allow_all	Create	admin	172.25.22.250	View Details
	2023-03-13 11:36:32	test	Create	admin	172.20.36.39	View Details
	2023-03-10 12:31:20	allow_all	Move	admin	172.26.36.232	View Details
	2023-03-10 12:30:54	123	Move	admin	172.26.36.232	View Details
	2023-03-10 12:28:27	111	Delete	admin	172.26.36.232	View Details
	2023-03-10 12:25:27	111	Create	admin	172.26.36.232	View Details
	2023-03-09 14:08:59	123	Edit	admin	172.20.36.27	View Details
	2023-03-08 16:22:55	123	Edit	-	-	View Details
	2023-03-08 16:22:23	123	Edit	-	-	View Details
	2023-03-08 10:15:29	123	Move	-	-	View Details

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

Back Change Details			
Operation Info Policy Name: 123	Change Time: 2023-03-09 14:08:59	Account/IP: admin/172.20.36.27	
Change Details			
			Check Changed Items Only
	Policy	Before the Change	After the Change
	Name	123	123
	Policy Group	def-group	def-group
	Priority	1	1
	Description	any	any
Sro	. Security Zone	any	any
	Src. Address	any	any
Des	it. Security Zone	any	any
	Dest. Address	any	any
	Service	any	any
	Арр	any	any
	Time Range	any	any
	Action	Permit	Permit
Intr	usion Prevention	1234-block	<mark>Chang</mark> 1234-alert
V	irus 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.

									융 Simulation Space
Ξ	🕀 Creat	Bat	tch Operation \sim	More ~ 🖸 Refresh	Custom	Field Type	All	∨ Enter a k	eyword. Q
qu		Priority	Name	Src. Security Zone/I	Src. Address	Src. Region	Dest. Security Zone/I	Dest. Address	Operation
	Defe	ult Delle		internace			merioce		
~	♥ Dela	uit Polic	y Gloup						
		1	chptest	any	any	any	any	any	Edit More 🗸
		2	Default Po	any	any	any	any	anv	Edit More ~
	ip Q	Q v Defa	P Create Bat P Priority Create Default Polic 1	Priority Name Default Policy Group 1 chptest	P Create Batch Operation More Create Batch Operation More Create Batch Operation More Create Batch Operation Nore Create Batch Operation More Create Batch Operation Create Batch Operate Create Batch Operation Create Batch Operate	P Priority Name Src. Security Zone/I Priority Name any any	Priority Name Src. Security Zone/I Default Policy Group O Default Policy Group 1 chptest any any any any	Priority Name Src. Security Zone/I Src. Address Src. Region Priority Name any	P Priority Name Src. Security Zone/l nterface Src. Address Src. Region Dest. Security Zone/l nterface Default Policy Group 1 chptest any any any any any any any

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

Simulation Run									Ba
③ Simulation space is inde network.You can apply police								t policies do not tal	ke effect on the real X
				Start Simulation					Reload Policy
olicy Group	Ξ	⊖ Create B	atch Operation 🗸	More 🗸 😋 Refres	h 🖪 Custom	Field Type	All	✓ Enter a key	yword. Q
Add Policy Group Keyword	•	Priority	/ Name	Src. Security Zone/I nterface	Src. Address	Src. Region	Dest. Security Zone/I nterface	Dest. Address	Operation
All Groups	~	∨ Default Poli	cy Group						
BE (2) Default		1	chptest	any	any	any	any	any	🚺 Edit More 🗸
		2	Default Po	any	any	any	any	any	Edit More ~

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

Set Simulation Dura	tio	n	(\times)
Simulation Duration	1	Hour	~
Start Simulation		Cancel	

(5) Click Start Simulation.

The system automatically performs simulation run for the selected policies.

			the polic	ies pass simulat	ion verification to avoid	risks to services			t policies do not tak		
RunningOOMinute (planned duration: Thour) Stop Simulation - You can leave this page temporarily and perform operations after the execution result is generated. Stop Simulation											
						eal Network	-				
olicy Group		• Create	Bate	th Operation ~	More V Refres	h Custom	Field Type	All	← Enter a key	rword. Q	
			Priority	Name	Src. Security Zone/I nterface	Src. Address	Src. Region	Dest. Security Zone/I nterface	Dest. Address	Operation	

(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.

imulation Results	s That Differ from Actual	Execution Results			
Due to capacity limi	tations, only the details about the	e first 100,000 simulation re	esults are recorded.		
Refresh 🔇 Clear	Result				
rc. Address	Actual Execution Result	Simulation Result	Hit Count in Actual Exec ution	Hit Count in Simulation	Details
			•		
		No	o data		

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

Follow-up Procedure

- O&M personnel can copy a currently effective security policy to the simulation space and modify the policy as required. For example, the O&M personnel can add, modify, and delete the policies according to service requirements.
- When the O&M personnel verify that there are no problems with the security policies in the simulation space, they can export the security policies to make them effective and replace the current security policies.

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.

Security Policy									邰 Simulation Space
Policy Group	≡	🕒 Create	Batch Operation \sim	More ~ C Refre	esh 🖸 Custom	Field Type	All	∨ Enter a	keyword. Q
Add Policy Group		Price	Import	ity Zone/I	Src. Address	Src. Region	Dest. Security Zone/I	Dest. Address	Operation
Keyword	Q	 Default 	Basic Protocol Packet F				interface		
All Groups	^		1 chptest	any	any	any	any	any	Edit More ~
BE (L) Deltare in			2 Default Po	any	any	any	any	any	Edit More ~

(3) The system displays a tip.

 Tip
 Image: Constraint 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

 Download CSV Sample File

 Drag the file here, or click Select to select a file.

 Drag the file here, or click Select to select a file.

 If imported configurations conflict with existing configurations,
 OK

 Cancel

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

Note

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

- (5) Drag the configuration file to the upload area or click **Select** to upload the configuration file to the device.
- (6) Configure the method used when data conflicts.

When the imported data conflicts with the existing data, the following processing methods can be used:

- **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.

Security Policy									හි Simulation Spa
Policy Group	≡	🕀 Create	Batch Operation \sim	More ~ 🖸 Refree	ih 🔀 Custom Fie	ld Type	All	∨ Enter a	keyword. Q
🕀 Add Policy Group		Pri	Import Export	ity Zone/I face	Src. Address	Src. Region	Dest. Security Zone/I	Dest. Address	Operation
Keyword		✓ Default	Basic Protocol Packe	t Filtering					
All Groups	^								
8 (2) Default			1 chptest	any	any	any	any	any	Edit More ~
			2 Default Po	any	any	any	any	any	Edit More 🗸

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.

Security Policy											හි Simulation Space
Policy Group	Ξ	📀 Crea	te	Batch Operation 🗸	More ~	C Refres	Custom	Field Type	All	∽ Enter a	keyword. Q
Add Policy Group			Prio	Import Export		ity Zone/I face	Src. Address	Src. Region	Dest. Security Zone/I nterface	Dest. Address	Operation
Keyword All Groups	Q	~ Def	ult P	Basic Protocol Packet	Filtering						
BE (2) Default	^		1	chptest		any	any	any	any	any	Edit More ~
			2	Default Po		any	any	any	any	any	Edit More ~

(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

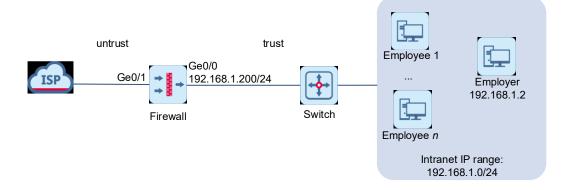
2. Service Demands

In the office scenario shown in <u>Figure 8-6</u>, 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.

Ruffe Z Series Firewall	습 Home	Ø Monitor	Network	₽= Object	I Policy	🕸 System	
☐ Interface ~	DHCP S	Service List					
Physical Interface	DHCP Ser						
Subinterface	DHCF Set	ver					
Bridge Interface	🕒 Creat	te 🔟 Delete	C Refresh				All Protocols
Aggregate Interface						Address Deves (Devfi	Default Gate
Tunnel Interface		Name	Interface	Pro	tocol Type	Address Range/Prefi x	way
圆 Zono							

- 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.
- Allocate IP addresses based on the actual needs. In this example, the 192.168.1.0/24 addresses are allocated.

< Back Create DHCP Serv	ice	
Protocol Type	• IPv4 O IPv6	
Basic Info		
* Name	test	
* ① Interface	Ge0/0(Off 192.168.1.200/24) v	
* 🕕 IP Assignment Range	192.168.1.1-192.168.1.254	
* Subnet	192.168.1.0/24	
* Default Gateway	192.168.1.200	
* Primary DNS Server	8.8.8.8	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	0	Day	1	Hour	0	Minute
Primary WINS Server						
① Option 43	ip v					
① Option 138						
Secondary WINS Server						
Reserved IP Address/Range						
① Binding Host MAC	192.168.1.2	2/d8:9e:f3:3f:c	15:64	1.		
					Save	

d Check whether the DHCP server function is automatically enabled. If it is disabled, manually enable it.

Ruijie Z Series Firewall	습 Home	Ø Monitor	Network	은 Object 🛛 🖾	Policy	© System		Q Search for	r a function	P	⊗ [1 Ø	្ព	0
☑ Interface ∨	DHCP S	Service List												
Physical Interface	DHCP Ser	ver												
Subinterface														
Bridge Interface	🕒 Creat	te 🔟 Delete	Refresh				All Protocols		Enter an inter	face, a su	ibnet ad	Idress or a		2
Aggregate Interface						Address Range/Prefi	Default Gate							
Tunnel Interface		Name	Interface	Protoco	ol Type	x	way	Lease Time	DNS		0	peration		
🕑 Zone		test	Ge0/0	IPv	.4	192.168.1.1-	192.168.1.20	1Hour0Minut	8.8.8.8			dit Delete		
Hand Routing		test	660/0	11-14	/4	192.168.1.254	0	е	0.0.0.0		EC	ait Delete		

- (2) Configuring the IP Address Objects
 - a Choose Object > Address > IPv4 Address and click Create to create an IP address object for employees.

Ruijie Z Series Firewall	ය Home ම Monitor	⊕ Network	Object 🖾 Policy	🕲 System	Q Se	arch for a function
P Address	IPv4 Address IPv4 A	ddress Group	IPv6 Address	IPv6 Address Group	MAC Address	MAC Address Group
 App Content Identification 	🕒 Create 🛅 Delete 😋	Refresh				Enter the keyv
Service	Name	IP Address/	/Range	Address Group	Description	Reference
	ippool_Br0	10.1.1.0/24		-	sslvpn gateway[Br	2 View

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 Addr	ess Object
Basic Info	
* Name	allstaff
Description	
IP Address/Range	
* ① IP Address/Range	192.168.1.1-192.168.1.254
	<i>h</i>
	Save

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.

< Back Add IPv4 Addr	ess Object	
Basic Info		
* Name	boss	
Description		
IP Address/Range		
* (1) IP Address/Range	192.168.1.2	
		Save

After all address objects are created, the following figure is displayed.

IPv4 Address	IPv4 Address Group	IPv6 Address	IPv6 Address Group	MAC Address	MAC Address Group	
🕀 Create 📋 De	elete C Refresh				Enter the ke	yword. Q
Name	IP Addre	ess/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.

RI	DIFIC Z Series Firew	vall 습 Home	Monitor	Network	, ₽_ Object	중 Policy	System		۵	Search for a fun	ction
8	Security Policy \sim	Security Pol	licy								
F	Policy Config Wizard Security Policy	Policy Group		Ξ	🕒 Create	Batch Ope	ration ~ More	∽ 😋 Refre	sh 📴 Custom	Field	Enter a key
	Policy Optimization	⊕ A	dd Policy Group	p							Туре
	Policy Life Cycle	Keyword		Q	Pr	iority N	ama	curity Zone/I terface	Src. Address	Src. Region	Dest. Seci nte
4	Port Scan	All Groups		^	√ Defaul	t 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**.

\otimes
dd it in the simulation ?
can be simulated before tion helps you identify cies in advance and avoid ual execution.
This Again
Create

- 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.
- 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.
- Set Src. Security Zone/Interface and Dest. Security Zone/Interface according to the actual needs. In this example, trust and untrust are selected.
- Expand **App**, **User**, **Effective Time**. Set **App** to an application that is allowed to be accessed. In this example, select **Work-OA**.
- Set Action Option to Permit and then click Save.

Basic Info	þ		
* Nam	e forallstaff		
Enabled State	e Enable		
* Policy Grou	Default Policy Group	~	⊕ Add Group
* Priorit	y Default Policy	~	Before 🗸
Description	n Enter the security policy na	me desc	
Src. and Dest	•		
Src. Securit			
Zone/Interfac		~	
* Src. Addres	s allstaff	~	
Src. Regio	n any	\sim	
Dest. Securit	y untrust	\sim	
Zone/Interfac	e		
* Dest. Addres	s any	\sim	
Dest. Security	untrust	\sim	
Zone/Interface			
Dest. Address	any	\sim	
Dest. Region	any	~	
Service	any	~	
Action Option	-		
_			
/	App、User、Effective Time \vee		

Intrusion Prevention Disable

Dest. Security	untrust	~		
Zone/Interface				
* Dest. Address	any	~		
Dest. Region	any	~		
Service	any	~		
Арр	Work-OA	~]	
User	any	~		
Effective Time	any	~	⊕ Add One-Off Time Plan	⊕ Add Cyclic Time Plan
Action Option	• Permit 🔿 Deny			
	Fold A			
Content Security	Fold A			
Content Security	Fold ~			
-	Disable			
Intrusion Prevention	Disable			
Intrusion Prevention Virus Protection	Disable Disable			
Intrusion Prevention Virus Protection URL Filtering	Disable Disable Disable			

- 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.
- 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.
- Set Src. Security Zone/Interface and Dest. Security Zone/Interface according to the actual needs. In this example, trust and untrust are selected.
- Set other parameters to any and Action Option to Permit to permit traffic from the employer's IP address.

< Back	Create Se	curity Policy	
	Basic Info		
	* Name	forboss	
	Enabled State	Enable	
	* Policy Group	Default Policy Group \sim	⊕ Add Group
	* Priority	forallstaff \sim	Before 🗸
	Description	Enter the security policy name desc	
	Src. and Dest.		
	Src. Security	trust ~	
i	Zone/Interface		
	* Src. Address	boss \lor	
	Src. Region	any \lor	
	Dest. Security	untrust \lor	
1	Zone/Interface		
*	Dest. Address	any	

* Priority	forallstaff	\sim	Before v
Description	Enter the security policy name desc		
Src. and Dest.			
Src. Security	trust	\sim	
Zone/Interface			_
* Src. Address	boss	\sim]
Src. Region	any	~	-
Dest. Security	untrust	\sim	
Zone/Interface			
* Dest. Address	any	\sim	
Dest. Region	any	\sim	
Service	any	\sim	
Action Option	• Permit 🔿 Deny		
	App、User、Effective Time $ \sim $		
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.

Crea	ate Batc	h Operation \checkmark	More V 🖸 Refres	h 🚺 Custom	Field	Enter a key	vord.	O
						Туре	All	`
	Priority	Name	Src. Security Zone/I nterface	Src. Address	Src. Region	Dest. Seci nte	Operation	
∨ Def	ault Policy	Group						
	1	forboss	trust	boss	any	un	Edit More ~	
	2	forallstaff	trust	allstaff	any	un	Edit More ~	
	3	Default Po	any	any	any	é	Edit More ~	

8.13 Traffic Control Policy

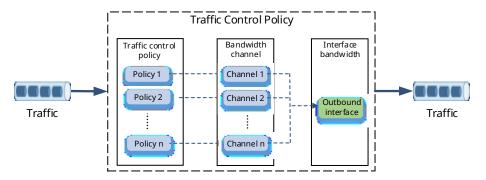
8.13.1 Overview

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

The processing procedure of traffic control policies is as follows:



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

8.13.2 Configuring Traffic Control Policies

1. Configuring Egress Bandwidth

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

Traffic C	Control Policy)								
Custom P	Policy Bandwidth Channel	🖉 Line Cor	nfig							
🕀 Create	e 🛅 Delete 🖪 Copy	✓ Enable	O Disable	🖲 Move	S Clear H	lit Record	C Refresh			
	Policy Name	Line	Src. Address	Dest. Address	Service	URL	Арр	User/Use r Group	Action	Bandwid h Channel
							No Data			

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

Traffic Cont	trol Policy		
< Back	ine Config Any unidentified	WAN interfaces? Configure W	/AN Interface
Interface	🗹 Ge0/7 🔽 Ge0/8		
Ge0/7			
Uplink	50	Mbps ~	
Downlink	100	Mbps ~	
Ge0/8			
Uplink	100	Mbps ~	
Downlink	200	Mbps ~	
			Save

Note

The outbound interface must be a WAN interface.

(4) Click Save.

2. Configuring Bandwidth Channels

- (1) Choose **Policy > Traffic Control Policy**.
- (2) Click the Bandwidth Channel. Click Create.

Traffic Control Policy		
Custom Policy Bandwidth Chan	nel 🖉 Line Config	
😧 Create 🗄 Copy	lete C Refresh	
Channel N ame	Overall Rate Limit	IP-based Rate Limit
		No Data

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

< Back Add Bandwidt	h Channel			
Basic Info				
* Name	Enter a keyword.			
Overall Rate Limit ①				
Max. Uplink Rate	Enter a keyword.	Mbps	\sim	
Guaranteed Uplink Rate	Enter a keyword.	Mbps	\sim	
Max. Downlink Rate	Enter a keyword.	Mbps	\sim	
Guaranteed Downlink Rate	Enter a keyword.	Mbps	\sim	
IP-based Traffic Limit ①				
Max. Uplink Rate	Enter a keyword.	Mbps	\sim	
Max. Downlink Rate	Enter a keyword.	Mbps	\sim	
Priority				
① Priority	4 (Medium)	~		
① Enable Refined Traffic				
Limiting				

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

ltem	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	If this function is enabled, the device performs weight-basedscheduling on the traffic entering the channel based on the servicepriority and guarantees the bandwidth of key services first when thebandwidth is insufficient.If this function is not enabled, services transmitted over the tunnelcompete for bandwidth resources without priority differentiation.Refined traffic limiting can be enabled only when the priority value is1. It does not take effect when it is enabled for parent or childpolicies.	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.

Custom P	olicy Bandwidth Channel	🖉 Line Cor	nfiq						
🕀 Create		e Senable	O Disable	e 🕑 Move	🔇 Clear H	lit Record	C Refresh		
	Policy Name	Line	Src. Address	Dest. Address	Service	URL	Арр	User/Use r Group	Actio

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

< Back	Add Traf	fic Control Policy
	Basic Info	
	* Name	Enter a keyword.
Pa	arent Policy	Enter or select a value.
	Location	Select a policy.
En	abled State	• Enable O Disable
	Line	
	* Line	Select the value. \sim
Src	. and Dest.	
S	irc. Address	any ~
De	est. Address	any ~
Services	s and Apps	
	Service	any ~
	Арр	any ~
	URL	
	URL	any ~
User/l	Jser Group	
User/	User Group	any ~
Action	Execution	
	Action	• Limit 🔿 No Rate Limit 🔿 Block
*	Bandwidth	Select the value. \checkmark \odot Add Bandwidth Channel
	Channel	
т	ime Range	
1	lime Range	any \checkmark \odot Add One-Off Time Plan \odot Add Cyclic Time Plan
		Save

ltem	Description	Remarks
Basic Info		•
Name	Name of the traffic control policy	[Example]
Name		Policy_1
Parent Policy	 When creating a traffic control policy, you can configure another traffic control policy as its parent policy. In this case, the current policy is a child policy. Traffic is preferentially matched against the parent policy and then the child policy until the lowest level of the child policy is matched. If traffic matches both the parent policy and the child policy, traffic control is performed based on the child policy. If traffic matches only the parent policy but not the child policy. Up to three levels of parent-child policies are supported. For overall rate limiting, note that the maximum uplink or downlink bandwidth of a parent policy must be larger than or equal to that of its child policy, and its child policy. 	Select an existing traffic control policy from the drop-down list.
	cannot be the same.	
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.		1
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 A	apps	1

Item	Description	Remarks
Service	The traffic of specified services matches the policy.	[Example]
		any
Арр	The traffic of specified applications matches the policy.	[Example]
		any
URL		
URL	The traffic of specified URLs matches the policy.	[Example]
		any
User/User Gro	up	
User/User	The traffic of specified users or user groups matches the policy.	[Example]
Group	Group	
Action Executi	on	
	The action the device performs for the traffic matching the policy.	
Action	 Limit: The device forwards the packets based on the bandwidth limits configured for the selected bandwidth channel. 	
Action	 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]
Anio Rango		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 Serv	ice					
Protocol Type	o IPv4 ○ IF	Pv6				
Basic Info						
* Name	Enter the name					
* ① Interface	Select an inter	ace.	~			
* ① IP Assignment Range						
* Subnet	Example: 192.1	68.1.0/24.	/	1		
* Default Gateway						
* Primary DNS Server				Use S	ystem DNS Setting	gs
Secondary DNS Server						
≣ ↑ Advanced						
* Lease Time	0	Day	1	Hour	0	Minute
Primary WINS Server						
① Option 43	ip ~					
① Option 138						
Secondary WINS Server						
① Reserved IP Address/Range						
① Binding Host MAC				1		
U billaring Host MAC			/	:		
						_
						Save

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.	 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	-	

b Set parameters of the DHCP server.

Item	Description	Remarks
Lease Time	Address lease period. In general, terminal devices automatically renews the lease in connected state to keep the IP address unchanged. If the lease is not renewed due to disconnection or network instability, the IP addresses are reclaimed after the lease expires. When the terminal devices recover connectivity, they will request the addresses again.	 The lease period ranges from 3 minutes to 365 days. The default lease period is 1 hour. [Example] 1 hour
Primary WINS Server	Windows Internet Naming Service (WINS) is used to register host names of network basic input/output system (NetBIOS) and resolve IP addresses based on host names.	This parameter is optional. The value is empty by default. [Example] 10.1.1.4
Option 43	Option 43 carried in DHCP packets. Option 43 is typically used in wireless network management scenarios to notify APs of the IP address of the wireless access controller (AC) so that the APs can register with the AC. When the AC and APs are on different LANs, the APs cannot discover the AC in broadcast mode. In this case, Option 43 needs to be configured for DHCP response packets on the DHCP server.	 The supported option types vary with AP models. Select Option 43 or Option 138 based on the supported option types of managed APs. Two formats are supported: 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.
- $(4) \quad \text{Configure the DHCP server information}.$
 - a Click Create.

The Create DHC	Service page	e is displayed	. Set IPv6 .
----------------	--------------	----------------	---------------------

< Back Create DHCP S	ervice							
Protocol Ty	pe 🔿 lpv4 🔹	руб						
Basic In	fo							
* 🕕 Interfa	select an interface.				n interface.			
* Primary DNS Serv	ver			Enter the	e DNS server add	lress.		
Secondary DNS Serv	ver							
* Lease Tir	ne 0	Day 8		Hour	0	Minute		
Address Po	ol							
⊕ c	reate 🔟 Delete							
	Туре		Prefix		Available P	refix Length	Operation	
	iype		T T T T T				operation	
				No D	ata			
				Sav	re			

b Set parameters of the DHCP server.

ltem	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				
⊕ Create	Delete			
	Туре	Prefix	Available Prefix Length	Operation
		No	Data	
		S	ave	

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

Create Address Poo	bl	\otimes
* Type	 Network Address Prefix 	
* Prefix	Enter Prefix	
Available Prefix Length	Enter Available Prefix Length	
	OK Cancel	

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.

Product Cookbook

Address Management List				
Bind IP/MAC O Unbind S	Refresh			IPv4 IPv6
Assigned IP	MAC	Lease Time	Assignment Mode	Operation
		No Data		

- (7) Process the IP addresses.
- Select addresses and click **Bind IP/MAC** or **Bind** in the **Operation** column to fixedly allocate IP addresses to the hosts with the corresponding MAC addresses.
- Select addresses and click **Unbind** to cancel the binding relationship between IP addresses and MAC addresses.

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

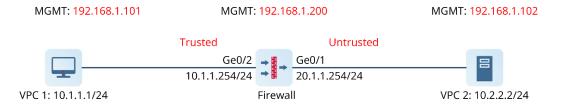
The IP addresses in blocklist cannot be used to log in to the firewall.

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**.

Image: Create in Delete i	IPv4 Allowlist							
	⊕ Create 🗓 Del	☺ Create ☺ Refresh ☺ Enable ☺ Disable [] Import [] Export						
	Allowlist	Allowlist Allowist Type Description					Operation	
No Data								

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

< Back Add Allowlist	
ІР Туре	IPv4
Allowlist Type	• Src. Address 🔿 Dest. Address
* () IP Address/Range	
Description	

ltem	Description	Remarks
Allowlist Type	 Type of the allowlist: Src. Address: Permit packets sent from this address. Dest. Address: Permit packets sent to this address. 	[Example] Src. Address
IP Address/Range	Allowlist IP address/range.	 The following three formats are supported: Single IP address: 192.168.1.1 Subnet: 192.168.1.0/24 IP address range: 192.168.1.1- 192.168.1.10

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

IPv4 /	14 Allowlist IPv6 Allowlist IPv4 Blocklist IPv6 Blocklist Temporary IPv4 Blocklist Temporary IPv6 Blocklist							
O Create Delete C Refresh Enable Disable Disable Disable Enter the keyword. C							Q	
	Allowlist Allowlist Type			Description	Operation			
	172.26.1.19	S	rc. Address			-	Edit 📋 Delet	

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**.

Ruffie Z Series Firewall	습 Home 🛛 Monitor ⊕ Network	은 Object 😨 Policy	(3) System	🖗 Network Discovery	Ø Network Mgmt	Quick Onboarding	Policy Wizard	ဂြ Customer Service	्र admin
l Security Policy > 命 Port Scan 函 Traffic Learning	IPv4 Allowlist IPv6 Allowlist		IPv6 Blocklist Temp Dle 🕻 Import 🚺 Export	orary IPv4 Blocklist	Temporar	y IPv6 Blocklist	Enter the	keyword.	
Security Defense	Allowlist	Allowlist Type	No E	Data	Description			Operation	
Blocklist and Allowlist Reputation Center SSL Proxy			NO L	2 63 5.62					
eey SSL Proxy >									

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

< Back Add Allowlist		
ІР Туре	IPv6	
Allowlist Type	• Src. Address	O Dest. Address
* ① IP Address/Range		
Description		

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

IPv4 Allowlist	IPv6 Allowlist	IPv4 Blocklist	IPv6 Blocklist	Temporary IPv4 Blocklist	Temporary IPv6 Blocklist		
O Create Image: Delete C Refresh Image: O Disable Image: Delete Image: Delete				Enter the keyword.	Q		
Allowlist		Allowlist Type		Description	Operation		
2000::1	Si	rc. Address				Edit 🖻 Dele	ete

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.

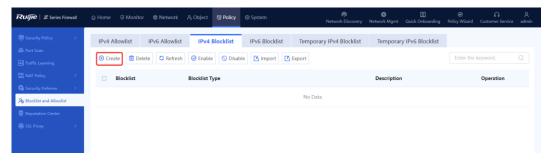
8.15.5 Creating an IPv4 Blocklist

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	
ІР Туре	IPv4
Blocklist Type	• Src. Address 🛛 Dest. Address
* () IP Address/Range	
Description	

Item	Description	Remarks
Blocklist Type	 Type of the blocklist: Src. Address: Block packets sent from this address. Dest. Address: Block packets sent to this address. 	[Example] Src. Address
IP Address/Range	Blocklist IP address/range.	 The following three formats are supported: Single IP address: 192.168.1.1 Subnet: 192.168.1.0/24 IP address range: 192.168.1.10

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

IPv4 Allowlist IPv6 Allo	owlist IPv4 Blocklist	IPv6 Blocklist Temporary IPv4 Block	list Temporary IPv6 Blocklist	
⊕ Create 📋 Delete 😋 Re	Enter the keyword. Q			
Blocklist Blocklist Type			Description	Operation
. 1.1.1.1	Src. Address		-	idit 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**.

Ruijie Z Series Firewall	🚊 Home 🛛 Monitor ⊕ №	Network A≞ Object	System 🕄 Policy	ጫ Network Disc	🕲 overy Network Mgmt	L Quick Onboarding	Ø Policy Wizard	Customer Service	Q admin	
 (e) Security Policy → (e) Port Scan (f) Traffic Learning 			Blocklist IPv6 Block		klist Tempora	ry IPv6 Blocklist	Enter the	keyword.		
Star Policy →	Biocklist Biocklist Type Description							Operation		
An Blocklist and Allowlist	No Data									
Reputation Center SSL Proxy >										

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

< Back Add Blocklist		
ІР Туре	IPv6	
Blocklist Type	• Src. Address	O Dest. Address
* () IP Address/Range		
Description		
		11

ltem	Description	Remarks
Blocklist Type	 Type of the blocklist: Src. Address: Block packets sent from this address. Dest. Address: Block packets sent to this address. 	[Example] Src. Address
IP Address/Range	Blocklist IP address/range.	 The following three formats are supported: Single IP address: 1234::100 Subnet: 1234:100::/64 IP address range: 1234::100-2345::100

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

IPv4 Allowlist IPv6 Allo	wlist IPv4 Blocklist IPv6 Block	dist Temporary IPv4 Blocklist Tempora	ary IPv6 Blocklist
🕑 Create 🔟 Delete 🔇 Re	efresh 📀 Enable 🚫 Disable 🗹 Impor	t 🚺 Export	Enter the keyword. Q
Blocklist	Blocklist Type	Descript	tion Operation
2003::1	Src. Address	-	Edit Delete

Follow-up Procedure

- To delete multiple blocklist policies in a batch, select the policies that you want to delete and click Delete.
- To enable multiple blocklist policies in a batch, select the policies that you want to enable and click **Enable**.
- To disable multiple blocklist policies in a batch, select the policies that you want to disable and click **Disable**.
- To export all blocklist configurations, click **Export**.
- Click **Import** to download the import template and upload the configured file, or directly select the CSV file to be uploaded. Then, click **Confirm** to start the import task.
- Enter the blocklist IP address, full or part of the blocklist description in the search box to search for the policies. Fuzzy search is supported.

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.

Ruffie Z Series Firewall	습 Home	유 Object 😨 Policy	System	M Network Disc	🔕 overy Network Mgmt	L Quick Onboarding	Policy Wizard	Customer Service	ې admin
ll Security Policy > 命 Port Scan	IPv4 Allowlist IPv6 Allowlist	IPv4 Blocklist	IPv6 Blocklist	Temporary IPv4 Block	ist Temporar	y IPv6 Blocklist	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		
In Traffic Learning Set NAT Policy	Create Delete Create Refresh		Adding Time	Blocking Dur Remaining ation uration	Blocking D Source	Descript		Operation	
Blocklist and Allowlist				No Data					
a) SSL Proxy →									

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

< Back Add Temporar	y Blocklist	
ІР Туре	IPv4	
Blocklist Type	• Src. Address 🛛 Dest. Ad	ldress
* () IP Address/Range		
Blocking Duration	5	Minute \vee (Range: 3 min to 15 days)
Description		le le

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

Ruijie Z Series Firewall	습 Home 🛛 Monitor 🔀 Network	은 Object 😨 Policy	⊜ System	M Network Discov	😵 ry Network Mgmt	Quick Onboarding	Policy Wizard	ြ Customer Service	ې admi
Image: Becurity Policy → Image: Becurity Policy →	IPv4 Allowlist IPv6 Allowlist	IPv4 Blocklist	IPv6 Blocklist	Temporary IPv4 Blocklist	Temporary	IPv6 Blocklist			
(#) Port Scan	🕑 Create 📋 Delete 🗳 Refresh	Set Blocking Dur	ation				Enter an I	P address.	
Security Defense	No. IP	Туре А	Adding Time	Blocking Dur Remaining Blo ation uration	cking D Source	Descript	tion	Operation	
An Blocklist and Allowlist				No Data					
 Reputation Center SSL Proxy 									

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

< Back Add Tempora	ry Blocklist
IP Туре	IPv6
Blocklist Type	• Src. Address O Dest. Address
* ① IP Address/Range	
Blocking Duration	5 Minute \checkmark (Range: 3 min to 15 days)
Description	

ltem	Description	Remarks
Blocklist Type	 Type of the temporary blocklist: Src. Address: Block packets sent from this address. Dest. Address: Block packets sent to this address. 	[Example] Src. Address
IP Address/Range	Temporary blocklist IP address/range.	 The following three formats are supported: Single IP address: 1234::100 Subnet: 1234:100::/64 IP address range: 1234::100-2345::100

ltem	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.

		urity Rule Base 🗸			En	ter an ID or a	name. Q
	Rule ID	Defense Name	Threat Type	Threat Subtype	Severity	Action	Operation
	4259841	D-LINK DIR-615 cross-stat	Spoofing Attack	CSRF	 Medium 	Alarm	View Details
	4259842	Western Digital mycloud	Spoofing Attack	CSRF	• High	Block	View Details
	4259843	Wiki Cross Site Request F	Spoofing Attack	CSRF	 Medium 	Block	View Details
	4259844	Easy hosting control panel	Spoofing Attack	CSRF	 Medium 	Alarm	View Details
	4259845	DedeCMS V5.7 Backgroun	Spoofing Attack	CSRF	• High	Block	View Details
	4259846	iRZ Mobile Routers Cross	Spoofing Attack	CSRF	 Medium 	Block	View Details
	4259847	Insomnia Shell request	Spoofing Attack	CSRF	• High	Block	View Details
	4259848	D-Link DSL-2740B Cross S	Spoofing Attack	CSRF	 Medium 	Alarm	View Details
	4259849	Airlive IP Camera Cross Sit	Spoofing Attack	CSRF	 Medium 	Alarm	View Details
	4259850	Fortinet Fortigate Firewall	Spoofing Attack	CSRF	 Medium 	Alarm	View Details
10 \	/ Page Tot	al:12041		Go to 1 <	1 2 3	4 5	6 ··· 1205 >

(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.

1 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 <u>https://cloud.ruijienetworks.com</u> 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

	Monitoring Configuration Maintenance			+ Add Demo Project
A yangliwen@ruij v	ALL V Search Network Q		(GMT+0:00)Africa/Abidjan Manage	Project Take Over Network Unbind Device
Dashboard Topology Alarm	AP List New firmware available for 3 devices	elected		Auto Refresh: 💽 🤂 🖒 📰 🗸 🖸
Report	Status , SN Config Status , MAC	Alias MGMT IP Egress	IP Clients Network Firmware Version	Offline Time Model Description Action
Network	Online <u>NAEK0E3BH0009</u> Synchronized 00d2.f80e.3b			- RAP2260(G) <u>Empty</u> 📎 📺
Voucher	Online NAEK0E3BH0010 Synchronized 00d2.f80e.3b	001 <u>Ruijie</u> 192.168.110.10 10.148.0.	110 - test ReveeOS 1.206.2020	- RAP2260(G) Empty () 📺
B Device	Online <u>NAEK0E3BH0011</u> Synchronized 00d2.f80e.3b	011 <u>Ruijie</u> 192.168.110.11 10.148.0.	110 - test ReveeOS 1.206.2020	- RAP2260(G) <u>Empty</u> 📀 📋
AP	Online NAEK0E3BH0007 Synchronized 00d2:180e.3b	071 <u>Ruille</u> 192.168.110.7 10.148.0.	110 - lest ReyeeOS 1.202.1915	- RAP1260(G) Empty. () 📋
AC	Online <u>NAEK0E3BH0008</u> Synchronized 00d2.f80e.3b	081 <u>Ruijie</u> 192.168.110.8 10.148.0.	110 - test ReyeeOS 1.202.1915	- RAP1260(G) Empty 💿 📋
Switch	First	Previous Page 1 of 1	Next Last	10 🔺 5 in total
Gateway				
Home Router				
Bridge				
Terminal				
Cameras				
NVR				
IP Phone				
Client				
Wi_Ei Client				

The system displays the basic device information such as status, SN, device, management address, software version, and device model.

(3) Click **SN** to enter the device management page. View device basic information, panel information, interface information, and status.

Device Details		×
WAN LAN Disconnected Disabled PPPE Static IP DHCP Copper SFP Image: Copper Signer Image: Copper Signer Image: Copper Image: Copper <td>Basic Alias: SN: MAC: Model: Egress IP MGMT IP Firmware Version: Description</td> <td>Ruijie / NAEKOE3BH0001 0000/80e.3b11 EG310GH-E 10.148.0.110 192.168.110.1 ReyeeOS 1.206.2023</td>	Basic Alias: SN: MAC: Model: Egress IP MGMT IP Firmware Version: Description	Ruijie / NAEKOE3BH0001 0000/80e.3b11 EG310GH-E 10.148.0.110 192.168.110.1 ReyeeOS 1.206.2023
CPU & Memory Usage Connectivity		Last 24 Hours Last 7 Days
CPU Usage Memory Usage Flash 4:00 8:00 12:00	16:00 20	0:00 0:00
Log Record Device Log Config Log		
Type Updated At Online/Offline Device goes online for the first time	Content	V QSearch 😔 📰 V
First Previous Page 1 of 1 Next Last		10 🔺 1 in total

You can click the titles one by one to manage devices.

- Device panel: includes information such as interface distribution on panel.
- Basic information: includes device name, device model, SN, MAC address, and software version.
- Status: includes CPU and memory usage, offline status, and connectivity status.
- Interface information: By clicking the titles in status information, you can view detailed interface information, such as WAN/LAN port information (such as port number, mode, and subnet mask).



Figure 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	1

Figure 8-10 Status Information

Overview Confi	g								
CPU & Memory Us	age		Connectiv	ty			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

IP地址

2. Managing Tunnels

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

Figure 8-12 Tunnel Management

eWeb SSH Tunnel Locate	
Device panel	
100M/1000M 10M Disconnected Front panel	Back Panel (Can not be configured)
Please select a port to check its details.	

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

Figure 8-13 Creating a Tunnel

Tunnel (SN: N	IAEK0E3BH	0010)						>			
Create	Tunnel										
Type: eW	leb	~ [Create Tunnel								
							Local	Global			
Tunnel	List						Ð	80 ▼			
If the tunnel	If the tunnel is unavailable, please re-create it or contact us for support.										
Туре	Host	Port	Destination Device	Destination Port	Expired at	Status	Action				
				No Data							
			First Previous Page	0 of 0 Next Last		C	10 🔺 🛛 0 ir	n total			

3. Upgrading Device Software/Firmware

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

Ruíjie	Monitoring Configuration Maintenance				+ Add Demo	Project 🥵 🗘 🚱 🕹
A yangliwen@ruij v	Version Details Private Firmware					
🖶 Logs						
Operation Log						⊕ #+8
Config Log	Upload Firmware Delete 0 Selected					Version, Applicable Q Search
Upgrade Log						
9 Upgrade	Firmware Version File	File Size (MB)	Applicable Model	Uploaded at	Released at	Description Action
Upgrade			No Data			
Firmware		First Previous	Page 0 of 0 Next	Last		10 🔺 0 in tota

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

Product by PLACE	Monitoring Cor	nfiguration Maint	enance •				+ Add Demo Project	¶≎ e	6 6
yangliwen@ruij 🗸	ALL \sim / test \sim	Search Network	λ			(GMT+8:00)Asia/Sha	nghai Manage Project Take Over N	etwork Unb	ind Device
Logs									
Operation Log				otner		ESW_1.0(1)B1P20,Release(09200219)			1
Config Log						Previous	Page 1 of 2 Next		
Upgrade Log									
Upgrade									
Upgrade	1.5.1.11								
	Device List							÷	## * 50
Firmware	Upgrade Upgra	de All 0 Selected					SN, Alias, Description Q	Advanced S	earch \vee
	Status	A SN N	etwork Alias	Model	Hardware Version	Current Version	Recommended Version	Description	Action
	🗌 🥥 Online	NAEK0E3BH0001 to	est Ruijie	EG310GH-E	1.00	ReyeeOS 1.206.2023	ReyeeOS 1.216.1504		Upgrade
						ReyeeOS 1.200.2023	ReyeeUS 1.216.1504		
	🗌 🎯 Online	NAEK0E3BH0002 b	est Ruijie	NBS3200-48GT4XS	1.00	ReyeeOS 1.202.1818	ReyeeOS 1.218.1413		Upgrade
	OnlineOnline		est Ruijie est Ruijie	NBS3200-48GT4XS NBS3100-24GT4SFP-P					Upgrade Upgrade
		NAEK0E3BH0003 b			1.00	ReyeeOS 1.202.1818	ReyeeOS 1.218.1413		
	Online	NAEK0E3BH0003 b NAEK0E3BH0004 b	est Ruijie	NBS3100-24GT4SFP-P	1.00	ReyeeOS 1.202.1818 ReyeeOS 1.202.1818	ReyeeOS 1.218.1413 ReyeeOS 1.218.1413		<u>Upgrade</u>
	Online Online	NAEK0E3BH0003 b NAEK0E3BH0004 b NAEK0E3BH0005 b	est Ruijie est Ruijie	NBS3100-24GT4SFP-P NBS3100-24GT4SFP-P	1.00 1.00 1.00	ReyeeOS 1.202.1818 ReyeeOS 1.202.1818 ReyeeOS 1.202.1818	ReyeeOS 1.218.1413 ReyeeOS 1.218.1413 ReyeeOS 1.218.1413		Upgrade Upgrade
	 Online Online Online 	NAEK0E3BH0003 b NAEK0E3BH0004 b NAEK0E3BH0005 b NAEK0E3BH0006 b	est Ruije est Ruije est Ruije	NBS3100-24GT4SFP-P NBS3100-24GT4SFP-P NBS3100-24GT4SFP-P	1.00 1.00 1.00 1.00	ReyeeOS 1.202.1818 ReyeeOS 1.202.1818 ReyeeOS 1.202.1818 ReyeeOS 1.202.1818	ReyeeOS 1.218.1413 ReyeeOS 1.218.1413 ReyeeOS 1.218.1413 ReyeeOS 1.218.1413		Upgrade Upgrade Upgrade
	 Online Online Online Online Online 	NAEK0E3BH0003 b NAEK0E3BH0004 b NAEK0E3BH0005 b NAEK0E3BH0006 b NAEK0E3BH0006 b NAEK0E3BH0009 b	est Ruijie est Ruijie est Ruijie est Ruijie	NBS3100-24GT4SFP-P NBS3100-24GT4SFP-P NBS3100-24GT4SFP-P ES218GC-P	1.00 1.00 1.00 1.00 1.00	ReyeeOS 1.202.1818 ReyeeOS 1.202.1818 ReyeeOS 1.202.1818 ReyeeOS 1.202.1818 ESW_1.0(1)81P20.Release(09200219)	ReyeeOS 1.218.1413 ReyeeOS 1.218.1413 ReyeeOS 1.218.1413 ReyeeOS 1.218.1413 ReyeeOS 1.218.1413 ESW_1.0(1)B1P20 Release(10130318)		Upgrade Upgrade Upgrade Upgrade
	 Online Online Online Online Online Online Online 	NAEK0E3BH0003 b NAEK0E3BH0004 b NAEK0E3BH0005 b NAEK0E3BH0006 b NAEK0E3BH0009 b NAEK0E3BH0009 b NAEK0E3BH00010 b	est Ruijie est Ruijie est Ruijie est Ruijie	NBS3100-24GT4SFP-P NBS3100-24GT4SFP-P NBS3100-24GT4SFP-P ES218GC-P RAP2260(G)	1.00 1.00 1.00 1.00 1.00 1.00	Reyee/OS 1 202.1818 Reyee/OS 1 202.1818 Reyee/OS 1 202.1818 Reyee/OS 1 202.1818 ESW_1.0(1)81F20.Release(09200219) Reyee/OS 1 206.2020	ReyeeOS 1.218.1413 ReyeeOS 1.218.1413 ReyeeOS 1.218.1413 ReyeeOS 1.218.1413 ESW_1.0(1)B1P20.Release(10130318) ReyeeOS 1.218.1410		Upgrade Upgrade Upgrade Upgrade Upgrade
	 Online Online Online Online Online Online Online Online Online 	NAEK0E3BH0003 b NAEK0E3BH0004 b NAEK0E3BH0005 b NAEK0E3BH0006 b NAEK0E3BH0009 b NAEK0E3BH0010 b NAEK0E3BH0010 b	est Ruijie est Ruijie est Ruijie est Ruijie est Ruijie	NBS3100-24GT4SFP-P NBS3100-24GT4SFP-P NBS3100-24GT4SFP-P ES218GC-P RAP2260(G) RAP2260(G)	1.00 1.00 1.00 1.00 1.00 1.00 1.00	Reyee/OS 1 202.1518 Reyee/OS 1 202.1518 Reyee/OS 1 202.1518 Reyee/OS 1 202.1518 Reyee/OS 1 202.1518 ESW_1.0(1)81P20.Release(09200219) Reyee/OS 1 205.2020 Reyee/OS 1 205.2020	ReyecOS 1.218.1413 ReyecOS 1.218.1413 ReyecOS 1.218.1413 ReyecOS 1.218.1413 ESW_1 0(1)81F20.Release(1013038) ReyecOS 1.218.1410 ReyecOS 1.218.1410		Upgrade Upgrade Upgrade Upgrade Upgrade Upgrade

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

Upgrade	×
Check in Maintenance > Log >Upgrade Log	
Model: NBS3100-24GT4SFP-P Hardware Version: 1.00 Current Version: ReyeeOS 1.202.1818 Upgrade Version: ReyeeOS 1.218.1413 Firmware Details ~ Upgrade Device: 1	× Select Firmware
Scheduled Upgrade	
Advanced Settings ~	Start Upgrade Cancel
	Cancor

(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.

	Monitoring C	onfiguration Ma	intenance •					+ Add Demo Proj	ect 🛯 🕶 🗘 🚱 🔇	8
A yangliwen@ruij v	Upgrade Log									÷ 53
🗎 Logs							Started at	Ended at	C Sea	
Operation Log							Stated at			ii ci i
Config Log	Operator	Description	Target Version	Process	Time Range	Created At		Result (Success/Failure/Aborted)	Acti	ion
Upgrade Log					No Data	i i i				
를 Upgrade			First	Previous	Page 0 of 0	Next	ast		10 🔺 0 in	tota
Upgrade										
Firmware										

Figure 8-14 Upgrade Result

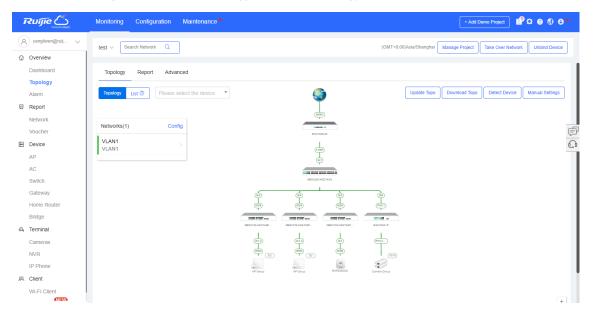
4. Viewing Network Topology

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.

< Back Add DNS	
* DNS Server Address1	
	Save

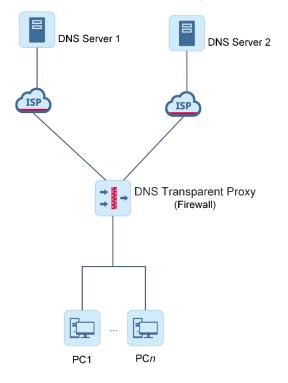
- b Enter the IP address of the DNS server 1 in the DNS Server Address1 input box.
- c Click Save.
- (3) (Optional) If multiple DNS servers are configured in the network environment, you can set the IP address for the second or third DNS server.

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 <u>8.23</u> 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.

DNS	DNS Transparent Proxy		
~	is function requires that DNS request traffic be nsparent proxy policy. You can configure DNS s		
DNS Tran	sparent Proxy		
Routing N	Node Egress Load Balancing \lor		
Proxy In	terface Excluded Domain Name Proxy Policy		
🕀 Creat	te 🔟 Delete 🤗 Enable 🚫 Disable	C Refresh	
	Outbound Interface	Monitoring Status	Primary DNS Server Address
			No Data

(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.

DNS	DNS Transparent Proxy				
				, the device distributes DNS request traffic to tbound interface for specific domain names	
DNS Trans	sparent Proxy				
Routing N					
Proxy Int	Egress Load Balancing Src. IP-based XV	Policy			
😌 Creat	e 🕻 Interface Bandwidth-based isa	able 😋 Refresh		Enter an ir	iterface name or IP address. Q
	Outbound Interface	Monitoring Status	Active DNS Server Address	Standby DNS Server Address	Operation
			No Data		

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 <u>8.23</u> Outbound Interface Load Balancing.
Egress Load Balancing	DNS request packets and other traffic are forwarded based on the forwarding mode described in <u>8.23</u> 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 <u>8.23</u> Outbound Interface Load Balancing.

- (4) Configure DNS proxy parameters.
- Configure a proxy interface.
 - a Click Create.

DNS	DNS Transparent Proxy				
			en identifying DNS request traffic, the device distribut ure an outbound interface for specific domain names		vers on different lines based on the DNS
DNS Trans	sparent Proxy 💽				
Routing N	flode Egress Load Balancing \sim				
Proxy Int		efresh			Enter an interface name or IP address
	Outbound Interface	Monitoring Status	Primary DNS Server Address	Secondary DNS Server Address	Operation
			No Data		

b Create a DNS proxy interface.

< Back Add Proxy Interface		
* Outbound Interface	Select ~	
* Primary DNS Server Address	Enter	
Secondary DNS Server Address	Enter	
DNS Probe	Select ~	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 <u>8.22 Link Detection</u> .

- c Click Save.
- Configure excluded domain names.
 - a Click Create.

DNS DNS Transparent Proxy	
① This function requires that DNS request traffic be transparently forwarded by the device. When identifying DNS request traffic, the device distributes DNS request traffic to distributes	
DNS Transparent Proxy 💽	
Routing Mode Egress Load Balancing \checkmark	
Proxy Interface Excluded Domain Name Proxy Policy	
⊕ Create ⊕ Create ⊕ Create	Enter a domain name or IP address.
Domain Name Primary DNS Server Address Secondary DNS Server Address	Operation

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.

< Back Add Excluded Domain Name						
* 🕕 Domain Name	secloud1.ruijie.com.cn					
Primary DNS Address	Select	~				
Secondary DNS Address	Select	\sim				

Item	Description	Remarks
	DNS domain name exclusion provides three matching modes: Exact match: Enter the complete domain name, such as www.ruijie.com.	
Domain Name	Prefix match: Enter an incomplete domain name ended with an asterisk (*), for example, www.ruijie.*.	[Example]
	Suffix match: Enter an incomplete domain name started with an asterisk (*), for example, *.ruijie.com.	www.test.com
	The matching priorities in descending order are as follows: exact match, suffix match, and prefix match. Fuzzy match in other formats is not supported.	
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.

DNS	DNS Transparent Proxy							
	① This function requires that DNS request traffic be transparently forwarded by the device. When identifying DNS request traffic, the device distributes DNS request traffic to different DNS servers on different lines based on the DNS transparent proxy policy. You can configure DNS servers for different extranet lines, or configure an outbound interface for specific domain name for domain name resolution.							
DNS Transp	arent Proxy 💽							
Routing Mc	Egress Load Balancing							
Proxy Inter	face Excluded Domain Name	Proxy Policy						
🕒 Create	🛅 Delete 🥝 Enable	S Disable S Move Cle	ar Hit Record 🖸 Refresh				Enter a polic	y name or IP address.
	Priority Name	Description	Src. Address	Dest. Address	Service	Proxy Action	Hit Count	Operation
				No Data				

b Configure a proxy pol	icy.
-------------------------	------

Back Add Proxy Pol	icy				
Basic Info					
* Name	Enter the policy name.				
Enabled State	• Enable 🔿 Disable				
Adjacent Policy	Select a policy.		Before	\sim	
Description					
		li			
Src. and Dest.					
* Src. Address	Select the source address.				
* Dest. Address	Select the destination address. \sim				
* 🕕 Service	Select a service.				
Action Settings					
Proxy Action	• Proxy 🔿 No Proxy				

Save

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.	1	1

Item	Description	Remarks		
Src. Address	Source address of a DNS request packet.	 Click the drop-down list, and select a source address in the To-be-selected area. The selected address is automatically added to the Selected area. Click Add Address or Add Address Group to add a source address. [Example] any 		
Dest. Address	Destination address of a DNS request packet.	 Click the drop-down list, and select a destination address in the To-be-selected area. The selected address is automatically added to the Selected area. Click Add Address or Add Address Group to add a destination address. [Example] any 		
Service	Service type of a DNS request packet.	 Click the drop-down list, and select a service in the To-be-selected area. The selected service is automatically added to the Selected area. Click Add Service or Add Service Group to add a service. [Example] dns-t 		
Action Settings				
Proxy Action	Whether to enable DNS transparent proxy for DNS request packets.	[Example] Proxy		

c Click Save.

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.

DDNS								
⊕ Create	🔟 Delete 🕻	Refresh						
(i) Up to	8 DDNSs are sup	ported. Currently, Peanutl	Hull (Oray), PubYun (332	2), DynDns, No-IP, an	d custom DDNSs are sup	ported.		
	Policy Name	Service Provider	Domain Name	Username	Bound Interface	Operating Status	Update Time	Operation
					No Data			

(3) Configure a DDNS policy.

Create DDNS Policy		\otimes
* Policy Name	Enter a policy name.	
* Service Provider	Select a service provider.	
* Username	Enter an username.	
* Password	Enter a password.	
* (i) Bound Interface	Select an interface.	
* Domain Name	Enter a domain name.	
	Cancel OK	

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.	 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.

Intelligent Routing



(3) Set parameters of intelligent routing.

< Back Create Intellige	ent Routing			
Basic Info				
* Name				
Enabled State	• Enable 🔿 Disable			
Adjacent Policy	Select a policy. v	Before ~		
Description				
	ĥ			
Matching Conditions				
Inbound Interface	Select an inbound interface or sourc \vee			
Src. Address	Select the source address. \sim			
Dest. Address	Select the destination address. $\qquad \lor$			
Service	Select a service. \sim			
User	Select a user. V			
Арр	Select an application. \sim			
Effective Time	Select ~	⊕ Add One-Off Time Plan ⊕ A	Add Cyclic Time Plan	
Action Settings				
Action Option	• Forwarding O No Intelligent Routing	3		
Outbound Interface Type	 Single Interface Multiple Interface 	s		
* Intelligent Routing Mode	Based on Src. IP Hash $\qquad \lor$			
Outbound Interface List				
	🕤 Create 📋 Delete 😋 Refresh			
	Interface	Next-Hop Address	s Uplink Load Threshold Do	wnlink
			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						

ltem	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 Cond	itions	
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

ltem	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		
Арр	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	8	8		
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	 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		For details about link detection, see <u>8.22</u> 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**.

Ruijie Z Series Firewall	û Home 🛛 Monitor ⊕	Network P Object	@ Policy 😂 System	ကြာ Network Discovery	⊗ Network Mgmt	€ Quick Onboarding	Policy Wizard	Customer Service	Q admin
똍 Address	ISP Address Library								
🚱 Арр —	🕒 Create 🛅 Delete	🛃 Import 🚺 Export	C Refresh				Enter a na	ime.	Q
図 URL Category 身 Service	Name				-				
🛱 Time Plan	Default Address Lib		Description	Last Update	lime			eration v Details	
👰 ISP Address Library		- July					VIEV	VDetails	
⑧ User Authentication > □ Gertificate >									
Content Template >									
🗐 Security Rule Base									

(2) Set parameters of the ISP address library.

< Back Create	e ISP Address Library		
	* Name		
C	escription	li di	
* ISP Ac	ldress List		
	↔ Create 🔟 Delete		Enter an IP address or I Q
		IP Address/Range	Operation
		No Data	
	Total: 0		

ltem	Description	Remarks
Name	Name of the ISP address library.	Characters such as `~!#%^&*+\ {};:'"/<>? and spaces are not allowed. [Example] Address library 1
Description	Description of the ISP address library.	Characters such as `~!#%^&*+\ {};:'''/<>? are not allowed. [Example] Address library 1
ISP Address List	IP addresses contained in the address library.	 Click Create to enter a single IP address or an IP address range. Three configuration methods are supported: IP address: One or multiple IP addresses. Input an IP address per line. Press Enter to separate lines. Example: 192.168.20.3 IP address range: A contiguous range of addresses. Connect the start IP address and end IP address with a hyphen (-). Example: 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.

Ruíjie Z Series Firewall	습 Home 🤤 Monitor 🕀 Networ	rk 🔑 Object 🖾 Policy ۞ System		€ Ø ि 央 nboarding Policy Wizard Customer Service admin
IP Address	ISP Address Library			
App	🕒 Create 📋 Delete 🚺 Imp	ort 🚺 Export 🖸 Refresh		Enter a name. Q
図 URL Category 导 Service	Name	Description	Last Update Time	Operation
📅 Time Plan	Default Address Library	-	-	View Details
Q ISP Address Library (B) User Authentication >				
Certificate >				
Content Template >				
😑 Security Rule Base				

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

Import		\otimes
Downloa	d CSV Template	
* Nam	ISP Address Library Name	
e		
* File	Select the file to be imported.	
	Browse	
	Confirm Cancel	

- (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**.

A 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 <u>https://secloud1.ruijie.com.cn</u>, choose **Signature Library Upgrade** > **ISP Address Library**, and select a suitable version to download.

Ruíjie	2	Library Upgrade V	ersion Upgrade De	vice Authorization	Validity Period Query	SSLVPN				ු tes
App Ider	ntification Library	IPS Library AV-H	ASH Library AV-SD	K Library URL L	ibrary Threat Intellig	ence Library	SP Address Library			
Product	Type Select a type	Product Serie	Select the series.	 ✓ Model 	Select a model.	Software Version	Select a software ve V	Reset		
No.	File Name	Version Number	Version Description	Model	Software Version	Release Date	File Size (MB)	MD5	Operation	
1	isp_20221202.1005.	. 20221202.1005	isp_20221202.1005	Z5100,Z5100-S,Z3	Universal	2022-12-02	0.01	6a2e2877b88cd04	± Download	
2	isp_20221030.1000.	. 20221030.1000	isp_20221030.1000	Z5100,Z5100-S,Z3	Universal	2022-10-30	0.01	0ABAF66F14A49F	± Download	

(2) Open the Signature Library Upgrade page.

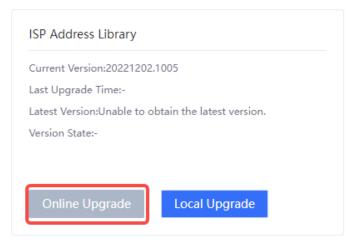
Open the web page on the device, and choose System > Signature Library Upgrade.

Ruffe Z Series Firewall	습 Home	System) 🛞 iscovery Network Mg	t Quick Onboarding	Policy Wizard	ရ Customer Service	ې admin	
🔏 Admin 🗸 🗸	Signature Library Upgrade							
Admin Admin Role System Canfig) Fault Diagnosis) Cloud Management Flatform Signature Library Upgrade Signature Maintenance)	Enable Auto Upgrade Upgrade Time-Daily 6 Vinus Protection Signature Library (Deep Scan) Vinus Protection Signature Library (Quick Scan) Intrusion Prevention Signature Library Vinus Protection Signature Library Vinus Protection Signature Library Intrusion Prevention Signature Library Intrusion Prevention Signature Library Interview Int							
	Gupgrade All Upgrade all signature libraries online simultaneousl	llys)						
	App Identification Signature Library	Virus Protection Signature Library (Deep Scan)	Vi	us Protection Signatu	re Library (Quic	k Scan)		
	Current Version20230217.1245 Last Upgrade Time- Latest Versiont/Inable to obtain the latest version. Version State- Activation StatesActivated	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 prot signature Bibrary for deep scan is not loaded	La: Lat Ve	rent Version:20230309.02 t Upgrade Time:- est Version:Unable to obt sion State:- ivation State:Activated		ion.		
	Online Upgrade Local Upgrade system versionRaliback	Online Upgrade d Local Upgrade		Online Upgrade	Local Upgrad	e		
Ē		Intrusion Prevention Signature Library	ISI	Address Library				

- (3) Find out ISP Address Library, and select Online Upgrade or Local Upgrade according to actual situation.
 - Online Upgrade: When the current version information about the firewall exists on the cloud platform and a new version is available, online upgrade of the device system can be performed on the firewall.



The firewall must be connected to the Internet.



- o Local Upgrade
- a Click Local Upgrade.

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

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

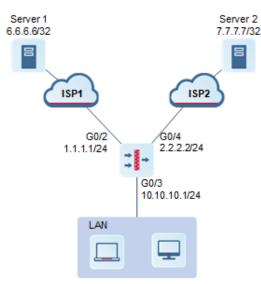
Local U	Jpgrade			0
page a process	nd download the latest upgrade	e file. Then, perform the fail. Note: The file name	ud1.ruijie.com.cn.On the platform, access the Signature Library Upgrade upgrade locally. Do not close or refresh this page during the upgrade cannot contain any Chinese or full-width character. Before the upgrade,	
Download	Download Link:https://seclo	oud1.ruijie.com.cn		
Import	Select an upgrade file.	Browse		
		Upgrade Now	Disable	

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.

Ge0/2	-	m	Routing	untrust	IPv4: Static IP	1.1.1/24	-	1500	Edit
Ge0/3	-	m	Routing	trust	IPv4: Static IP	10.10.10.1/24	-	1500	Edit
Ge0/4	-	m	Routing	untrust	IPv4: Static IP	2.2.2/24	-	1500	Edit

- (2) Configure ISP address library.
 - a Choose Object > ISP Address Library and click Create.

Ruíjie Z Series Firewall	습 Home 🛛 Monitor	₽_ Object ເ⊠ Policy ② System	🖗 🔕 🗈 Network Discovery Network Mgmt Quick Onbo	စ် ရှိ ၃ arding Policy Wizard Customer Service admin
똍 Address	ISP Address Library			
App	🕑 Create 📋 Delete 🕑 Import	🚺 Export 🖸 Refresh		Enter a name. Q
፼ URL Category - Service	□ Name	Description	Last Update Time	Operation
🛱 Time Plan	Default Address Library	-	-	View Details
Q ISP Address Library Over Authentication >				
Certificate				
Content Template >				
🗐 Security Rule Base				

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.

	* Name ISP1		
	Description	le le	
* ISP	Address List		
	€ Create		Enter an IP address or I Q
		IP Address/Range	Operation
		6.6.6.6	Delete
	Total: 1		
3ack Crea	te ISP Address Library		
	* Name ISP2		
	* Name ISP2		
	* Name ISP2 Description		Enter an IP address or I Q
	* Name ISP2 Description Address List	IP Address/Range	Enter an IP address or 1 Q Operation
	* Name ISP2 Description Address List	IP Address/Range 7.7.7.7	

(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 v	
① MTU	1500	
MAC	00:d0:f8:22:37:0b	Restore Default MAC
Link Detection	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 v	
() MTU	1500	
MAC	00:d0:f8:22:37:0d	Restore Default MAC
Link Detection	Link Detection ~	

Ruíjie Z Series Firewall	☆ Home	work 은 Object ເ영 Policy (한 S	stem Metwork Discovery	⊗ Network Mgmt	⊉ Quick Onboarding	Ø Policy Wizard	റ Customer Service	Q admin
☐ Interface >	Address Library Route							
図 Zone 븝 Routing ~	C Refresh					Enter a n	ame or an IP a	Q
Static Routing	Interface		ISP Addres	ss Library				
Intelligent Routing	Ge0/2		ISP1					
Address Library Route Routing Table	Ge0/4		ISP2					
簡 SSL VPN >								
60 DNS								
🔲 DHCP >								
H VRRP								

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

< Back Create Se	ecurity Policy		
Basic Info			
* Name	trust_to_untrust		
Enabled State	• Enable 🔿 Disable		
* Policy Group	Default Policy Group	\sim	
* Adjacent Policy	allow_all	\sim	Before ~
Description	Enter the security policy name desc		
Src. and Dest.			
* Src. Security Zone	trust	\sim	
* Src. Address	lan_users	\sim	
* Dest. Security	untrust	\sim	
Zone			
* Dest. Address	any	~	

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.

Ruffe Z Series Firewall	☆ Home	은 Object 😨 Policy ۞ System	ကြာ 😵 Network Discovery Network Mgmt	▲ Quick Onboarding	Ø Policy Wizard C	റ Customer Service	Q admin
Interface	Address Library Route						
😨 Zone							
🖶 Routing 🗸 🗸	C Refresh				Enter a name	e or an IP a	Q
Static Routing	Interface		ISP Address Library				
Intelligent Routing	Ge0/2		ISP1				
Address Library Route	Ge0/4		ISP2				
Routing Table							
iii SSL VPN >							
60 DNS							
🗩 рнср >							
link Detection							
🔛 VRRP							

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 x *n*.
- When two devices are connected by a single network cable, if the link is disconnected, the services carried on the link will be interrupted. However, when multiple connected interfaces are aggregated and bound, if one member link is disconnected, the device automatically distributes the traffic of the faulty link to other member links. As long as one link is working, the services carried on these interfaces will not be interrupted.

Procedure

(1) Choose Network > Interface > Aggregate Interface.

Ruijie Z Series Firewal	≙ Home	Monitor	Network	,₽= Object	Policy	⊕ System			Retwork Discovery	🕲 Network Mgmt	L Quick Onboardin	Policy Wizard	Customer Service	ر adm
	Aggregat	e Interface												
	⊕ Create	🕝 Enable	O Disable	📋 Delete	C Refr	esh								
Bridge Interface	🗌 Inte	erface Name	Descrip	tion	м	ode	Zone	Connection Type	IP	Aggregat	on Mode Me	mber Interfaces	Operation	
Aggregate Interface								No Data						

(2) Click Create.

The system opens the Add Aggregate Interface page.

< Back Add Aggregat	e Interface
Basic Info	
* Interface Name	Enter an interface name.
Connection Status	Enable O Disable
Mode	Routing Mode Transparent Mode Off-Path Mode
Zone	Select a zone. V O Add Security Zone
Interface Type	WAN Interface LAN Interface
Description	Enter the description.
Member Interface	To-be-selected (0) Select All Selected (0) Clear
	Enter the keyword.
	Ge0/3
	Ge0/4
	Ge0/5
	Ge0/6
	Ge0/7
Address	
* Connection Type	Static Address O DHCP O No IP Address
* IP/Mask	
Next-Hop Address	
Default Route	
Line Bandwidth	
Uplink	Mbps v
Downlink	Mbps v
Access Management	
	en local defense is disabled, access management cannot be configured, and existing configurations become invalid. To configu iense
Permit	HTTPS PING SSH
Advanced Settings	
Aggregation Mode	Static Aggregation \lor
ISP Address Library	ISP Address Library V
① MTU	1500
① MAC	Example: d8:9e:f3:3f:d5:64
Link Detection	Link Detection ~
Reverse Path Limited	
	Save
	Jure

(3) Set parameters of aggregate interface.

Item	Description	Remarks
Interface Name	Name of the aggregate interface.	The interface name can contain only uppercase and lowercase letters and digits. [Example] Ag1
Connection Status	Enables or disables the interface.	[Example] Enable
Mode	 Interface access mode. Routing Mode: forwards traffic based on IP addresses. Transparent Mode: forwards traffic based on MAC addresses. Off-Path Mode: only receives mirrored traffic, but does not forward traffic. 	[Example] Routing Mode
Bridge Interface	Bridge group to which the interface belongs in transparent mode.	This parameter is available when the transparent mode is used. [Example] br0
Zone	Security zone to which the interface belongs.	[Example] trust
Interface Type	Logical attribute of the interface.	[Example] LAN Interface
Description	Interface description, showing the purpose of the interface.	Characters such as `~!#%^&*+\ {};:'"/<>? are not 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			
IP address obtaining method of the interface. Valid values: Static Address and DHCP.If No IP Address is selected, the aggregate interface does not have an IP address. In this case, ensure that another management channel is configured, for example, you can access the device using the IP address of another interface.		This parameter is available when the Routing Mode is used. [Example] Static Address			
IP/Mask	IPv4 address and mask of the interface.	This parameter is available when Connection Type is set to Static Address. [Example] 192.168.1.1/24			
Next-Hop Address	Next-hop address of the forwarded data. Generally, it is the address of the next routing device.	This parameter is available when Connection Type is set to Static Address. [Example] 192.168.1.2/24			
Default Route	Whether to generate the default route.	[Example] Enabled			
Line Bandwidth	Limited interface bandwidth, including upload bandwidth and download bandwidth.	Enter the bandwidth value and select a unit. The unit can be kbps or mbps. When kbps is selected as the unit, the value ranges from 1 to 100,000,000. When mbps is selected as the unit, the value ranges from 1 to 100,000. [Example] 100 kbps			

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 Setting	s					
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 <u>8.22 Link Detection</u> .				

🛕 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**.

Aggregate Inte	rface							
 Generate Ge	able 🚫 Disable 🛅 Del	ete 😋 Refresh						
Interface N	ame Description	Mode	Zone	Connection Type	IP	Aggregation Mode	Member Interfaces	Operation
ag1	-	Transparent	trust	-	-	Static Aggregation		Edit 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.

Product Cookbook

Link Detection	Detection Log					
transmitted over				d, the system immediately disables caution.	the line to ensure that ap	plication traffic can be
Link Detection						
😉 Create 🔟 Dele	te 😋 Refresh				Enter	a name or an inte Q
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	Enter the link detection name.								
 Minimum Survivability Nodes 	1								
Detection Node									
① Detection Node	• Create Delete								
	Node Name	Protocol T	o-Be-Detected Dest. IP	Domain Name	Port Number	Outbound Int	erface	Next-Hop Address	Detection
	4						No Data		
	10 / Page Total:0							Go to 1	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
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.

Link Detection	Detection Log							
C Refresh				Time	 2024-04-10	to	2024-04-10	Enter details co
		Time					Details	
			No Data					

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.

Back Edit Physical I	nterface	
Basic Info		
Interface Name	Ge0/2	
Description		
Connection Status	• Enable 🔿 Disable	
Mode	• Routing Mode 🔿 Transparent Mode 🔾	Off-Path Mode
*Zone	trust \lor \ominus	Add Security Zone
Interface Type	• WAN Interface O LAN Interface	
Address		
ІР Туре	IPv4 IPv6	
Connection Type	• Static Address O DHCP O PPPoE	○ No IP Address
*IP/Mask	30.0.1/24	
Next-Hop Address		
Default Route		
Line Bandwidth		
Uplink	Mbps ~	
Downlink	Mbps ~	
Access Management		
Permit	🗹 HTTPS 🗹 PING 🗹 SSH	
Advanced		
ISP Address Library	ISP Address Library	
① MTU	1500	
MAC	48:81:d4:cd:13:6d	estore Default MAC
Link Detection	test v	
Reverse Path Limited		
		Save

K Back Edit	Static Rou	ting	
	IP Туре	IPv4	
* Dest. IP	Range/Mask	60.0.0/24	
Next-Hop Address			
	Interface	Ge0/2	\sim
_	* ① Priority	5	
Ľ	ink Detection	test	~
	Description		

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 <u>Figure 8-15</u>, 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.

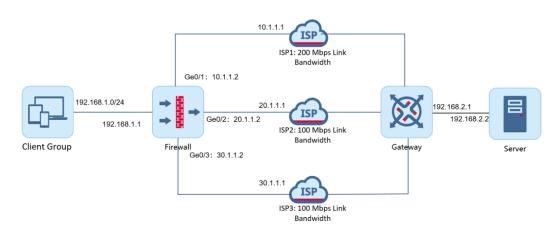


Figure 8-15 Topology of a Network with Specific Routes

(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
 - a Choose Network > Routing > Egress Load Balancing > Global Config.
 - b Select Bandwidth-based and Uplink Bandwidth from the Balancing Mode drop-down lists.

Global Config	Session Info				
 Balancing Mode 	Bandwidth-based	~	Uplink Bandwidth	\sim	Save
⊘ Enable 🚫 Dis	sable C Refresh				

- 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**.

Ruffic Z Series Firewall	습 Home 🛛 Monitor 🕕	Network 🔑 Object 😳 Policy 🔅 Syst	tem	Quick Onboarding Policy V) A A Vizard Customer Service admin
Interface Physical Interface	K Back Edit Interface				
Subinterface	Basic Info				
Bridge Interface	Interface Name	Ge0/1			
Aggregate Interface	Interface Bandwidth				
Tunnel Interface	OUplink Bandwidth	200	Mbps ~		
l Zone	①Downlink Bandwidth	200	Mbps ~		
🖶 Routing 🗸 🗸	① Threshold				
Static Routing	* Uplink Load Threshold	80	96		
Egress Load Balancing					
Address Library Route	* Downlink Load Threshold	80	96		
OSPF	Weight				
Routing Table	* Weight	200000			
Routing Policy	Priority				
SSL VPN >	* Priority	1			
IPsec VPN >	Max. Connections				
DHCP O	* (1) Max. Connections	2000			
W Link Detection					
☑ Neighbor Status >					
					C
			Save		
E					

Configure the parameters for Ge0/2 and click **Save**.

Ruffie Z Series Firewall	습 Home 🛛 Monitor 🔮 N	Network P= Object	© System		
Interface ~ Physical Interface Subinterface Bridge Interface	Back Edit Interface Basic Info Interface Name	Ge0/2			
Aggregate Interface Tunnel Interface ☑ Zone ⇔ Routing ~	Interface Bandwidth OUplink Bandwidth ODownlink Bandwidth	100	Mbps v Mbps v		
Static Routing Intelligent Routing Egress Load Balancing	Threshold Uplink Load Threshold Downlink Load Threshold		96 96		
Address Library Route OSPF Routing Table Routing Policy	Weight * Weight Priority	100000			
SSLVPN → El IPsec VPN → El DNS →	* Priority Max. Connections				
 ➡ DHCP > ⊗ Link Detection ➡ VRRP ➡ Neighbor Status > 	* 🕐 Max. Connections	2000			
					💽 Consult
Ξ			Save		

Configure the parameters for Ge0/3 and click **Save**.

Ruffie Z Series Firewall	🛆 Home 🛛 Monitor 🔀 N	Network 🔑 Object 🐨 Policy 🐵 Syst	tem	Quick Onboarding Policy Wizard	이 오 Customer Service admin
🖾 Interface 🗸 🗸	< Back Edit Interface				
Physical Interface	Basic Info				
Subinterface Bridge Interface	Interface Name	Ge0/3			
Aggregate Interface	Interface Bandwidth				
Tunnel Interface	()Uplink Bandwidth	100	Mbps ~		
圆 Zone					
🖶 Routing 🗸 🗸	①Downlink Bandwidth	100	Mbps ~		
Static Routing	① Threshold				
Intelligent Routing	* Uplink Load Threshold	80	96		
Egress Load Balancing	* Downlink Load Threshold	80	%		
Address Library Route	Weight				
OSPF Routing Table	* Weight	100000			
Routing Table					
SSL VPN	Priority				
IPsec VPN >	* Priority	1			
ten dins →	Max. Connections				
园 DHCP >	* () Max. Connections	2000			
link Detection					
URRP					
Neighbor Status >					
					A
					.
					Ę.
			_		
æ			Save		
11					

(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.

IPv4 Address	IPv4 Address Group	IPv6 Address	IPv6 Address Group
⊕ Create 🔟 De	elete C Refresh		
Name	IP Addre	ess/Range	
client-subne	et 192.168.	1.0/24	
server-subn	et 192.168.	2.0/24	

Choose Policy > Security Policy > Security Policy and click Create to create a security policy.

< Back Edit Se	curity Policy	
Basic Infe	,	
* Nam	e allow-outbond	
Enabled State	e Enable	
* Policy Group	Default Policy Group	⊙ Add Group
Description	n Enter the security policy name desc	
Src. and Dest	L	
Src. Security Zon	e any \lor	
* Src. Addres	s client-subnet \sim	
Src. Region	n any ~	
Dest. Security Zon	e any \checkmark	
* Dest. Addres	s server-subnet \lor	
Dest. Regio	n any ~	
Servio	e any \lor	
Action Option	n 💿 Permit i Deny	
	App、User、Effective Time \vee	
Content Securit	1	
Intrusion Prevention	n Disable	
Virus Protection	1 Disable	
URL Filtering	Disable	
Keyword Filtering	Disable	
Advance	d Settings	
		Save

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 Туре	IPv4					
* Dest. IP Range/Mask	192.168.2.0/24					
Next-Hop Address	10.1.1.1					
Interface	Ge0/1 ~					
* ① Priority	5					
Link Detection	Link Detection V					
Description	ISP1 route					
	11					

Create a static route to the server through the ISP2 link and click **Save**.

< Back	Edit Static Rou	ting	
	IP Туре	IPv4	
*[Dest. IP Range/Mask	192.168.2.0/24	
	Next-Hop Address	20.1.1.1	
	Interface	Ge0/2 v	
	* () Priority	5	
	Link Detection	Link Detection ~	
	Description	ISP2 route	

Create a static route to the server through the ISP3 link and click Save.

< Back Edit Static Rou	ting
ІР Туре	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 \lor
Description	ISP3 route
	1

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-base	ed v Uplink Bandwidth	 ✓ Save 			DNS Proxy:Disabled Configure
Service Enable Disable	h			Enter an ir	nterface name. Q
Interface Name	Uplink Bandwidth	Downlink Bandwidth	Uplink Load Threshold	Downlink Load Threshold	Operation
Ge0/2	100Mbps	100Mbps	80	80	Edit
Ge0/3	100Mbps	100Mbps	80	80	Edit
Ge0/1	200Mbps	200Mbps	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.

Traffic Trend



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.

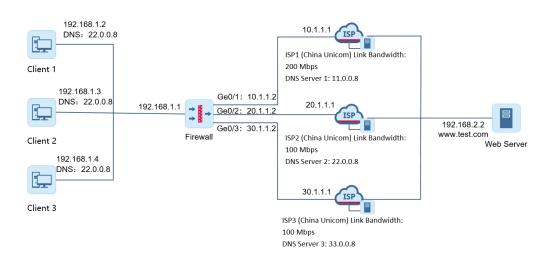


Figure 8-16 Topology of DNS Transparent Proxy

🚺 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
 - a Choose Network > Routing > Egress Load Balancing > Global Config.
 - b Select Bandwidth-based and Uplink Bandwidth from the Balancing Mode drop-down lists.

Global Config	Session Info			
Balancing Mode	Bandwidth-based	V Uplink Bandwidth	~	Save
Senable Senable	sable C Refresh			

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**.

Ruffie Z Series Firewall	🛆 Home 🛛 😔 Monitor 🔒 N	Network 🔑 Object 🖾 Policy 🖨 Sy	stem	L Quick Onboarding	Policy Wizard Customer Service admin
Interface Physical Interface	K Back Edit Interface				
Subinterface	Basic Info				
Bridge Interface	Interface Name	Ge0/1			
Aggregate Interface	Interface Bandwidth				
Tunnel Interface	OUplink Bandwidth	200	Mbps ~		
団 Zone	①Downlink Bandwidth	200	Mbps ~		
🖶 Routing 🛛 🗸	① Threshold				
Static Routing			-		
Intelligent Routing Egress Load Balancing	* Uplink Load Threshold		96		
Address Library Route	* Downlink Load Threshold	80	96		
OSPF	Weight				
Routing Table	* Weight	200000			
Routing Policy	Priority				
SSL VPN >	* Priority	1			
IPsec VPN >	Max. Connections				
	* (1) Max. Connections	2000			
S Link Detection	- U Mac connections	2000			
URRP					
🖾 Neighbor Status 🔷 🗧					
					(e)
					onsult
			Save		
Œ					

Configure the parameters for Ge0/2 and click **Save**.

Ruffie Z Series Firewall	습 Home 🛛 Monitor 🔮 N	Network 🔑 Object 🖾 Policy	© System	Quick Onboarding Policy Wizard Customer Service admin
Interface ~ Physical Interface Subinterface Bridge Interface	Back Edit Interface Basic Info Interface Name	Ge0/2		
Aggregate Interface Tunnel Interface 2 Zone Cone	Interface Bandwidth OUplink Bandwidth ODownlink Bandwidth	100	Mbps v Mbps v	
Static Routing Intelligent Routing Egress Load Balancing	Threshold * Uplink Load Threshold * Downlink Load Threshold		56 56	
Address Library Route OSPF Routing Table Routing Policy	Weight * Weight Priority	100000		
⊖ SSLVPN → ☐ IPsec VPN → ☐ DNS →	* Priority Max. Connections			
 ➡ DHCP > ⊗ Link Detection ➡ VRRP ☑ NR8P ☑ Neighbor Status > 	* 🕐 Max. Connections	2000		
				ę
E			Save	

Configure the parameters for Ge0/3 and click **Save**.

Ruijie Z Series Firewall	🛆 Home 🛛 😡 Monitor 🔀 N	letwork දී Object ල Policy ල Sy	stern	E Quick Onboarding	Ø Policy Wizard	Customer Service	오 admin
🖺 Interface 🗸 🗸	< Back Edit Interface						
Physical Interface	Basic Info						
Subinterface Bridge Interface	Interface Name	Ge0/3					
Aggregate Interface	Interface Bandwidth						
Tunnel Interface	OUplink Bandwidth	100	Mbps ~				
厦 Zone	ODownlink Bandwidth	100	Mbps ~				
🖶 Routing 🛁 👻		100	тыра				
Static Routing	① Threshold						
Intelligent Routing	* Uplink Load Threshold		%				
Egress Load Balancing Address Library Route	* Downlink Load Threshold	80	%				
OSPF	Weight						
Routing Table	* Weight	100000					
Routing Policy	Priority						
SSL VPN	* Priority	1					
IPsec VPN >	Max. Connections						
dns >							
■ DHCP > Sink Detection	* () Max. Connections	2000					
WRRP							
☑ Neighbor Status →							
							0 Com
							nsult
			Save				
Ē							

(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.

IPv4 Address	IPv4 Address Group	IPv6 Address	IPv6 Address Group
 Generate Generate Denerate 	elete C Refresh		
Name	IP Addre	ess/Range	
client-subn	et 192.168.	1.0/24	
server-subr	net 192.168.	2.0/24	

Choose Policy > Security Policy > Security Policy and click Create to create a security policy.

< Back	Edit Secu	urity Policy	
	Basic Info		
	* Name	allow-outbond	
E	nabled State	Enable	
*	Policy Group	Default Policy Group V	⊙ Add Group
	Description	Enter the security policy name desc	
Sr	c. and Dest.		
Src. S	ecurity Zone	any \vee	
*	Src. Address	client-subnet \sim	
	Src. Region	any \vee	
Dest. S	ecurity Zone	any \vee	
* D	est. Address	server-subnet \sim	
	Dest. Region	any \vee	
	Service	any \vee	
A	ction Option	• Permit 🔿 Deny	
		App、User、Effective Time \sim	
Cont	ent Security		
Intrusio	n Prevention	Disable	
Viru	is Protection	Disable	
	JRL Filtering	Disable	
Keyw	ord Filtering	Disable	
	Advanced	Settings	
			Save

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	China Unicom (CHN)	\sim		
① MTU	1500			
MAC	00:d0:f8:22:36:ec		Restore Default MAC	
Link Detection	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	China Telecom (CHN)	\otimes	
① MTU	1500		
MAC	00:d0:f8:22:36:ed		Restore Default MAC
Link Detection	Link Detection	~	
Reverse Path Limited			

Click **Edit** in the **Operation** column of Ge0/3 and associate the interface with the address library of China Telecom.

Advanced			
ISP Address Library	China Telecom (CHN) $\qquad \lor$		
① MTU	1500		
MAC	00:d0:f8:22:36:ee	Restore Default MAC	
Link Detection	Link Detection \sim		
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**.

< Back Edit Proxy Pol	icy	
Basic Info		
* Name	dp-policy1	
Enabled State	• Enable 🔿 Disable	
Adjacent Policy	Select a policy.	After
Description		
Src. and Dest.		
* Src. Address	client-subnet	~
* Dest. Address	server-subnet	~
* () Service	dns-u,dns-t	~
Action Settings		
Proxy Action	Proxy O No Proxy	

c Configure a proxy interface.

Set the primary DNS server address of Ge0/1 to 11.0.0.8 and click **Save**.

< Back Edit DNS Proxy		
* Outbound Interface	Ge0/1 ~	
* Active DNS Server Address	11.0.0.8	
Standby DNS Server Address	Enter	
DNS Probe	Select ~	Add Link Detection

Set the primary DNS server address of Ge0/2 to 22.0.0.8 and click Save.

< Back Edit DNS Proxy		
* Outbound Interface	Ge0/2 ~	
* Active DNS Server Address	22.0.0.8	
Standby DNS Server Address	Enter	
DNS Probe	Select ~	⊕ Add Link Detection

Set the primary DNS server address of Ge0/3 to 33.0.0.8 and click Save.

K Back Edit DNS Proxy		
* Outbound Interface	Ge0/3 ~	
* Active DNS Server Address	33.0.0.8	
Standby DNS Server Address	Enter	
DNS Probe	Select v	Add Link Detection

6. Verification

• Checking the MLLB Configuration

Choose **Network > Routing > Egress Load Balancing** to check the balancing mode and interface bandwidth.

Globa	al Config Session Info						
) Balan	Bandwidth-based	V Uplink Bandwidth	✓ Save			DNS Proxy:Enabled	Configure
🕑 Ena	able 🚫 Disable 🖸 Refresh					Enter an interface name.	Q
	Interface Name	Uplink Bandwidth	Downlink Bandwidth	Uplink Load Threshold	Downlink Load Thre	shold Operation	
	Ge0/2	100Mbps	100Mbps	80	80	C Edit	
	Ge0/3	100Mbps	100Mbps	80	80	C Edit	
	Ge0/1	200Mbps	200Mbps	80	80	C Edit	

• Checking ISP Routes

Choose Network > Routing > Address Library Route to check ISP equal-cost routes.

Address Library Route	
C Refresh	Enter a name or an IP address, Q
Interface ISP Address Libr	ary
Ge0/1 China Unicom (C	HN)
Ge0/2 China Telecom (C	HN)
Ge0/3 China Telecom (C	

• 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.

Routing Mod	de Egress Load Balancing \vee				
Proxy Interf	face Exclude Domain Name Proxy I	Policy			
Create	🗓 Delete 🔗 Enable 🚫 Disa	ble C Refresh		E	inter an interface name or IP address. Q
	Outbound Interface	Monitoring Status	Active DNS Server Address	Standby DNS Server Address	Operation
	Ge0/1	Not detected.	11.0.0.8	-	Edit Delete
	Ge0/2	Not detected.	22.0.0.8	-	Edit Delete

Choose **Network > DNS > DNS > DNS Transparent Proxy** and click the **Proxy Policy** tab to check the policy configuration.

e Farece Lee	d Ralancing							
e Egress Load	u Balancing							
ce Exclude Do	main Name	Proxy Policy						
[name or IP address.
Delete 🔹	🕑 Enable 🔤 🤇	🛇 Disable 🛛 🕚 Move	S Clear Hit Record	G Refresh			Enter a policy	name of IP address.
	ce Exclude Do	ce Exclude Domain Name	ze Exclude Domain Name Proxy Policy	ze Exclude Domain Name Pray Policy				

• 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.

Interface:Ge0/1		Uplink	 Downlink 		
18.00Kbps					
15.00Kbps					
12.00Kbps	V V	V V	V V	V V V	V
9.00Kbps					
6.00Kbps					
3.00Kbps					
Obps	21:05	21:05	21:07	21:08	21:09
Interface:Ge0/2		Uplink	Downlink		
10.00Kbps					
8.00Kbps					
6.00Kbps	V V	V V V	V V	VV	V V
4.00Kbps					
2.00Kbps					
Obps	21:05	21:05	21:07	21:08	21:09
Interface:Ge0/3		Uplink	Downlink		
10.00Kbps					
				_	
8.00Kbps					
6.00Kbps					
4.00Kbps					
2.00Kbps					

8.23.4 Configuring MLLB Based on Link Priority for Intelligent Routing

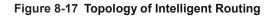
1. Applicable Products and Versions

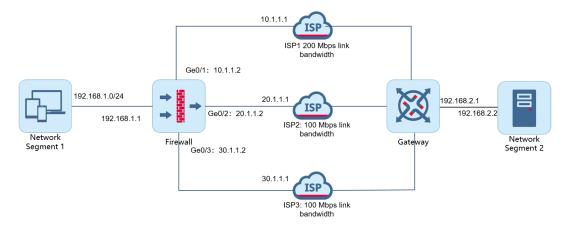
Table 8-19Products and Versions

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 <u>Figure 8-17</u>, 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.





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.
 - a 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.

IPv4 Address	IPv4 Address Group	IPv6 Address	IPv6 Address Group				
IFV4 Address	IF V4 Address Group	IF VO Address	IF VO Address Group				
🕒 Create 🗓 De	⊕ Create Image: Delete C Refresh						
Name	IP Addre	ess/Range					
client-subne	et 192.168.	1.0/24					
server-subn	net 192.168.	2.0/24					

b Choose **Policy > Security Policy > Security Policy** and click **Create** to create a security policy.

< Back Edit Sec	urity Policy	
Basic Info		
* Name	allow-outbond	
Enabled State	Enable	
* Policy Group	Default Policy Group ~	⊙ Add Group
Description	Enter the security policy name desc	
Src. and Dest.		
Src. Security Zone	any \lor	
* Src. Address	client-subnet \sim	
Src. Region	any \lor	
Dest. Security Zone	any \lor	
* Dest. Address	server-subnet \lor	
Dest. Region	any \lor	
Service	any \lor	
Action Option	• Permit O Deny	
	App、User、Effective Time \sim	
Content Security		
Intrusion Prevention	Disable	
Virus Protection	Disable	
URL Filtering	Disable	
Keyword Filtering	Disable	
Advanced	Settings	
		Save

- 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	t Routing	
Basic Info		
* Name	pbr_001	
Enabled State	• Enable 🔿 Disable	
Adjacent Policy	Select a policy. \sim	After \lor
Description		
Matching Conditions		
Inbound Interface	any \lor	
Src. Address	client-subnet \sim	
Dest. Address	server-subnet \sim	
Service	any \lor	
User	any \lor	
Арр	InternetFinance \sim	
Effective Time	any ~	⊕ Add One-Off Time Plan ⊕ Add Cyclic Time Plan
Action Settings		
Action Option	• Forwarding O No Intelligent Routing	J
Outbound Interface Type	 Single Interface Multiple Interface 	25
* Intelligent Routing Mode	Based on Link Priority \sim	
Outbound Interface List	🕒 Create 📋 Delete 🙄 Refresh	

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		\otimes
Basic Info		
* Interface Name	Ge0/1 ~	
* Next-Hop Address	10.1.1.1	
① Threshold		
Uplink Load Threshold		%
Downlink Load Threshold		%
Weight		
Weight		
Priority		
Priority	10	
Max. Connections		
Max. Connections	2000	
Add Outbound Interface		\otimes
Basic Info		
* Interface Name	Ge0/2 ~	
* Next-Hop Address	20.1.1.1	
① Threshold		
Uplink Load Threshold	80	%
Downlink Load Threshold	80	%
Downlink Load Threshold Weight	80	
	80	
Weight		
Weight Weight		
Weight Weight Priority	100000	
Weight Weight Priority Priority	100000	

Cancel

Confirm

Add Outbound Interface		\otimes
Basic Info		
basic into		
* Interface Name	Ge0/3 ~	
* Next-Hop Address	30.1.1.1	
① Threshold		
Uplink Load Threshold		%
Downlink Load Threshold	80	%
Weight		
Weight	100000	
Priority		
Priority	1	
Max. Connections		
Max. Connections	2000	
	Confirm Cancel	

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											
<u> </u>		conditions in a rule are in figured for a matching co		1 C C C C C C C C C C C C C C C C C C C								×
	🛅 Delete	Senable Senable	Move	S Clear Hit Record	T Cus	tom Field	C Refresh			Enter an IP add	ress or a service.	Q
Prio	ority Name	Inbound Interface	Src. Address	Dest. Address	Service	Арр	User	Effective Time	Action	Intelligent Routing Mode	Outbound Inter	face
□ 1	l pbr_001	any	client-subnet	server-subnet	any	Interne	any	any	Forwarding	Based on Link Priority	Ge0/1,Ge0/2,Ge	0/3

Action Settings								
Action Option	 Forwarding 	O No Int	elligent Routing					
Outbound Interface Type	 Single Interf 	ace 💿 M	ultiple Interfaces	•				
* Intelligent Routing Mode	Based on Lini	c Priority						
Outbound Interface List	⊖ Create	🔟 Delete	C Refresh					
		Interface		Priority	Next-Hop Address	Uplink Load Threshold	Downlink Load Threshold	Operation
		Ge0/1		10	10.1.1.1	80%	80%	Edit Delete
		Ge0/2		5	20.1.1.1	80%	80%	Edit Delete
		Ge0/3		1	30.1.1.1	80%	80%	Edit Delete
	Total: 3							
Link Detection	Link Detectio	n		 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

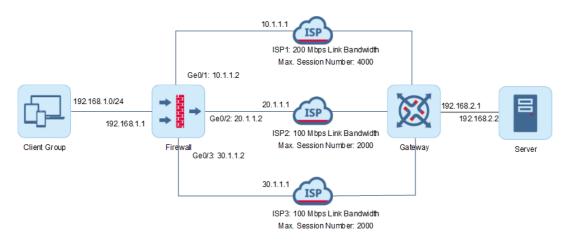
Table 8-20Products and Versions

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 <u>Figure 8-18</u>, 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.





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
 - a Choose Network > Routing > Egress Load Balancing > Global Config.
 - b Select Based on Bandwidth+Session from the Balancing Mode drop-down list.

Global Config	Session Info	
Balancing Mode	Based on Bandwidth+Session	✓ Save
Senable	Disable C Refresh	

- 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**.

Ruíjie Z Series Firen	will 😭 Home 🤤 Monitor 🕕 🕅			ی ای کی
	C Back Edit Interface			
	Basic Info			
	Interface Bandwidth			
	OUplink Bandwidth	200	Mbps v	
	①Downlink Bandwidth	200	Mbps ~	
	() Threshold			
Intelligent Routing	* Uplink Load Threshold	80	%	
Egress Load Balancing	 Downlink Load Threshold 	80	%	
	Weight			
	* Weight	1000000		
	Priority			
	Priority	1		C
	Max. Session Number			
	> * () Max. Session Number	4000		•
🛞 Link Detection				
	5			
	=		Save	

Configure the parameters for Ge0/2 and click **Save**.

Ruijie Z Series Firewall		k Az Object & Policy @ System	표
🖾 Interface 🗸 🗸	< Back Edit Interface		
Physical Interface Subinterface	Basic Info		
Bridge Interface	Interface Name Ge0/2		
Aggregate Interface	Interface Bandwidth		
Tunnel Interface	OUplink Bandwidth 100	Mbps ~	
图 Zone li Routing ~	ODownlink Bandwidth 100	Mbps ~	
Static Routing	① Threshold		
Intelligent Routing	* Uplink Load Threshold 80	96	
Egress Load Balancing	* Downlink Load Threshold 80	96	
Address Library Koute	Weight		
Routing Table	* Weight 100	0000	
Routing Policy	Priority		
SSL VPN →	* Priority 1		
	Max. Session Number		
貝 DHCP >	* () Max. Session Number 200	0	U
Link Detection			
III VRRP			
		Save	
臣			

Configure the parameters for Ge0/3 and click Save.

Ruifie Z Series Firewall	ර Home ම Monitor 🕀 Network දී Object හ Policy ම Sys	tem	Quick Onboarding Policy Wizard Customer Service admin
🗐 Interface 🗸 🗸	Back Edit Interface		
Physical Interface	Basic Info		
Subinterface	Interface Name Ge0/3		
Bridge Interface			
Aggregate Interface	Interface Bandwidth		
Tunnel Interface	①Uplink Bandwidth 100	Mbps 🗸	
图 Zone	ODownlink Bandwidth 100	Mbps ~	
Static Routing	() Threshold		
Intelligent Routing	Uplink Load Threshold 80	96	
Egress Load Balancing			
Address Library Route	* Downlink Load Threshold 80	96	
OSPF	Weight		
Routing Table	* Weight 1000000		
Routing Policy	Priority		
■ SSL VPN >	* Priority 1		
IPsec VPN >	- Priority 1		8
	Max. Session Number		Corrul
DHCP >	* ③ Max. Session Number 2000		
S Link Detection			
III VRRP			
🖾 Neighbor Status 🔷 🗧		_	
		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.

IPv4 Address	IPv4 Address Group	IPv6 Address	IPv6 Address Group				
Name	IP Addro	ess/Range					
client-subn	et 192.168.	1.0/24					
server-subn	net 192.168.	2.0/24					

Choose Policy > Security Policy > Security Policy and click Create to create a security policy.

< Back Edit Secu	urity Policy	
Basic Info		
* Name	allow-outbond	
Enabled State	Enable	
* Policy Group	Default Policy Group \lor	⊙ Add Group
Description	Enter the security policy name desc	
Src. and Dest.		
Src. Security Zone	any \vee	
* Src. Address	client-subnet \sim	
Src. Region	any \checkmark	
Dest. Security Zone	any \lor	
* Dest. Address	server-subnet \sim	
Dest. Region	any \lor	
Service	any \lor	
Action Option	• Permit 🔿 Deny	
	App、User、Effective Time $\ \sim$	
Content Security		
Intrusion Prevention	Disable	
Virus Protection	Disable	
URL Filtering	Disable	
Keyword Filtering	Disable	
Advanced	Settings	
		Save

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 $\ensuremath{\textbf{Save}}$.

< Back Edit Static Routing						
IP Туре - I	Pv4					
* Dest. IP Range/Mask	192.168.2.0/24					
Next-Hop Address	10.1.1.1					
Interface	Ge0/1 V					
* ① Priority	5					
Link Detection	Link Detection \sim					
Description	ISP1 route					

Create a static route to the server through the ISP2 link and click **Save**.

< Back Edit Static Rou	ting
ІР Туре	IPv4
* Dest. IP Range/Mask	192.168.2.0/24
Next-Hop Address	20.1.1.1
Interface	Ge0/2 ~
* ① Priority	5
Link Detection	Link Detection V
Description	ISP2 route

Create a static route to the server through the ISP3 link and click **Save**.

< Back Edit Static Rou	ting
ІР Туре	IPv4
* Dest. IP Range/Mask	192.168.2.0/24
Next-Hop Address	30.1.1.1
Interface	Ge0/3 ~
* ① Priority	5
Link Detection	Link Detection V
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.

Sloba	I Config Session Info						
alancir	ng Mode Based on Bandwidth	h+Session	Save				
Enal	ble 🚫 Disable 🖸 Refresh					Enter an	interface name.
	Interface Name	Max. Session Number ①	Uplink Bandwidth	Downlink Bandwidth	Uplink Load Threshold	Downlink Load Threshold	Operation
	Ge0/1	Max. Session Number ① 4000 🗹	Uplink Bandwidth 200Mbps	200Mbps	Uplink Load Threshold 80%	Downlink Load Threshold	Operation 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.

Traffic Trend

Interface:Ge0/1		 Uplink D 	ownlink		
0.00Kbps		opini. O			
3.00Kbps		- , , , , , , , , , , , , , , , , , , ,			
5.00Kbps	VV	V V	V V V		V
LOOKbps					
2.00Kbps					
0bps	20:58	20:59	21:00	21:01	
Interface:Ge0/2		Uplink D	ownlink		
i.00Kbps		 opink Di 	pwname		
1.00Kbps					
3.00Kbps		VV		/ V V	V
S.OOKDPS					
1.00Kbps					
	20.58	20:59	21:00	21:01	
.00Kbps Obps	20:58			21.01	
0bps	20:58		21:00 Swelink	21:01	
0bps	20:58			21.01	
0bps Interface:Ge0/3 5.00Kbps K.00Kbps	20:59			21:01	V-
Interface:Ge0/3 5.00Kbps 5.00Kbps	2058			21.01	V
LOOKbps Obps Interface:Ge0/3 LOOKbps LOOKbps ZOOKbps	2058			2101	V-
0bps Interface:Ge0/3 5.00Kbps K.00Kbps	2059			21:01	V-

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.

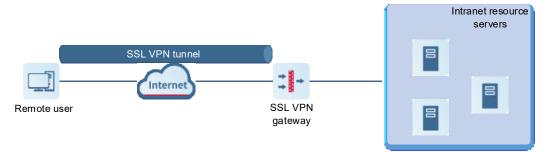
Interface Name	Uplink Bandwidth	Downlink Bandwidth	Uplink Load Threshold	Downlink Load Threshold	Operation
Ge0/1	200Mbps	200Mbps	80%	80%	Edit
Ge0/2	100Mbps	100Mbps	80%	80%	Edit
Ge0/3	100Mbps	100Mbps	80%	80%	Edit

 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).

icense Config			
-			
. Before activating a device, register on and log in to Kuijie Secur latform is used for activating and changing device licenses and r	re Cloud Platform at (https://secloud1.ruijie.com.cn must be kept confidential.)	n). On the platform, access the Device Authorization page, and generate a	license file: (The account of this
. Select an activation mode based on device connection status.F	or threat intelligence, only online activation is su	upported.	
Activate Online		You can choose to perform manual activation.	
Activate Now	. =•	Activate Manually	
evice SN:MACCFXZ32005K Copy			
icense Info			How to Obtain License
			How to Obtain License
Performance License			
	formance:2G) Performance to Be Added:0G		3G /3G
vallable Performance:3G(Basic Performance:1G+Added New Per	formance:2G) Performance to Be Added:0G		3G /3G
Performance License wallable Performance:3G(Basic Performance:1G+Added New Per SL VPN License (Firewall Mix Performance)	formance:2G) Performance to Be Added:0G		3G /3G
vallable Performance:3GBasic Performance:1G+Added New Per		sions)	3G /3G
vallable Performance:3GBasic Performance:1G+Added New Per SSL VPN License (Firewall Mix Performance) Jax. Concurrent License Sessions102(20 concurrent free license		slons)	3G /3G
vallable Performance:3G(Basic Performance:1G+Added New Per		slons)	3G /3G

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

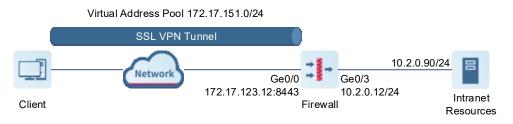
Table 8-21 Products and Versions

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	 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	 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.

< Bac	Edit Physical I	nterface
	Basic Info	
	Interface Name	Ge0/0
	Description	
	Connection Status	Enable Disable
	Mode	Routing Mode Transparent Mode Off-Path Mode
	* Zone	untrust V Add Security Zone
		WAN Interface LAN Interface
	Address	
	IP Туре	IPv4 IPv6
	Connection Type	Static Address O DHCP O PPPoE
	* IP/Mask	172.17.123.12/24
	* Next-Hop Address	172.17.123.1
	Default Route	
	Line Bandwidth	
	Uplink	Select V
	Downlink	Select V
	Access Management	
	Permit	🛛 HTTPS 🕑 PING 🕑 SSH
	Advanced	
	ISP Address Library	ISP Address Library V
	0 MTU	1500
	MA	Restore Default MAC
	Link Detection	Link Detection V
		Save

- 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.

User Management			
Default Authentication Domain			
User Structure Oreate User Group	E User Group Members Add ∨	Create User Group	\otimes
 옷 All Groups 옷 jmeter 옷 group1 	- Group	User Group Name group1 Parent Group Enter or select a value.	
		Save Cancel	

- c Click Save.
- d Click **Add** and choose **User**.

User Management			
Default Authentication Domain	\sim		
User Structure	E	User Group Members	
Create User Group		Add V 🔟 Delete 🔗 Enable 🚫 Disable 😋 Refresh More V	
 ペ All Groups 		User I=me Group	Account Expiry Date
& jmeter		Users	
& group1			

- 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	user1
Enabled State	• Enable 🔿 Disable
Displayed Username	Enter the displayed username.
* Parent Group	/default/group1 v
Description	Enter user description.
Password	
* ① Password	
* Confirm Password	•••••
Advanced Settings	

- 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	example
() Gateway Type	Exclusive Shared
* Gateway Address	Ge0/0(Off 172.17.123.12/26 V 172.17.123.12 O Port Number 8443
	· Create
Domain Name	Enter a domain name.
Intranet DNS	Enter an intranet DNS server address.
•	Create
Preferred DNS	O Intranet DNS Customer DNS
ET Advanced	
Protocol	
* Protocol Version	✓ TLS1.2 □ TLS1.1 □ TLS1.0
* Algorithm Suite	🛛 TLS-ECDHE-RSA-WITH-AES128-CBC-SHA256 🛛 🛃 TLS-ECDHE-RSA-WITH-AES256-CBC-SHA384 🛛 🗹 TLS-RSA-WITH-AES256-CBC-SHA
Gateway Certificate	default ~
Concurrency Control	
* () Max. Concurrent Users	20

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	O Login Control
Authentication	
* 🕕 User Authentication Domain de	efault ③ Create User Authentication Domain
Prevent Brute-Force Attack	
User Lockout	D
* ① Max. User Attempts 5	Time * O Lockout Period 300 Second
Single IP Lockout	D
* () Max. Single IP Attempts 5	Time * () Lockout Period 300 Second
Login Verification	
() Graphic Verification	
* ① Enable upon 0	Consecutive Input Errors
① Hardware Signature Verification	
* ① Maximum Signatures Bound to Each 3	
User Auto Hardware Signature Approval 	
Auto Hardhard Signature Approval O	
Auto Approval of Trusted Public Terminals	
Idle Timeout	
* ① The idle status will time out after 3	0 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

Add SSL VPN Gateway		
⊘ Basic Config	Add Tunnel Resource Group	
Basic Confia	* Tunnel Resource resource_grp_1	
* ① Available IP Ranges 172.17.151.0/255.255.255.0	Group Name	
Tunnel Mode Full Tunnel Split Tunnel	Description Enter the tunnel re group description Name	
* ① Tunnel Access Keep-Alive Interval 30 S	S Resource Config List Resource Type IP Subnet Domain Name	
* Max. Disconnection Time 180 S Enable SSL VPN Private Line		
Note: When this function is er	r Protocol any V	
Tunnel Resource List	Resource Name	
• Create I Delete	Confirm Cancel	
Resource Group Name Resource	No Data	
	Total: 0	
	Confirm Cancel	
Total: 0		

Click **Confirm** to create the resource. Then click Confirm to create the resource group, as shown in the following figure.

⊘ Basic Config	🖉 Login Control
Basic Config	
* ① Available IP Ranges	172.17.151.0/255.255.255.0
() Tunnel Mode	G Full Tunnel O Split Tunnel
* ① Tunnel Access Keep-Alive Interval	30 Second
* 🕕 Max. Disconnection Time	180 Second
Enable SSL VPN Private Line	 Note: When this function is enabled, a private line where only the SSL VPN can be accessed will be set up after you log in to the SSL VPN.
Tunnel Resource List	
	Delete
Resource Gr	roup Name Resource
resource_gr	p_1 resource_1
Total: 1	

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

Create Delete		Add License	
Policy Name	User/User Group	* Authorization policy_1 Policy Name	
] default	/default	* User/User group1 @ Group	
		IP Tunnel resource_grp_1 ® Resource	
otal: 1		Description Enter the license in	formation description.
		Confirm	Cancel

Click **Confirm** to save the authorization policy.

Click Finish. In the dialog box that is displayed, click Confirm.

Tip	\otimes
The SSL VPN virtual gateway a policy sslvpn_c2s_example to VPN tu	permit traffic from the SSL
Confirm	Cancel

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**.

Ruijie sslvpn		-	-	×
	Welcome to Ruijie SSLVPN			
	https://172.17.123.12:8443			
	user1			
	Save Password Remember Me			
	Login			
	About			

b After login succeeds, the client obtains the assigned virtual address.

Ruijie SSLVPN		-	×
\mathbf{O}	Service Address 172.17.123.12:8443		
user1 State • Online	Current User user1		
Online time 00:00:12	State Online		
🗔 Resource	Virtual Address 172.17.153.2		
間 Connection	Sent 💕	Received 0 B	
国 About	2		
Setting	Sending rate	Receiving rate 0 B/S	
🗄 Logout	Loss(Up/Down) 🔊	Delayed 0 ms	

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

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.

D Rates A Other Catery Legin Time Legin Time Legin Time Virtual Address Oslino Duration Updies Traffic Describing Operation Operation example user1 127.75512 456cond 240.00p/rpts 240.00p/rpts Office Office	Online User Info Lock Use	Info Lock IP Info								
	C Refresh R Offine						G	example \sim 1	Enfor a usomamo.	
	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	Offine	

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

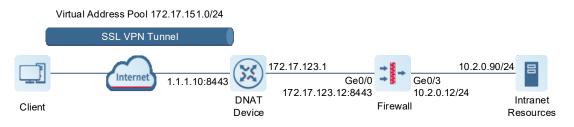
Table 8-22 Products and Versions

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	 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	 Interface: Ge0/0 (172.17.123.12), untrust Interface: Ge0/3 (10.2.0.12), trust 	
SSL VPN gateway configuration	 Manually configured address: 1.1.1.10:8443 Interface: Ge0/0 (172.17.123.12:8443) 	
Authentication mode	Local authentication	
SSL VPN user	 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.

K Back Edit Physical I	nterface	
Basic Info		
Interface Name	Ge0/0	
Description		
Connection Status	• Enable 💿 Disable	
Mode	Routing Mode	Off-Path Mode
* Zone	untrust \vee	O Add Security Zone
Interface Type	• WAN Interface 🛛 LAN Interface	, ,
Address		
ІР Туре	IPv4 IPv6	
Connection Type	• Static Address O DHCP O PPPoE	
* IP/Mask	172.17.123.12/24	
* Next-Hop Address	172.17.123.1	
Default Route		-
Line Bandwidth		
Uplink	Select v	
Downlink	Select V	
Access Management		
Permit	🖌 HTTPS 🕑 PING 🗹 SSH	
Advanced		
ISP Address Library	ISP Address Library V	
© MTU	1500	
MA		Restore Default MAC
Link Detection	Link Detection V	
		Save

- 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.

User Management		
Default Authentication Domain		
User Structure 🛛 🖻	User Group Members Add Image:	\otimes
 ✓ R All Groups R jmeter R group1 	Name Group User Group Name group1 Parent Group Enter or set Enter or set	slect a value.
	Sa	ve Cancel

c Click Save.

d Click Add and choose User.

User Management					
Default Authentication Domain	- ×				
User Structure	Ē	User Group Members			
 Create User Group 		Add 🗸 🔟 Delete	📀 Enable 🚫 Disable	C Refresh More 🗸	
		User I= me	Group		Account Expiry Date
& jmeter		Users			
& group1					

- 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	user1
Enabled State	• Enable 🔿 Disable
Displayed Username	Enter the displayed username.
* Parent Group	/default/group1 V
Description	Enter user description.
Password	
* ① Password	
* Confirm Password	
I 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 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 			O Log	gin Control	
Network Config					
* Gateway Name	example				
① Gateway Type	• Exclusive 🔾 Shared				
* Gateway Address	Ge0/0(Off 172.17.123.12/26 >	172.17.123.12	① Port Number	8443	
	Manually Configure IP	1.1.1.10	① Port Number	8443	1 Delete
	· Create				
Domain Name	Enter a domain name.				
Intranet DNS	Enter an intranet DNS server addres	SS.			
⊕ (Create				
Preferred DNS	 Intranet DNS Customer I 	DNS			
≣t Advanced					
Protocol					
* Protocol Version	Z TLS1.2 🗌 TLS1.1 🗌 TLS	51.0			
* Algorithm Suite	✓ TLS-ECDHE-RSA-WITH-AES128-	-CBC-SHA256 🗹 TLS-ECDHE	-RSA-WITH-AES256	-CBC-SHA384	✓ TLS-RSA-WITH-AES256-CBC-SHA
Gateway Certificate	default	~			
Concurrency Control					
* 🕕 Max. Concurrent Users	20				

Click Next.

b Perform Authentication Configuration

The default authentication domain is used. Therefore, use the default configuration for parameters on this page.

K Back Add SSL VPN Gateway	
⊘ Basic Config	O Login Control
Authentication	
* 🕖 User Authentication Domain	default ⓒ Create User Authentication Domain
Prevent Brute-Force Attack	
User Lockout	
* 🕐 Max. User Attempts	5 Time * O Lockout Period 300 Second
Single IP Lockout	
* () Max. Single IP Attempts	5 Time * () Lockout Period 300 Second
Login Verification	
① Graphic Verification	
* () Enable upon	0 Consecutive Input Errors
① Hardware Signature Verification	
* ① Maximum Signatures Bound to Each	3
User	
Auto Hardware signature Approva O Auto User Unbinding	
Auto Approval of Trusted Public Terminals	
Idle Timeout	
* ① 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

Add SSL VPN Gateway		
🚫 Basic Config	Add Tunnel Resource Group	
Basic Confie	* Tunnel Resource resource_grp_1 Group Name	8
Tunnel Mode O Full Tunnel Split Tunnel	Description Enter the tunnel re group description. Name	
* () Tunnel Access Keep-Alive Interval 30 5 * () Max. Disconnection Time 160 5	* Resource Config List Resource Type IP Subnet Domain Name	
Enable SSL VPN Private Line	Create Delete Protocol any	
Tunnel Resource List	Resource Name Resource Name Confirm Cancel	
Create Delete Resource Group Name Resource	No Data	
	Total: 0	
	Confirm Cancel	
Total: 0		

Click **Confirm** to create the resource. Then click **Confirm** to create the resource group, as shown in the following figure.

⊘ Basic Co	onfig		⊘ Login Control
	Basic Config		
* 🕕 Avail	lable IP Ranges	172.17.151.0/255.255.255.0	
Q) Tunnel Mode	🔿 Full Tunnel 🛛 o Split Tu	nnel
* () Tunnel Access Kee	p-Alive Interval	30	Second
* 🕕 Max. Disco	onnection Time	180	Second
Enable SSL V	PN Private Line	Note: When this function	is enabled, a private line where only the SSL VPN can be accessed will be set up after you log in to the SSL VPN.
Tunne	Resource List		
€	Create 🔟 De	elete	
	Resource Gro	oup Name Reso	purce
	resource_grp	_1 resources	urce_1
Tot	al: 1		

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

⊘ Basic Config	💭 Login Control	
Create	Add License	⊗
Policy Name User/User Group	* Authorization Policy Name	policy_1
default /default	* User/User Group	group1 ©
	IP Tunnel Resource	resource_grp_1 ®
Total: 1	Description	Enter the license information description.
		Confirm

Click Confirm to save the authorization policy.

Click Finish. In the dialog box that is displayed, click Confirm.

Тір	\otimes
The SSL VPN virtual gateway a policy sslvpn_c2s_example to VPN tur	permit traffic from the SSL
Confirm	Cancel

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**.

Ruijie Isslvpn		-	×
	Welcome to Ruijie SSLVPN		
	https://1.1.1.10:8443		
	user1		
	Save Password Remember Me		
	Login		
	About		

b After login succeeds, the client obtains the assigned virtual address.

RUIJIe SSLVPN		- ×	(
Ω	Service Address 1.1.1.10:8443		
user1 State • Online	Current User user1		
Online time 00:00:46	State Online		
📑 Resource	Virtual Address 172.17.153.2		
関 Connection	Sent 💕	Received 1 KB	
国 About			
Setting	Sending rate	Receiving rate 0 B/S	
🖃 Logout	Loss(Up/Down)	Delayed 1 ms	

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

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.

C Rutess R Ottos Data database Description Descriprescription <thdescription< th=""></thdescription<>	Online User Info Lock Us	er Info Lock IP Info								
	C Refresh & Offline						Ga	teway example ~	Enfor a usomamo.	
example user1 172:17:151.2 435econd 240.00bytes 240.00bytes Office	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	Offine	

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)

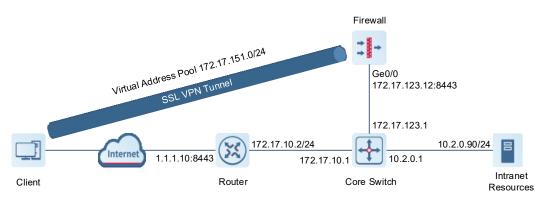
1. Applicable Products and Versions

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)	 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	 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	 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	 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.

Basic Info	
Interface Name Ge0/0	
Description	
Connection Status 🧿 Enable 💿 Disable	
Mode 💿 Routing Mode 💿 Transparent Mode 💿 Off-Path Mode	
* Zone trust \checkmark () Add Security Zone	
Interface Type 🔘 WAN Interface 🔹 LAN Interface	
Address	
IP Type IPv4 IPv6	
Connection Type 💿 Static Address 🔷 DHCP 🔷 PPPoE	
* IP/Mask 172.17.123.12/24	
Line Bandwidth	
Uplink Select V	
Downlink Select V	
Access Management	
Permit 🗹 HTTPS 🗹 PING 🗹 SSH	
Advanced	
① MTU 1500	
MAC 50:00:00:12:00:00 Restore Default 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.

Back Create Static R	outing
ІР Туре	IPv4
* Dest. IP Range/Mask	0.0.0/0
Next-Hop Address	172.17.123.1
Interface	Ge0/0 V
* ① Priority	5
Link Detection	Link Detection \lor
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	Ξ	User Group Members	🛛 Enable 🚫 Disable 😋	Refresh	Create User Gro	pup	\otimes
 옷 All Groups 옷 jmeter 옷 group1 		Name	Group		* User Group Name Parent Group	group1 Enter or select a value.	
						Save	

- c Click Save.
- d Click Add and choose User.

User Management

Default Authentication Domain	~				
User Structure	Ξ	User Group Membe	ers		
		Add 🗸 🔟 Delete	e 🔗 Enable 🚫 Disable 😋	Refresh More 🗸	
All Groups		User Jame	Group		Account Expiry Date
& jmeter		Users	•		
& group1					

- 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	user1	
Enabled State	• Enable 🔿 Disable	
Displayed Username	Enter the displayed username.	
* Parent Group	/default/group1 ~	
Description	Enter user description.	
Password		
* ① Password	•••••	
* Confirm Password	•••••	
Advanced Settings		

- 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.
- 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			O Log	in Control	
Network Config					
* Gateway Name	example				
① Gateway Type	• Exclusive 🔾 Shared				
* Gateway Address	Ge0/0(Off 172.17.123.12/26 >	172.17.123.12	① Port Number	8443	
	Manually Configure IP V	1.1.1.10	① Port Number	8443	Delete
	③ Create				
Domain Name	Enter a domain name.				
Intranet DNS	Enter an intranet DNS server addres	SS.			
⊕ (Create				
Preferred DNS	 Intranet DNS Customer I 	DNS			
≣t Advanced					
Protocol					
* Protocol Version	Z TLS1.2 🗌 TLS1.1 🗌 TLS	51.0			
* Algorithm Suite	TLS-ECDHE-RSA-WITH-AES128-	CBC-SHA256 🗹 TLS-EC	DHE-RSA-WITH-AES256	-CBC-SHA384	✓ TLS-RSA-WITH-AES256-CBC-SHA
Gateway Certificate	default	~			
Concurrency Control					
* () Max. Concurrent Users	20				

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	
* ① User Authentication Domain default	Create User Authentication Domain
Prevent Brute-Force Attack	
User Lockout	
* ① Max. User Attempts 5	Time * ① Lockout Period 300 Second
Single IP Lockout 🗾	
* () Max. Single IP Attempts 5	Time * ① Lockout Period 300 Second
Login Verification	
() Graphic Verification	
* ① Enable upon 0	Consecutive Input Errors
① Hardware Signature Verification	
* ① Maximum Signatures Bound to Each 3	
User	
Auto Hardware Signature Approval	
① Auto User Unbinding	
Auto Approval of Trusted Public Terminals	
Idle Timeout	
* ① The idle status will time out after 30	minutes.
Client Version Control	
Available Client Versions 🧕 Any '	/ersion 📀 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

< Back Add SSL VPN Gateway		
⊘ Basic Config	Add Tunnel Resource Group	
Basic Config	* Tunnel Resource resource_grp_1)
* ① Available IP Ranges 172.17.151.0/255.255.255.0	Group Name * Resource resource 1	
Tunnel Mode O Full Tunnel Split Tunnel O Tunnel Access Keep-Alive Interval 30 S	el Description Enter the tunnel re- group description Name	
* Max. Disconnection Time 180 S	* Resource Config List Resource Type Subnet Domain Name	
Enable SSL VPN Private Line	er Create Delete Protocol any ~	
Tunnel Resource List	Resource Name Ri	
Create	Confirm Cancel	
Resource Group Name Resource	ee No Data	
	Total: 0	
Total: 0	Confirm Cancel	

Click **Confirm** to create the resource. Then click **Confirm** to create the resource group, as shown in the following figure.

Sasic Config	🖉 Login Control
Basic Co	nfig
* 🕕 Available IP Ra	nges 172.17.151.0/255.255.25.0
() Tunnel N	Node 🔿 Full Tunnel 💿 Split Tunnel
* ① Tunnel Access Keep-Alive Int	erval 30 Second
* 🕕 Max. Disconnection	Time 180 Second
Enable SSL VPN Private	Line Note: When this function is enabled, a private line where only the SSL VPN can be accessed will be set up after you log in to the SSL VPN.
Tunnel Resource	List
⊕ Create	Delete
Resour	rce Group Name Resource
resour	ce_grp_1 resource_1
Total: 1	

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.

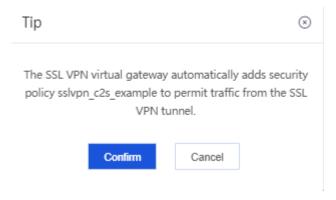
Click Create and create an authorization policy as follows:

- o Authorization Policy Name: policy_1
- o User/User Group: group1
- o IP Tunnel Resource: resource_grp_1

Create Delete Policy Name User/User Group * Authorization Policy Name * Objecy Name	ense List	Add License	C
" User/User groupt groupt v Group IP Tunnel resource_grp_1 v Resource Description Enter the license information description.	Policy Name	h7_1	
Description Enter the license information description.		Group IP Tunnel resource.grp.	
	tal: 1		ense information description.

Click Confirm to save the authorization policy.

Click Finish. In the dialog box that is displayed, click Confirm.



(5) Configuring an SNAT Policy



- 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:

1 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 O DNAT O Twice Nat
Basic Info	
* Name	sslvpn_resource_nat
Enabled State	Senable ○ Disable
Description	Enter the description.
Time Range	any \lor \odot Add One-Off Time Plan \odot Add Cyclic Time Plan
Packet Before NAT	
* Src. Security Zone	untrust ~
* Src. Address	ippool_example ~
* Dest. Security Zone	trust ~
* Dest. Address	res_example ~
* Service	any 🗸
Packet After NAT	
Src. Address Translated	Address Pool Oesignated IP Outbound Interface Address

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**.

Ruijie Isslvpn		_	×
	Welcome to Ruijie SSLVPN		
	https://1.1.1.10:8443		
	user1		
	•••••		
	Save Password Remember Me		
	Login		
	About		

b After login succeeds, the client obtains the assigned virtual address.

Ruijie SSLVPN		- ×
Ω	Service Address 1.1.1.10:8443	
user1 State • Online	Current User user1	
Online time 00:00:46	State Online	
📑 Resource	Virtual Address 172.17.153.2	
関 Connection	Sent 💕	Received 1 KB
国 About		
O Setting	Sending rate 💕	Receiving rate O B/S
🖃 Logout	Loss(Up/Down)	Delayed 1 ms

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

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.

C Retent R Ottos Catheory Records C Editor a comptile C Editor a comptile	Online User Info	Lock User Info Lock IP Info							
	C Refresh 🖁 Offine						G	iateway example ~	Enter a username.
	Gateway Name	Username	Login Time	Login IP	Virtual Address	Online Duration	Uplink Traffic	Downlink Traffic	Operation
example user1 172.17.151.2 435econd 240.00bytes 240.00bytes 000		user1			172.17.151.2	43Second	240.00bytes	240.00bytes	Offine

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

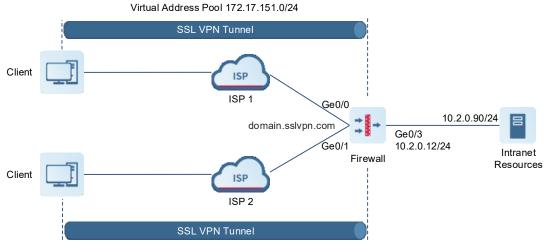
Table 8-24 Products and Versions

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.



Virtual Address Pool 172.17.151.0/24

Item	Description	Remarks
Network interface	 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	 Interface 1: Ge0/0:8443 Interface 2: Ge0/1:8443 Domain name: domain.sslvpn.com 	

Authentication mode	Local authentication	
SSL VPN user	 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	e Ge0/0	
Description	n	
Connection Status	s 💿 Enable 💿 Disable	
Mode	e 💽 Routing Mode 🛛 Transparent Mode 🔵 O	/ff-Path Mode
* Zone	e untrust 🗸 🖉 Ad	d Security Zone
Interface Type	e 💿 WAN Interface i LAN Interface	
Address	5	
ІР Туре	e IPv4 IPv6	
Connection Type	e 💽 Static Address 🔿 DHCP 🔿 PPPoE	
* IP/Mask	k 172.17.123.12/24	
* Next-Hop Address	s 172.17.123.1	
Default Route	•	
Line Bandwidth	1	
Uplink	k Select ~	
Downlink	k Select ~	
Access Management	t	
	t 🔽 HTTPS 🔽 PING 🔽 SSH	
Advanced		
ISP Address Library	y ISP Address Library ~	
0 MTU	J 1500	
MA	Rest	ore Default MAC
Link Detection	Link Detection	
		Save

- 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.

User Management			
Default Authentication Domain			
User Structure 📮	User Group Members	Create User Group	\otimes
 冬 All Groups 冬 jmeter ※ group1 	Name Group	* User Group Name group1	
		Parent Group Enter or select a value.	
	and the second s	Permanent	

- c Click Save.
- d Click Add and choose User.

User Management			
Default Authentication Domain	\sim		
User Structure	Ξ	User Group Members	
Create User Group		Add 🗸 🛅 Delete 🥝 Enable 🛇 Disable 🖏 Refresh More 🗸	
		User I me Group	Account Expiry Date
% jmeter		Users	
& group1			
ペ All Groups 発 jmeter		Userme Group	Account Expiry Date

- 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	user1	
Enabled State	• Enable 🔿 Disable	
Displayed Username	Enter the displayed username.	
* Parent Group	/default/group1 \sim	
Description	Enter user description.	
Password		
* ① Password	•••••	
* Confirm Password	•••••	
I Advanced Settings		

- f Click Save.
- (3) Configuring a Gateway
 - a Perform Basic Configuration

Choose Network > SSL VPN > SSL VPN Gateway.

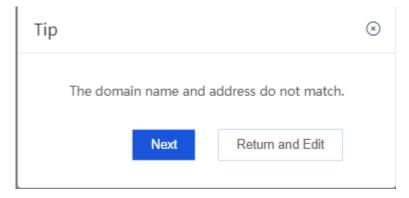
Click Create and create an SSL VPN gateway as follows:

- 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.

Basic Config			O Log	gin Control	
Network Config					
* Gateway Name	example				
🕕 Gateway Type	Exclusive				
* Gateway Address	Ge0/0(On 172.17.123.12/24 >	172.17.123.12	① Port Number	8443	
	Ge0/1(On 172.17.124.12/24 >	172.17.124.12	① Port Number	8443	i Delete
	Create				
Domain Name	Enter a domain name.				
Intranet DNS	Enter an intranet DNS server addre	SS.			
•	Create				
Preferred DNS	Intranet DNS OCustomer I	ONS			
≣t Advanced					
Protocol					
* Protocol Version	✓ TLS1.2 □ TLS1.1 □ TLS	51.0			
* Algorithm Suite	TLS-ECDHE-RSA-WITH-AES128-	CBC-SHA256 🗹 TI	S-ECDHE-RSA-WITH-AES256	-CBC-SHA384	✓ TLS-RSA-WITH-AES256-CBC-SHA
Gateway Certificate	default	~			
Concurrency Control					
* ① Max. Concurrent Users	20				

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				
* ① User Authentication Domain	default	Create User Authentication Doma	ain	
Prevent Brute-Force Attack				
User Lockout				
* ① Max. User Attempts	5	Time * ① Lockout Period	300	Second
Single IP Lockout				
* () Max. Single IP Attempts	5	Time * () Lockout Period	300	Second
Login Verification				
O Graphic Verification (
* () Enable upon	0	Consecutive Input Errors		
① Hardware Signature Verification (
* ① Maximum Signatures Bound to Each	3			
User				
 Auto Hardware Signature Approval (
O Auto User Unbinding (
① Auto Approval of Trusted Public Terminals (
Idle Timeout				
\bullet (1) The idle status will time out after	30	minutes.		
Client Version Control				
Available Client Versions	 Any Version 	 Latest Version on Secure Clou 	id 🔾 Custor	n 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

< Back Add SSL VPN Gateway					
Sasic Config	Add Tunnel Res	ource Group			
Basic Config	* Tunnel Resource	resource_grp_1	Add Resource		\otimes
* ① Available IP Ranges 172.17.151.0/255.255.255.0	Group Name		* Resource	resource_1	
O Tunnel Mode O Full Tunnel Split Tunnel Solit Tunnel Solit Tunnel	Description	Enter the tunnel re group description.	Name		
* Max. Disconnection Time 180 S	* Reso	urce Config List		OIP OSubnet ODomain Name URI	
Enable SSL VPN Private Line O Note: When this function is er	• Create	Delete	* () Resource Protocol	10.2.0.0/24	
Tunnel Resource List	Res	source Name R	Trotocor	any	
🕙 Create 📓 Delete				Confirm	
Resource Group Name Resource				No Data	
	Total: 0				
				Confirm Cancel	
Total: 0					

Click **Confirm** to create the resource. Then click **Confirm** to create the resource group, as shown in the following figure.

⊘ Basi	ic Config		⊘ Login Control
	Basic Config		
*①/	Available IP Ranges	172.17.151.0/255.255	5.255.0
	① Tunnel Mode	O Full Tunnel O	Split Tunnel
1 Tunnel Access	Keep-Alive Interval	30	Second
* 🕕 Max. E	Disconnection Time	180	Second
Enable SS	SL VPN Private Line	Note: When this for the second secon	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
Ти	nnel Resource List		
	🕒 Create 📋 D	elete	
	Resource Gr	oup Name	Resource
	resource_grp	o_1	resource_1
	Total: 1		
	rotal. T		

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

) Create	Add License	
Policy Name User/User Group	* Authorization policy_1 Policy Name	
] default /default	* User/User group1 © Group	~
	IP Tunnel resource_grp_1 ®	~
tal: 1	Description Enter the license information description.	

Click Confirm to save the authorization policy.

Click Finish	. In the dialog	box that is	displayed,	click Confirm
--------------	-----------------	-------------	------------	---------------

Tip	\otimes
The SSL VPN virtual gateway a policy sslvpn_c2s_example to VPN tu	permit traffic from the SSL
Confirm	Cancel

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**.

Ruijie SSLVPN		_	×
	Welcome to Ruijie SSLVPN		
	https://domain.sslvpn.com:8443		
	user1		
	Save Password 🗌 Remember Me		
	Login		
	About		

b After login succeeds, the client obtains the assigned virtual address.

Ruijie SSLVPN	- ×
Ω	Service Address domain.sslvpn.com:8443
user1 State • Online	Current User user1
Online time 00:01:23	State Online
📑 Resource	Virtual Address 172.17.153.2
🔋 Connection	Sent 🚱 Received 0 B 0 B
国 About	-
Setting	Sending rate Receiving rate 0 B/S 0 B/S
∃ Logout	Loss(Up/Down) Delayed 1 ms

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
 - 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.

Online User Info Lock U	ser Info Lock IP Info							
C Refresh & Offine						G	ateway example ~	Enfor a usorname.
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	Offine

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

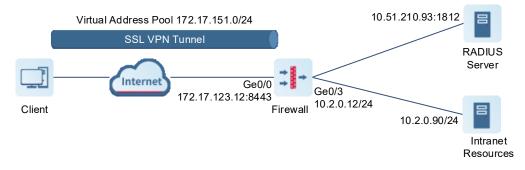
1. Applicable Products and Versions

 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	 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	 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	 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.

< Bac	ck Edit Physical I	nterface
	Basic Info	
	Interface Name	Ge0/0
	Description	
	Connection Status	Enable Disable
	Mode	Routing Mode
	* Zone	untrust V Add Security Zone
	Interface Type	WAN Interface LAN Interface
	Address	
	IP Туре	IPv4 IPv6
		• Static Address ODHCP OPPoE
	* IP/Mask	172.17.123.12/24
	* Next-Hop Address	172.17.123.1
	Default Route	
	Line Bandwidth	
	Uplink	Select v
	Downlink	Select V
		Joidy v
	Access Management	
	Permit	HTTPS PING SSH
	Advanced	
	ISP Address Library	ISP Address Library V
	0 MTU	1500
	MA	Restore Default MAC
	Link Detection	Link Detection V
		Save

- 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	smp					
* Shared Password						
* Active Authentication Server IP	10.51.210.93	 Authentication Port 	1812	 Accounting Port 	1813	Tx Interface S
Standby Authentication Server IP	Enter an IP address.	① Authentication Port	Enter the port number.	① Accounting Port	Enter the port number.	Tx Interface S
Et Advanced Settings						
Retransmission Times	3					
Unit	Byte					
Response Timeout	5					
① Enable Active Detection						
			Save			

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.
- 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	smp
Enabled State	Enable Disable
Description	Enter authentication domain description.
* Scenario	
SSL VPN Access	0 User Location Only Info on Server V Authentication Server smp V
WEBAUTH	0
Et Advanced Settings	
() Domain Name Removal	
 Default Online User 	/smp v
Group	
	Save

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	O Login Control
Network Config	
* Gateway Name	example
Gateway Type	Exclusive Shared
* Gateway Address	Ge0/0(Off 172.17.123.12/26 > 172.17.123.12 O Port Number 8443
	· Create
Domain Name	Enter a domain name.
Intranet DNS	Enter an intranet DNS server address.
•	Create
Preferred DNS	Intranet DNS Customer DNS
≣t Advanced	
Protocol	
* Protocol Version	Z TL51.2 🗌 TL51.1 🔲 TL51.0
* Algorithm Suite	Z TLS-ECDHE-RSA-WITH-AES128-CBC-SHA256 Z TLS-ECDHE-RSA-WITH-AES256-CBC-SHA384 Z TLS-RSA-WITH-AES256-CBC-SHA
Gateway Certificate	default ~
Concurrency Control	
* ① Max. Concurrent Users	20

Click Next.

b Perform Authentication Configuration

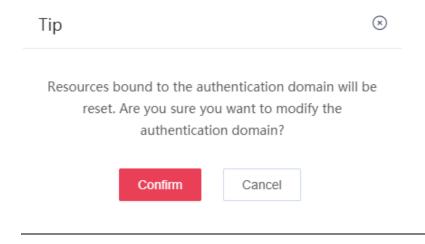
Set **User Authentication Domain** to the authentication domain **smp** configured in the previous step, and use the default configuration for the other parameters.

Sasic Config			• Login Control		
Authentication					
* () User Authentication Domain	smp	⊕ Create	User Authentication Do	main	
Prevent Brute-Force Attack					
User Lockout					
* ① Max. User Attempts	5	Time	* () Lockout Period	30	Second
Single IP Lockout					
* ① Max. Single IP Attempts	5	Time	* ① Lockout Period	300	Second
Login Verification					
① Graphic Verification					
* 🕕 Enable upon	0	Consecut	ive Input Errors		
① Hardware Signature Verification					
* () Maximum Signatures Bound to Each	3				
User					
① Auto Hardware Signature Approval					
① Auto User Unbinding					
① Auto Approval of Trusted Public Terminals					
Idle Timeout					
* () The idle status will time out after	30	minutes.			

Click Next.

1 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.



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

< Back Add	d SSL VPN Gateway			
\odot) Basic Config	Add Tunnel Resource Grou	qt	
	Basic Config O Available IP Ranges 172.17.151.0/255.255.255.0	* Tunnel Resource resource_gr	Add Resource	\otimes
	Tunnel Mode Full Tunnel Split Tunnel	Group Name Description Enter the tu group descr		
	ccess Keep-Alive Interval 30 Aax. Disconnection Time 180	* Resource Config L	ist Resource Type O IP O Subnet O Domain Name	
Enab	ble SSL VPN Private Line	• Create	* () Resource 10.2.0.024 Protocol any	
	Tunnel Resource List	Resource Name	R. Confirm Cancel	
	Resource Group Name Resource	e	No Data	
		Total: 0		
			Confirm Cancel	
	Total: 0			

Click **Confirm** to create the resource. Then click **Confirm** to create the resource group, as shown in the following figure.

⊘ Ba	sic Config		⊘ Login Control
	Basic Config		
* 🕕	Available IP Ranges	172.17.151.0/255.255.255.0	
	① Tunnel Mode	 Full Tunnel Split Tunnel 	unnel
1 Tunnel Access	s Keep-Alive Interval	30	Second
* 🕕 Max.	Disconnection Time	180	Second
Enable	SSL VPN Private Line	Note: When this function	n 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
т	unnel Resource List		
	Ocreate	elete	
	Resource Gr	oup Name Res	ource
	resource_grp	o_1 reso	purce_1
	Total: 1		
	Total. 1		

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

⊘ Basic Config		⊘ Login Control	
Create		Add License	\otimes
Policy Name	User/User Group	* Authorization policy_1 Policy Name	
🗆 default	/default	• User/User group1 @ Group	~
		IP Tunnel resource_grp_1 ® Resource	~
Total: 1		Description Enter the license information description.	
		Confirm Cancel	

Click **Confirm** to save the authorization policy.

Click Finish. In the dialog box that is displayed, click Confirm.

Tip	\otimes
The SSL VPN virtual gateway policy sslvpn_c2s_example to VPN tu	permit traffic from the SSL
Confirm	Cancel

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.

Rujje SSLVPN		_	\times	
	Welcome to Ruijie SSLVPN			
	https://172.17.123.12:8443			
	user1			
	•••••			
	Save Password Remember Me			
	Login			
	About			

b After login succeeds, the client obtains the assigned virtual address.

Ruijie SSLVPN		-	×
\mathbf{O}	Service Address 172.17.123.12:8443		
user1 State • Online	Current User user1		
Online time 00:00:12	State Online		
🛱 Resource	Virtual Address 172.17.153.2		
間 Connection	Sent 💕	Received 0 B	
国 About	Sending rate	Receiving rate	
Setting	Sending rate	0 B/S	
🖪 Logout	Loss(Up/Down) 🔊	Delayed 0 ms	

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
 - 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.

monnat	ION.							
Online User Info Lock Us	er Info Lock IP Info							
C Refresh R Offline						Gi	steway example ~	Enter a username. Q
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	Offline

- 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)

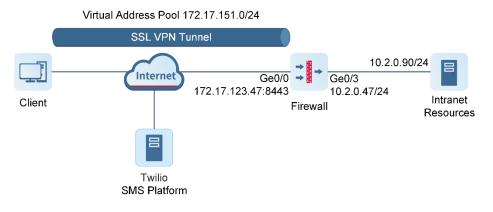
1. Applicable Products and Version

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	 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	 User group: group1 Username: user1 Password: test@123 Mobile number: 187xxxx9590 	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 Ge0/0	
Description	
Connection Status 🧿 Enable 🛛 🔵 Disab	le
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 O PPPoE
* IP/Mask 172.17.123.47/26	
* Next-Hop Address 172.17.123.1	
Default Route 🔵	
Line Bandwidth	
Uplink	Select V
Downlink	Select V
Line Bandwidth	
Uplink	Select V
Downlink	Select ~
Access Management	
Permit 🗹 HTTPS 🗌 PING	SSH
Advanced	
ISP Address Library ISP Address Library	~
① MTU 1500	
MAC	Restore Default 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.

Default Authentication Domain			
User Structure =	User Group Me	Create User Group	\otimes
Create User Group	Add 🗸 🛅 t	* User Group Name group1	
All Groups	Name	Parent Group /default v	
		Save Cancel	

- c Click Save.
- d Configure user information as follows:

Login Username: user1

Parent Group: /default/group1

Password: test@123

Mobile Number: 187xxxx9590. Enter a valid mobile number for receiving an SMS verification code.

< Back Add User		
Basic Info		
* Login Username	user1	
Enabled State	• Enable 🔿 Disable	
Displayed Username	Enter the displayed username.	
* Parent Group	/default/group1 V	
Description	Enter user description.	
Mobile Number		
Mobile Number	+86 ~ 187	
Password		
* ① Password	•••••	
* Confirm Password	•••••	

- 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 Au	thentication Server	
SMS Provider	🔿 Alibaba Cloud 🕕 🔹 Twilio 🕕	
* Server Name	Twilio	
* Account SID		
* Authentication Token	••••••	
* ① Sender Mobile Number		
* 🕕 SMS Template		
 Test Mobile Number 	Enter a test mobile number.	Send Test Message

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
• Basic Config	O Login Control O Add Resource
Network Config	
* Gateway Name	sslvpn
 Gateway Type 	Exclusive Shared
* Gateway Address	Ge0/0(Off 172.17.123.47/2€ > 172.17.123.47 ① Port Number 8443
	⊙ Create
Domain Name	Enter a domain name.
Intranet DNS	Enter an intranet DNS server address.
\odot	Create
Preferred DNS	Intranet DNS O Customer DNS
≣ ↑ Advanced	
Protocol	
* Protocol Version	▼ TLS1.2 □ TLS1.1 □ TLS1.0
* Algorithm Suite	☑ TLS-ECDHE-RSA-WITH-AES128-CBC-SHA256
Gateway Certificate	default \sim
Concurrency Control	
* () Max. Concurrent Users	10

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.

Basic Config	O Login Co	ontrol	Add Resource
Authentication			
* () User Authentication Domain	default	ation Domain	
SMS Two-Factor Authentication			
* SMS Authentication Server	Twilio	on Server	
SMS-based Manual Binding			
SMS-based Manual Unbinding			
Manual Mobile Number Submission			
① SMS Sending Limit	0		
Prevent Brute-Force Attack			
User Lockout			
* ① Max. User Attempts	5 Time * ① Lockout	Period 300	Second
Single IP Lockout			
* ① Max. Single IP Attempts	5 Time * ① Lockout	Period 300	Second
Login Verification			
① Graphic Verification			
* ① Enable upon	0 Consecutive Input Errors		
Hardware Signature Verification			
* ① Maximum Signatures Bound to Each	3		
User			
① Auto Hardware Signature Approval			
① Auto User Unbinding			
) Auto Approval of Trusted Public Terminals			
Idle Timeout			
* ()) The idle status will time out after	30 minutes.		

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

Add SSL VPN Gateway			
Sasic Config	Add Tunnel Resource Group		
Basic Config	* Tunnel Resource resource_grp_1	Add Resource	\otimes
* ① Available IP Ranges 172.17.151.0/255.255.255.0	Group Name	* Resource resource 1	
① Tunnel Mode 🔿 Full Tunnel 💿 Split Tunnel	Description Enter the tunnel re group description.	* Resource_1 Name	
* ① Tunnel Access Keep-Alive Interval 30 S * ② Max. Disconnection Time 180 S	* Resource Config List	Resource Type O IP Subnet O Domain Name	
Enable SSL VPN Private Line	• Create	* () Resource 10.2.0.0/24	
Note: When this function is er Tunnel Resource List	Resource Name R	Protocol any	~
© Create		Confirm	
Resource Group Name Resource		No Data	
	Total: 0		
Total: 0		Confirm Cancel	

Click **Confirm** to create the resource. Then click **Confirm** to create the resource group, as shown in the following figure.

Basic Config		O Login Control	Add Resource
Basic Config			
* ① Available IP Ranges	172.17.151.0/255.255.255.0		
① Tunnel Mode	 Full Tunnel Split Tunn 	nel	
* ① Tunnel Access Keep-Alive Interval	30	Second	
* () Max. Disconnection Time	180	Second	
Enable SSL VPN Private Line			
	• Note: When this function is	enabled, a private line where only the SSL VPN ca	an be accessed will be set up after you log in to the SSL VPN.
Tunnel Resource List			
↔ Create	elete		
Resource Gr	oup Name Resou	rce	Description
resource_grp	_1 resour	ce_1	

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

Basic Config		Add License		\otimes
ense List				
		* Authorization	policy_1	
Create Delete		Policy Name		
Policy Name	User/User Group	* User/User Gro	group1 3	\sim
default	/default	up		
		IP Tunnel Resou	resource_grp_1 ®	~
		rce		
		Description	Enter the license information description.	

Click **Confirm** to save the authorization policy.

Click Finish. In the dialog box that is displayed, click Confirm.

Tip	\otimes
policy sslvpn_c2s_sslvpn to	y automatically adds security permit traffic from the SSL tunnel.
Confirm	Cancel

6. Verification

- Verifying Client Login Authentication
- (1) Open the SSL VPN client and enter the gateway access information as follows:
 - o Server Address: https://172.17.123.47:8443
 - o Username: user1
 - o Password: test@123

 \times

Ruijie SSLVPN

Welcome to Ruijie SSLVPN

https://172.	.17.123.47:8443	
user1		
••••••		
🖌 Save Passw	vord Remember Me	
	Log In	
	About	

(2) Click **Log In**. The system displays a message indicating that the verification code for SMS two-factor authentication has been sent.

Ruffie SSLVPN		—	×				
Verifying login information							
Welcome to Ruijie SSLVPN							
Two-Factor Authentication	\otimes						
The dynamic verification code for two-factor authentication has been sent to your mobile phone ending in 9590,Please check your phone. The dynamic verification code is valid for 5 minutes.							
Verification Code 24S							
Cancel							
Log In							
About							

- (3) Enter the received SMS verification code and click Commit.
- (4) After login, choose **Connection** and check whether the client obtains a virtual address.

RUJIE	-	×
\bigcirc	Server Address 172.17.123.47:8443	
user1 State • Online	Current User user1	
Online Time 00:00:08	State Online	
🛱 Resources	Virtual Address 172.17.151.2	
間 Connection	Sent Received 0 B 0 B	
国 About		
Settings	Sending rate Receiving rate 0 B/S 0 B/S	
∃ Logout	Dropped (uplink/downlink)	

(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.

Online User Info	Lock User Info	Lock IP Info						
C Refresh A Offline					Gatew	ay sslvpn	✓ Enter a username.	
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.

SSL VPN Log								
🖸 Export 😋 Refr	esh				iQ Set	earch Criteria	Enter the keyword.	
Time 🗘	Severity	Username ≑	Gateway ¢	IP	Details			
	• Tip	user1	sslvpn		User [user1] enables the tunnel access service (tunnel IP [172.1]	17.151.2]).		
1	• 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:

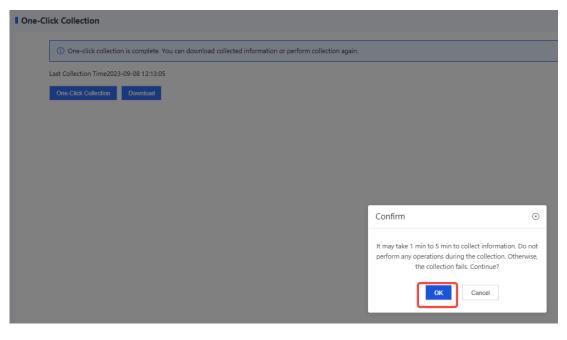
- a Collect client logs.
- b Log in to the client and obtain packets on the client.
- c Check the client environment.
- d Check whether resources are correctly configured.
- (2) Device Side

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.

One-Cl	Dne-Click Collection						
	① One-click collection is complete. You can download collected information or perform collection again.						
	Last Collection Time2023-09-08 12:13:05						
	One-Click Collection Download						

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*.

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.

Table 8-27 Description of SSL VPN Connection Failure Messages

Failed to parse the server address.	The input server address cannot be resolved to an IP address.	 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	DNAT configuration may be	Check whether networking
(networking fault).	incorrect.	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.

ło.	Time	Source	Destination	Protocol	Length Info
	16486 11:49:04.133165	172.17.96.130	172.17.123.12	DTLSv1.2	224 Client Hello
	16488 11:49:04.134204	172.17.123.12	172.17.96.130	DTLSv1.2	90 Hello Verify Request
	16489 11:49:04.134361	172.17.96.130	172.17.123.12	DTLSv1.2	244 Client Hello
	16490 11:49:04.135687	172.17.123.12	172.17.96.130	DTLSv1.2	90 Hello Verify Request
	16491 11:49:04.136135	172.17.123.12	172.17.96.130	DTLSv1.2	1223 Server Hello, Certificate, Server Hello Done
	16492 11:49:04.137270	172.17.96.130	172.17.123.12	DTLSv1.2	416 Client Key Exchange, Change Cipher Spec, Encrypted H
	16503 11:49:04.140679	172.17.123.12	172.17.96.130	DTLSv1.2	133 Change Cipher Spec, Encrypted Handshake Message
	16504 11:49:04.141114	172.17.96.130	172.17.123.12	DTLSv1.2	135 Application Data
	16505 11:49:04.142258	172.17.123.12	172.17.96.130	DTLSv1.2	103 Application Data
	16506 11:49:04.143130	172.17.96.130	172.17.123.12	DTLSv1.2	103 Application Data
	16507 11:49:04.144135	172.17.123.12	172.17.96.130	DTLSv1.2	103 Application Data
	16508 11:49:04.145876	172.17.123.12	172.17.96.130	DTLSv1.2	183 Application Data
-	16509 11:49:04.146428	172.17.96.130	172.17.123.12	DTLSv1.2	103 Application Data

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.

 Diagnostic Center

 Network Connectivity Diagnosis

 Image: Second Diagnosis Time: 2022-12-06 10:32:05

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								
	diagnostic parameters will be used th e: You are advised to minimize the rar							
* ① Src. Address	172.17.96.130	① Src. Port	Enter the Src. Port number.					
① Dest. Address	Enter the destination address.	① Dest. Port	Enter the Dest. Port number					
Inbound Interface	Select v	* Protocol	UDP ~]				
0 Src. MAC	Example: d8:9e:f3:3f:d5:64	🕕 Dest. MAC	Example: d8:9e:f3:3f:d5:64					
	Diagnose							
	Diagnose							

c Continuously ping intranet resources during the collection period.

Network Connectivity Diagnosis		Exit
Fault Diagnosis Trading Diagnostic Parameters: Src. Advers:172.17.96.130 Control of the Control of	Sex Partany Best Addressary Dest Partany Induced Hereforz ResolutIDP Sec. MAC. any Dest MAC. any Basic Config Detection Partany Partany	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<>>172.17.123.123.443	Packet 1 Product 12(17):81:10 Deck Address:12(17):81:10 Deck Address:12(17):121:12 Prostochulg: Sic. PortS&AB Deck FortB&AB Opprend: Read: - en el conded. Constituently Relig: Redet & Bicarded. Relig: weet text Constituently Relig: Redet & Bicarded. Relig: weet text Constituently Relig: Redet & Bicarded. Relig: weet text	Troubleshoot
Podet1 Podet2 Podet3 Podet4 Podet4 Podet7 Podet5 Podet5	Proce Prove P	
	Image: Second second Image: Second	Î

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			_															(3 Simulation Space
① Security Policy, Packet is discar	ded. Policy	name: test																
Policy Group		· Crea	ate 💼 De	iete 🕗 Enable	O Disal	ole 🖸 Refresh M	iore ~							Ту	pe All		Enter a keyword	
Add Policy Group			Priority	Name	Туре	Src. Security Zone	Src. Address	User/User Group	Dest. Security Zone	Dest. Address	Service	Арр	Time Range	Action	Content Security	Hit Count	Hit Session	Operation
Keyword All Groups	Q	~ Def	ault Policy G	iroup														
BE (4) Default			1	test		any	any	any	any	any	ping	any	any	Deny		12 Clear	View Details	C Edit Delete
a contract.			2	sslvpn_c2	IPv4	untrust	ippool_vgw	any	any	res_vgw	any	any	any	Permit		839 Clear	View Details	C Edit Delete
			3	s1		any	any	any	any	any	any	any	any	Permit)	43 Clear	View Details	C Edit Delete
			4	Default Po		any	any	any	any	any	any	any	any	Derry		0 Clear	View Details	Edit Delete

e Modify the matching rule of the corresponding security policy to permit the packets.

8.25 IPsec VPN

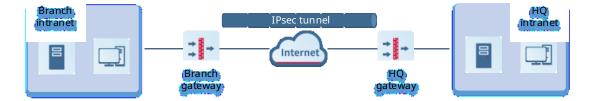
8.25.1 Overview

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.

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

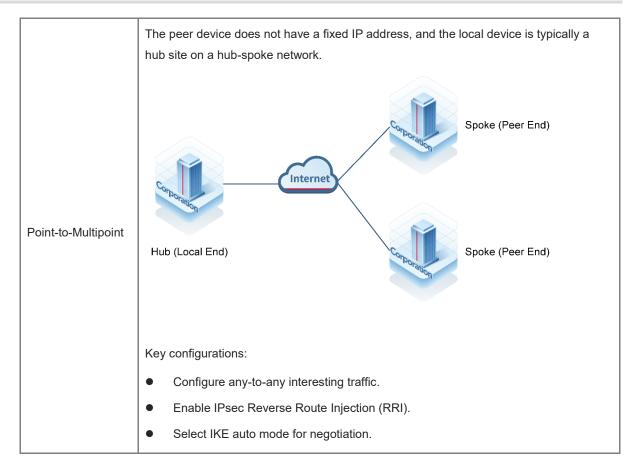
Internet Protocol Security (IPsec) is a protocol suite for establishing secure connections over public networks. The objective of IPsec is to provide security services for network layer traffic in IPv4 and IPv6 formats. Typically,

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	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.
	 Key configurations: 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.



8.25.4 Configuration Examples of Site-to-Site IPsec VPN

1. Applicable Products and Versions

Table 8-28 Products and Versions

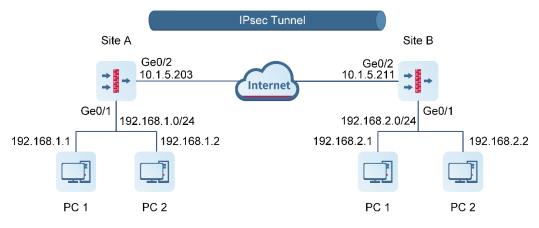
Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R6 or later

2. Service Demands

As shown in <u>Figure 8-20</u>, 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.
 - 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 Cor	fig Interesting Traffic Config	Config Verification
	* ① Tunnel Interface	ti 1	
	* Tunnel Name Si		
	* Scenario 💿	Point-to-Point 🔿 Point-to-Multip	oint
		Main Office Branch Office Branch Office	
	Cancel	xt	

- $\label{eq:constraint} c \quad \mbox{After completing the configuration, click } \textbf{Next}.$
- (2) Configure authentication.
 - a Configure parameters according to the following figure.

Ø	2		3	4)
Basic Config	Authentication	Config	Interesting Traffic Config	Config Ve	rification
	* Peer Address	10.1.5.2	211	Ping	
	* Outbound Interface	Ge0/2	~		
	* Authentication Mode	• Pre-sl	hared Key		
	* Key	•••••	00		
	* Confirm Key	•••••	••		

Previous	Cancel	Next

- b After completing the configuration, click **Next**.
- (3) Configure interesting traffic.
 - a Click Create. Configure parameters for interesting traffic according to the following figure.

O Basic Co	onfig	Auther	tication Config	Interesting	3 Traffic Config	Config Verification
	🕒 Crea	ate 🔟 Delete		Enter th	e keyword.	Q
		Proxy Mode	Local Network	Peer Network	Operation	
		Subnet-to-Sub	192.168.1.0/24	192.168.2.0/24	Edit Delete	
	10 ~	/ Page Total:1			Go to 1	1 >

Previous Cancel Next	
----------------------	--

- b After completing the configuration, click **Next**.
- (4) Verify configuration.
 - a After verifying the configuration, click **Finish**.

Ø Basic Config	Authentication	Config Interesting Traffic Co	
busic coning	Automication		
will be added to t	he custom tunnel list.		
	Basic Config	Edit	
	Tunnel Interface	vti1 ~	
	Tunnel Name	Site-to-Site	
	Scenario	Point-to-Point Point-to-Multip	oint 🕕
	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 Netw	ork
	192.168.1.0/24	192.168.2.0	/24
	Advanced Settings	Expand	
	Previous	Finish	

- Configuring Site B
- (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					(4)
Basic Config	Authentication (Config	Interest	ing Traffic	Config	Config Verification
	* (i) Tunnel Interface	vti	1			
	* Tunnel Name	Site-to	-Site		\otimes	
	* Scenario) Poin	t-to-Point	O Point	-to-Multipoi	nt
		Main	a Office	nternet	anch Office	
	Cancel	Next				

- c After completing the configuration, click **Next**.
- (2) Configure authentication.
 - a Configure parameters according to the following figure.

\bigcirc		2			3			4
Basic Co	onfig Au	thentication	Config	Interesti	ng Traffic Conf	ig	Config \	/erification
	*	Peer Address	10.1.5.2	.03			Ping]
	* Outbo	ound Interface	Ge0/2			\sim		
	* Authent	tication Mode	• Pre-sl	hared Key				
		* Key	•••••	••				
	:	* Confirm Key	•••••	••		(\times)		
			_					
	Previous	Cancel		Next				

- 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 Co	nfig	Auther	ntication Config	```````````````````````````````````````	3 Traffic Config	Config Verificatio
	🕀 Cre	eate 🔟 Delete		Enter th	e keyword.	Q
		Proxy Mode	Local Network	Peer Network	Operation	
		Subnet-to-Sub	192.168.2.0/24	192.168.1.0/24	Edit Delete	
	10 ~	/ Page Total:1			Go to 1	1 >

Previous	Cancel	Next	

- b After completing the configuration, click **Next**.
- (4) Verify configuration.
 - a After verifying the configuration, click **Finish**.

Ø)			4
Basic Config	Authenticati	on Config	Interesting Traf	fic Config	Config Verification
be added to the cu	stom tunnel list.				
	Basic Config	Edit			
	Tunnel Interface	vti1	~		
	Tunnel Name	Site-to-Site			
	Scenario	Point-to-Point ()	 Point-to-Multip 	point ()	
	Authentication Config	Edit			
	Peer Address	10.1.5.203			
	Outbound Interface	Ge0/2			
	Authentication Mode	 Pre-shared Key 			
	Кеу				
	Interesting Traffic Config	Edit			
	Local Network		Pee	r Network	
	192.168.2.0/24		192.	168.1.0/24	
	Advanced Settings	Expand			
	Previous	Cancel Finis	h		

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	vti1	
Security Zone	VPN-Zone v	⊕ Add Security Zone
* Tunnel Local Address	10.1.5.203	
Tunnel Remote Address	• IP 🔿 Dynamic	
	10.1.5.211	
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:

- 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.
- 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 Sec	curity Parameter Config
* Scenario	Point-to-Point Point-to-Multip	ooint 🕕
* Tunnel Name	Site-to-Site	
Description	Enter Tunnel Description	
* Enabled State	• Enable 🔿 Disable	
* Tunnel Interface	vti1 ~	⊕ Add Tunnel Interface
* Authentication Mode	Pre-shared Key \sim	
* Key	••••	
* Confirm Key	•••••	
* Local Address	• Interface ①	
	Ge0/2 V	
* Peer Address	10.1.5.211	Ping
* Local ID Type	IPV4_ADDRESS ~	
Verify Peer ID		
≣ ∓ Advanced		
Cancel	Next	

After completing the basic configuration, click $\ensuremath{\textit{Next}}.$

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.

	⊘ Basic Config	Interesting	g Traffic Config	3 Security Parameter Co	onfig
🕀 Cre	eate 🔟 Delete		Enter th	e keyword.	Q
	Proxy Mode	Local Network	Peer Network	Operation	
	Subnet-to-Sub	192.168.1.0/24	192.168.2.0/24	Edit Delete	
10 ~	/ Page Total:1			Go to 1 < 1	>

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.

- 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).
- 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.

⊘		3	
Basic Config Intere	sting Traffic Config	Security Parame	ter
		Config	
IKE Parameter			
* Negotiation Mode	IKEv1 Main Mode	\sim	
* Encryption Algorithm	AES-128 🛞	~	
* Verification Algorithm	SHA ®	\sim	
* DH Group	GROUP5 ®	~	
* ① SA Lifetime	86400		Second
IPsec Parameter			
* Protocol	ESP	~	
* Encapsulation Mode	Tunnel	~	
* Encryption Algorithm	AES-128 🛞	~	
* Verification Algorithm	SHA ®	\sim	
Perfect Forward Secrecy			
* (1) SA Lifetime	3600		Second

Click Finish to complete the configuration for the IPsec tunnel.

Cancel

(3) Create security policies.

Previous

Finish

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			
⊕ Create Im Delete C Refresh						
Name	I	IP Address/Range	Address Group			
Name VPN-remote		IP Address/Range	Address Group			

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 Sec	Back Edit Security Policy					
Basic Info						
* Name	VPN-outbound					
Enabled State	• Enable 🔿 Disable					
* Policy Group	Default Policy Group ~	Add Group				
Description	Enter the security policy name descrip					
Src. and Dest.						
* Src. Security Zone	any \vee					
* Src. Address	VPN-localsubnet \sim					
User/User Group	any \checkmark					
* Dest. Security	VPN-Zone ~					
Zone						
* Dest. Address	VPN-remotesubnet \sim					
Service						
Service	any \lor					

< Back Edit	Secu	rity Policy		
Basic	Info			
* N	lame	VPN-inbound		
Enabled	State	• Enable 🔿 Disable		
* Policy G	roup	Default Policy Group	Add (Group
Descrip	otion	Enter the security policy name descrip		
Src. and I	Dest.			
* Src. Security 2	Zone	VPN-Zone	/	
* Src. Add	dress	VPN-remotesubnet	~	
User/User G	roup	any	~	
* Dest. Sec	urity	any	/	
2	Zone			
* Dest. Add	dress	VPN-localsubnet	~	
Sei	rvice			
Se	rvice	any	/	

- (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 Rout	ting
ІР Туре	IPv4
* Dest. IP Range/Mask	192.168.2.0/24
Next-Hop Address	
Interface	vti1 ~
* ① Priority	5
Link Detection	Link Detection ~
Description	ipsec-route
	1

- 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:
 - 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 B: 10.1.5.211.
 - o Set Tunnel Remote Address to the default outbound interface address of Site A: 10.1.5.203.

< Back Edit Tunnel Interface Details						
* Interface Name	vti1					
Security Zone	Select Security Zone <	⊕ Add Security Zone				
* Tunnel Local Address	10.1.5.211					
Tunnel Remote Address	• IP 🔿 Dynamic					
	10.1.5.203					
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 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 10.1.5.203.
- 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 ①	point ()
* Tunnel Name	Site-to-Site	
Description	Enter Tunnel Description	
* Enabled State	• Enable 🔿 Disable	
* Tunnel Interface	vti1 ~	Add Tunnel Interface
* Authentication Mode	Pre-shared Key V	
* Key	•••••	
* Confirm Key	•••••	
* Local Address	• Interface ①	
	Ge0/2 ~	
* Peer Address	10.1.5.203	Ping
* Local ID Type	IPV4_ADDRESS ~	
Verify Peer ID		
≣ ∓ Advanced		
Cance	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 192.168.2.0/24 and Peer Network to 192.168.1.0/24.

	O Basic Config	Interesting 1) Iraffic Config S	ecurity Parameter Config)
🕀 Cre	eate 🔟 Delete		Enter the	keyword.	Q
	Proxy Mode	Local Network	Peer Network	Operation	
	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.

- 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).
- 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.

6	>	⊘		3				
Basic	Config Intere		sting Traffic	ting Traffic Config		Security Parameter		
						Config		
	IKE Paran	neter						
	* Negotiation N	Node	IKEv1 Mai	n Mode		~		
*	Encryption Algo	rithm	AES-128 🛞			~		
*	Verification Algo	rithm	SHA 🛞			~		
	* DH G	iroup	GROUP5 ®			~		
	* 🕕 SA Life	etime	86400				Second	
	IPsec Paran	neter						
	* Pro	tocol	ESP			~		
	* Encapsulation N	Node	Tunnel			~		
*	* Encryption Algorithm		AES-128 🛞			~		
*	Verification Algo	rithm	SHA 🛞			~		
Pe	erfect Forward Se	crecy						
	* (1) SA Life	etime	3600				Second	
	Previous		Cancel	Fini	sh			

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
⊖ Create 🗓 De	elete C Refresh		
Name	I	P Address/Range	Address Group
VPN-remot	esubnet	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 Secu	rity Policy	
Basic Info		
* Name	VPN-outbound	
Enabled State	• Enable 🔿 Disable	
* Policy Group	Default Policy Group ~	⊕ Add Group
Description	Enter the security policy name descrip	
Src. and Dest.		
* Src. Security Zone	any \lor	
* Src. Address	VPN-localsubnet \sim	
User/User Group	any \lor	
* Dest. Security	VPN-Zone ~	
Zone		
* Dest. Address	VPN-remotesubnet \sim	
Service		
Service	any \checkmark	

< Back Edit Secu	rity Policy	
Basic Info		
* Name	VPN-inbound	
Enabled State	• Enable 🔿 Disable	
* Policy Group	Default Policy Group	Add Group
Description	Enter the security policy name descrip	
Src. and Dest.		
* Src. Security Zone	VPN-Zone	/
* Src. Address	VPN-remotesubnet	~
User/User Group	any	/
* Dest. Security	any	/
Zone		
* Dest. Address	VPN-localsubnet	/
Service		
Service	any	/

- (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 Rou	ting
	IP Туре	IPv4
* [Dest. IP Range/Mask	192.168.1.0/24
	Next-Hop Address	
	Interface	vti1 ~
	* () Priority	5
	Link Detection	Link Detection ~
	Description	ipsec-route

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 nam	e.	Q
Tunnel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s)	Sei	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 C Refresh						innel name.	Q
Tunnel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packe	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.

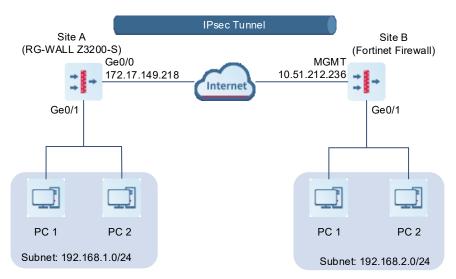


Figure 8-21 Site-to-Site Networking

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)	(2)		3		(4)
Basic Config	Authentication	n Config I	nteresting Tra	ffic Config	Config Verification
	* ① Tunnel Interface * Tunnel Name	vti 2 tunnel-to-Forti	net	8	
	* Scenario	Point-to-Poin	t 🔿 Point-t	o-Multipoint	
			Interne		ch Office
		Main Offi	ce		
				Brand	ch Office
	Cance	el Ne	xt		

- 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).
 - 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.

Ø	2-			-3		4
Basic Config	Authenticatio	n Config	Interesting	g Traffic Config	(Config Verification
	* Peer Address	10.51.212.2	236		Ping]
	* Outbound Interface	Ge0/0		~		
	* Authentication Mode	• Pre-share	ed Key			
	* 🕕 Key	•••••				
	* 🕕 Confirm Key	•••••		(\otimes)		
	Previous	Cancel	Next			

- (3)
 - a After completing the configuration, click **Next**.
- (4) Interesting Traffic Configuration
 - a Click Create. Configure parameters for interesting traffic as follows:
 - 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.

Proxy Mode Local Network Peer Network Operation Subnet-to-Su 192.168.1.0/24 192.168.2.0/24 Edit Delete	Creat	e 🛄 Delete		Enter the	e keyword.	Q
Subnet-to-Su 192.168.1.0/24 192.168.2.0/24 Edit Delete		Proxy Mode	Local Network	Peer Network	Operation	
		Subnet-to-Su	192.168.1.0/24	192.168.2.0/24	Edit Delete	
10 ∨ / Page Total:1 Go to 1 ✓ 1 >	10 ~	/ Page Total:1			Go to 1	1

- b After completing the configuration, click **Next**.
- (5) Verification
 - a Verify that the basic configuration, authentication configuration, and interesting traffic configuration are correct.

Ø			 		4)
Basic Config	Authenticatio	on Config	Interesting Traffic	Config Co	onfig Verification
	Basic Config	Edit			
	Tunnel Interface	vti2	\sim		
	Tunnel Name	tunnel-to-Fortinet			
	Scenario	Point-to-Point ()	Point-to-Multip	point ()	
	Authentication Config	Edit			
	Peer Address	10.51.212.236			
	Outbound Interface	Ge0/0	~		
	Authentication Mode	 Pre-shared Key 			
	① Кеу	00000			
	Interesting Traffic Config	Edit			
	Local Network		Peer	Network	
	192.168.1.0/24		192.16	58.2.0/24	

b Click **Advanced Settings** and modify the following IKE and IPsec parameters. Use the default configuration for the other parameters.

IKE parameters:

- Set IKE Version to IKEv1.
- Set Negotiation Mode to IKEv1 Main Mode.
- Set Encryption Algorithm to AES-128.
- o Set Verification Algorithm to SHA.
- Set DH Group to GROUP5.

Advanced Settings	Fold	
* Local ID Type	IPV4_ADDRESS ~	
① Peer ID Authentication		
DPD Type	Regular Mode \vee	
DPD Detection Interval	30	Second
DPD Retry Interval	5	Second
IKE Parameter		
IKE Parameter * ① IKE Version	✓ IKEv1 □ IKEv2	
	✓ IKEv1 ☐ IKEv2 IKEv1 Main Mode ∨	
* ① IKE Version		
* ① IKE Version * ① Negotiation Mode	IKEv1 Main Mode	
* ① IKE Version * ① Negotiation Mode * Encryption Algorithm	IKEv1 Main Mode ~ AES-128 ® ~	

IPsec parameters:

- Set Encryption Algorithm to AES-128.
- Set Verification Algorithm to SHA.
- Enable Perfect Forward Secrecy.
- Set DH Group to GROUP5.

∃↑ IPsec Parameter

	* Protocol	ESP		~	
* En	capsulation Mode	Tunnel		\sim	
* Enc	ryption Algorithm	AES-128 (8)		~	
* Verit	fication Algorithm	SHA 🛞		~	
Perfec	t Forward Secrecy				
	* DH Group	GROUP5		~	
	* 🕕 SA Lifetime	3600			Second
	① Tunnel MTU	1400			
	Previous	Cancel	Finish		

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.
 - Set NAT configuration to No NAT between sites.
 - o For the device type, use the default configuration.

VPN Creation Wizard					
1 VPN Setup	2) Authentication $>$ 3) Policy & Routing $>$ 4) Review Settings $>$				
Name	tunnel-to-z32-s		Site to Site - FortiGate		
Template type	Site to Site Hub-and-Spoke Remote Access Custom				
NAT configuration	No NAT between sites				
	This site is behind NAT			Internet	
	The remote site is behind NAT		~		
Remote device type	FortiGate		This FortiGate		Remote FortiGate
	altalta Cisco				
		. Deals	Nexts		
		< Back	Next > Cancel		

- 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).
 - 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.

VPN Creation Wizard						
🕢 VPN Setup 🔪 🛛 A	Authentication > 3 Policy & Routin	g 🔪 👍 Review Settings				
Remote device	IP Address Dynamic DNS			Site to Site - FortiGate		
Remote IP address	172.17.149.218]	~
Outgoing Interface	i wan1 (mgmt)	-				
Authentication method	Pre-shared Key Signature				Internet	
Pre-shared key	•••••	۲		This FortiGate		Remote FortiGate
				This Fortigate		nemole Fondale
			< Back	Next > Cancel		

- 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.

Product Cookbook

VPN Creation Wizard			
VPN Setup	Authentication 3 Policy & Routing	Review Settings	
Local interface	im wan1 (mgmt) ★	Site to Site - FortiGate	
Local subnets	192.168.2.0/24		\wedge
	0	Internet	
Remote Subnets	192.168.1.0/24		
	O	This FortiGate Re	emote FortiGate
Internet Access	None Share Local Use Remote		
		< Back Next > Cancel	

b After completing the configuration, click **Next**. The **Review Settings** page is displayed.

VPN Creation Wizard				
VPN Setup 🔪 🗸	Authentication 🔪 🕢 Policy & Routing 🔪 🥥 Review Settings			
Interpretation of the following set	tings should be reviewed prior to creating the VPN.			
Object Summary				
Phase 1 interface	tunnel-to-z32-s			
Local address group	tunnel-to-z32-s_local			
Remote address group	tunnel-to-z32-s_remote			
Phase 2 interface	tunnel-to-z32-s			
Static route	static			
Blackhole route	static			
Local to remote policies	vpn_tunnel-to-z32-s_local			
Remote to local policies	vpn_tunnel-to-z32-s_remote			
		< Back	Create	Cancel

- c After verifying the configuration, click **Create**.
- (4) VPN Authentication Configuration
 - a Choose **VPN** > **IPsec Tunnels**. The IPsec tunnel page is displayed.

+Create New - 🖋 Edit	Delete Matching Lo	gs Search	(٩	
	Tunnel ≑		Interface Binding \$	Status ≑	Ref. ≑
🖃 💷 Site to Site - FortiGate	0				
O 11		internal (port5)		O Inactive	2
🔮 s2s		m port2		O Inactive	2
🔮 tunnel-to-z32-s		🖷 wan1 (mgmt)		O Inactive	4
Type Remu Phase Com	e 2 Tunnel e 2 Tunnel e 1 tunnel-to-z32-s tunnel-to-z32-s VPN: tunnel-to-z32-s (Cr wizard) rences 4				

b Select the tunnel created in the previous step, and click **Edit**. In the dialog box that is displayed, click **Convert To Custom Tunnel**.

Product Cookbook

+Create New - & Edit 🗍 🙃 Delete 🖬 Sho	w Matching Logs Search	Edit VPN Tunnel		
Tunnel 🗢		Tunnel Template	Site to Site - FortiGate	
			Convert To Custom Tunnel	
• 11	🏾 internal (port5)			
⊙ s2s	m port2	Name	tunnel-to-z32-s	
😋 tunnel-to-z32-s	🖮 wan1 (mgmt)	Comments	VPN: tunnel-to-z32-s (Created by VPN wizard)	
🛨 😐 Custom 📎			by VPN wizard) // 44/255	
		Network	& Edit	
		Remote Gatewa	r: Static IP Address (172.17.149.218) , Outgoing Interface : mgmt	
		Authentication		
		Authentication	fethod : Pre-shared Key	
		Phase 2 Selectors		
			cal Address Remote Address	
		tunnel- to- tunnel	I-to-z32-s_local tunnel-to-z32-s_remote	
		z32-s		
			OK Cancel	

c Click **Edit** in the **Phase 1 Proposal** area and modify the authentication parameters according to the following figure.

Phase 1 Proposal	🖋 Edit
Algorithms : AES128-SHA256, AES256-SHA256, AES128-SHA1, AES256-S	SHA1
Diffie-Hellman Groups : 14, 5	

- o Set Encryption to AES128.
- Set Authentication to SHA1.
- Set Diffie-Hellman Group to 5.
- o Use the default configuration for the other parameters.

	Phase 1 Proposal	O Add				3	0 0
1	Encryption	AES128	•	Authentication	SHA1	•	_
	Diffie-Hellman Group		 32 21 15 	31 30 0 20 19 0 14 √ 5 0) 27) 16	
	Key Lifetime (secor	nds)	86400) 2] '	
	Local ID						

d Click the edit icon in the **Phase 2 Proposal** area and modify the authentication parameters according to the following figure.

Phase 2 Selectors	5		
Name	Local Address	Remote Address	O Add
tunnel-to-z32-s	tunnel-to-z32-s_local	tunnel-to-z32-s_remote	ø

- 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.
- Set Authentication to SHA1.
- Set Diffie-Hellman Group to 5.
- o Use the default configuration for the other parameters.

Edit Phase 2			4 🔊 ว
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	O Add		_
Encryption	AES128	✓ Authentication SHA1	✓ 2
Enable Replay Det	ection 🔽		
Enable Perfect For	ward Secree	:y (PFS) 🔽	
Diffie-Hellman Gro	oup		7 6
Local Port		All 🗹 🛛 3	
Remote Port		All 🔽	
Protocol		All 🔽	
Auto-negotiate			
Autokey Keep Aliv	e		
Key Lifetime		Seconds 👻	
Seconds		43200	

e After completing the modification, click **OK**.

Product Cookbook

+Create New - & Edit B Delete Mil Show		Edit VPN Tunnel				
		Name	tunnel-to-z32-	s		
				-z32-s (Created by VPN	4	
• 11	internal (port5)	Comments	wizard)			
O s2s	m port2				le.	
	i wan1 (mgmt)	Network				
E 🖵 Custom 🙆						
		Remote Gateway	Static IP Address (172.)	17.149.218), Interface:	mgmt	
		Authentication			🖋 Edit	
		Authentication M	ethod : Pre-shared Key			
		IKE Version: 1, M	ode : Main (ID protectio	n)		
		Phase 1 Proposal			🖋 Edit	
		Algorithms: AES1	28-SHA1			
		Diffie-Hellman Gr	oup:5			
		XAUTH			🖋 Edit	
		Type : Disabled				
		Phase 2 Selectors				
		Name	Local Address	Remote Address	O Add	
		tunnel-to-z32-s	192.168.2.0/24	192.168.1.0/24	1	
					1	
				ОК	Cancel	

6. Verification

Verifying Configuration of Site A (RG-WALL Z3200-S)

• Choose Network > IPsec VPN > Tunnel Monitoring. Verify that the tunnel status is Established.

Tunnel I	Vonitoring								
⊘ Start	t 🛇 Stop 😋 Refresh	Custom Field						Enter a tunnel name	
	Tunnel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Received Packets (By	Operation
	tunnel-to-Fortinet	Established	Point-to-Point	10.51.212.236	192.168.1.0/24->192.168.2.0/24	3596	0	0	Stop

• Choose Monitor > Log Monitoring > IPsec VPN Log. Check IPsec tunnel negotiation logs.

IPsec VPN Logs				
🚺 Export 🖸 Refre	esh Custom Field	Date 2024-08-23	to 2024-08-23	Log Level All ~ Inter a tunnel name, a peer address or a details. Q
Log Level	Time	Tunnel Name	Peer Address	Details
Medium	Time 2024-08-23 19:22:37	tunnel-to-Fortinet	Peer Address 10.51.212.236	Details IKE SA建立完成,cookle为: bce7f9412dacc6a4;8ca6232faf5d9cce

Verifying Configuration of Site B (Fortinet Firewall)

• Choose VPN > IPsec Tunnels. Verify that the tunnel status is established.

+Create New - Create New - Edit Delete	tching Logs Search	Q			
Tunnel 🗢	Interface Binding 🗢	Ref. \$	Template 🗢		
🖸 🗢 inactive 🕥					
♦ tunnel-to-z32-s	🖮 wan1 (mgmt)	4	😐 Custom		

• Select the IPsec tunnel and click **Show Matching Logs** to view IPsec tunnel negotiation logs.

Product Cookbook

+Create New - Kelit 🖻 Delete	ogs Search	Q			
Tunnel 🗢	Interface Binding 🗢	Ref. 🗘	Template 🗘		
D • inactive •					
O tunnel-to-z32-s	🖮 wan1 (mgmt)	4	😐 Custom		

Summary O Logs						
C VPN Tunnel == tunnel-to-z3						
Date/Time	Level	Action	Status	Message	VPN Tunnel 🛛 💙	
2024/08/23 19:18:45		tunnel-stats		IPsec tunnel statistics	tunnel-to-z32-s	
2024/08/23 19:16:30		negotiate	success	negotiate IPsec phase 2	tunnel-to-z32-s	
2024/08/23 19:16:30		negotiate	success	progress IPsec phase 2	tunnel-to-z32-s	
2024/08/23 19:16:30		negotiate	success	progress IPsec phase 2	tunnel-to-z32-s	
2024/08/23 19:16:30		tunnel-up		IPsec connection status change	tunnel-to-z32-s	
2024/08/23 19:16:30		phase2-up		IPsec phase 2 status change	tunnel-to-z32-s	
2024/08/23 19:16:30		install_sa		install IPsec SA	tunnel-to-z32-s	
2024/08/23 19:16:30		negotiate	success	progress IPsec phase 1	tunnel-to-z32-s	
2024/08/23 19:16:30		negotiate	success	progress IPsec phase 1	tunnel-to-z32-s	
2024/08/23 19:16:30		negotiate	success	progress IPsec phase 1	tunnel-to-z32-s	
2024/08/23 19:16:30		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 8-30Products and Versions

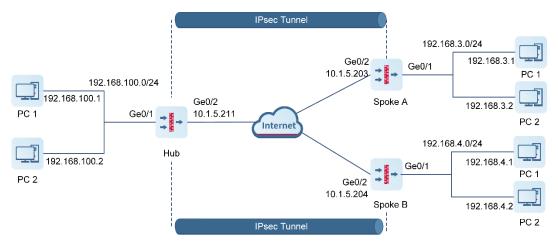
Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R6 or later

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 <u>Figure 8-22</u>. In a pointto-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.





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.
 - 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.

1 Basic Config	2 Authentication	3 (4) a Config Interesting Traffic Config Config Verification
	* (1) Tunnel Interface * Tunnel Name	vti 100
		Hub-Spoke O Point-to-Point O Point-to-Multipoint
		Main Office Branch Office
	Cancel	Next

- $\label{eq:constraint} c \quad \mbox{After completing the configuration, click } \textbf{Next}.$
- (2) Configure authentication.
 - a Configure parameters according to the following figure.

Ø	2		3		4
Basic Config	Authentication	Config	Interesting Traffic Config		Config Verification
	* Outbound Interface	Ge0/2		\sim	
	* Authentication Mode	• Pre-sł	hared Key		
	* Key	•••••	٠		
	* Confirm Key	•••••	•	(\times)	

	Previous	Cancel	Next
--	----------	--------	------

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

(3) Configure interesting traffic.

a Click **Create**. Configure parameters for interesting traffic according to the following figure.

⊘ asic Config	Authe	ntication Config		3) Traffic Config	Config Veri
🕒 Crea	te 🔟 Delete		Enter the	e keyword.	Q
	Proxy Mode	Local Network	Peer Network	Operation	
	Auto	any	any	Edit Delete	
10 ~	/ Page Total:1			Go to 1	1

Previous	Cancel	Next
----------	--------	------

- b After completing the configuration, click **Next**.
- (4) Verify configuration.
 - a After verifying the configuration, click **Finish**.

⊘ Basic Config	Authentication) Config Inte	eresting Traffic Confi	Config Verificatio	on
① The tunnel configured on the wizard will be added to the	he custom tunnel list.				
	Basic Config	Edit			
	Tunnel Interface	vti100			
	Tunnel Name	Hub-Spoke			
	Scenario	Point-to-Point (1)	 Point-to-Multipoin 	t ()	
	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 Car	ncel 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	34)
Basic Config	Authentication	Config Interesting Traffic Config Config Verification
	* () Tunnel Interface	vti 100
	* Tunnel Name	Site-to-Site 🛞
	* Scenario	Point-to-Point Point-to-Multipoint
		Main Office Branch Office
	Cancel	Next

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

(2) Configure authentication.

a Configure parameters according to the following figure.

Ø	2)	3		4
Basic Config	Authenticati	on Config	Interesting Traffic Conf	fig	Config Verification
	* Peer Address	10.1.5.211	\otimes	Ping	
	* Outbound Interface	Ge0/2	~		
	* Authentication Mode	• Pre-shared H	Key		
	* Key	*****			
	* Confirm Key	•••••			

Previous	Cancel	Next

- 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 Co	nfig	Authen	tication Config	Interesting Traffic	Config	Config Verification
	🕀 Crea	ite 🔟 Delete		Enter the k	eyword.	Q
		Proxy Mode	Local Network	Peer Network	Operation	
		Subnet-to-Subnet	192.168.3.0/24	192.168.100.0/24	Edit Delete	2
	10 ~	/ Page Total:1		G	Go to 1	1

- b After completing the configuration, click **Next**.
- (4) Verify configuration.
 - a After verifying the configuration, click **Finish**.

Ø)			4
Basic Config	Authenticati	on Config	Interesting Traffic	c Config	Config Verification
d will be added to the cu	istom tunnel list.				
	Basic Config	Edit			
	Tunnel Interface	vti100			
	Tunnel Name	Site-to-Site			
	Scenario	Point-to-Point ()	Point-to-Multipo	vint 🕕	
	Authentication Config	Edit			
	Peer Address	10.1.5.211			
	Outbound Interface	Ge0/2			
	Authentication Mode	 Pre-shared Key 			
	Кеу				
	Interesting Traffic Config	Edit			
	Local Network		Peer	Network	
	192.168.3.0/24		192.16	8.100.0/24	
	Advanced Settings	Expand			
	Previous	Cancel Finis	h		

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:
 - o Set Interface Name to vti100.
 - 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 the hub site: 10.1.5.211.
 - o Set Tunnel Remote Address to Dynamic.

< Back Create Tunnel	Interface Details	
* Interface Name	vti100	
Security Zone	VPN-Zone v	⊕ Add Security Zone
* Tunnel Local Address	10.1.5.211	
Tunnel Remote Address	O IP O 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:

- Set Tunnel Name to Hub-Spoke.
- o Set Enabled State to Enable.
- Set Tunnel Interface to vti100.
- Set Local Address to interface Ge0/2.
- For Authentication Mode, use the default value **Pre-shared Key**. Set both **Key** and **Confirm Key** to **ruijie123**.
- 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 ① Point-to-Multip 	oint 🕕
* Tunnel Name	Hub-Spoke	
Description	Enter Tunnel Description	
* Enabled State	• Enable 🔿 Disable	
* Tunnel Interface	vti100 v	
* Authentication Mode	Pre-shared Key \sim	
* Key	•••••	
* Confirm Key		
* Local Address	• Interface 🔿 IP	
	Ge0/2 ~	
* Local ID Type	IPV4_ADDRESS v	
Verify Peer ID		
≣ ↑ Advanced		
Reverse Route Injection		
Next-Hop Address	Enter Next-Hop Address	
* Priority	5	
С	ancel 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 Auto.

	Ø	2)	3
	Basic Config	Interesting Tr	affic Config	Security Parameter Config
🕀 Create	🗓 Delete		Enter t	he keyword. Q
	Proxy Mode	Local Network	Peer Network	Operation
	Auto	any	any	Edit Delete
10 ~	/ Page Total:1			Go to 1 < 1 >

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.

- 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).
- 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.

Ø			3	
Basic Config	Interes	ting Traffic Config	Security Parame	ter
			Config	
IKE	Parameter			
* Negotia	tion Mode	IKEv1 Main Mode	~	
* Encryption	Algorithm	AES-128 🛞	~	
* Verification	Algorithm	SHA 🛞	~	
*	DH Group	GROUP5 ®	~	
* 🕕 S	SA Lifetime	86400		Second
IPsec	Parameter			
	* Protocol	ESP	~	
* Encapsula	tion Mode	Tunnel	~	
* Encryption	Algorithm	AES-128 🛞	~	
* Verification	Algorithm	SHA 🛞	~	
Perfect Forwa	rd Secrecy			
* 🕕 S	SA Lifetime	3600		Second
<u>()</u> Ti	unnel MTU	1400		
Previou	s	Cancel Finis	sh	

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 Se	ecurity Policy		
Basic Info			
* Name	VPN-hub-outbound		
Enabled State	• Enable 🔿 Disable		
* Policy Group	Default Policy Group	~	⊕ Add Group
* Adjacent Policy	Default Policy	~	Before \vee
Description	Enter the security policy name descrip		
Src. and Dest.			
* Src. Security Zone	any	~	
* Src. Address	any	~	
User/User Group	any	~	
* Dest. Security	VPN-Zone	~	
Zone			
* Dest. Address	any	~	
Service			
Service	any	~	

< Back Create Se	ecurity Policy		
Basic Info			
* Name	VPN-hub-inbound		
Enabled State	• Enable 🔿 Disable		
* Policy Group	Default Policy Group	~	Odd Group
* Adjacent Policy	Default Policy	~	Before \lor
Description	Enter the security policy name descrip		
Src. and Dest.			
* Src. Security Zone	VPN-Zone	~	
* Src. Address	any	~	
User/User Group	any	~	
* Dest. Security	any	\sim	
Zone			
* Dest. Address	any	~	
Service			
Service	any	~	

- 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:
 - o Set Interface Name to vti1.
 - o 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.
 - o Set **Tunnel Remote Address** to the default outbound interface address of the hub site: 10.1.5.211.

< Back Edit Tunnel Int	erface Details	
* Interface Name	vti1	
Security Zone	VPN-Zone v	⊕ Add Security Zone
* Tunnel Local Address	10.1.5.203	
Tunnel Remote Address	• IP 🔿 Dynamic	
	10.1.5.211	
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:

- 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.
- 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 () O Point-to-Multip	point ()
* Tunnel Name	Site-to-Site	
Description	Enter Tunnel Description	
* Enabled State	• Enable 🔿 Disable	
* Tunnel Interface	vti1 ~	
* Authentication Mode	Pre-shared Key \lor	
* Key	•••••	
* Confirm Key	•••••	
* Local Address	• Interface ①	
	Ge0/2 ~	
* Peer Address	10.1.5.211 🛞	Ping
* Local ID Type	IPV4_ADDRESS ~]
Verify Peer ID		
≣ ∓ Advanced		
C	ancel 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		Interesting	2) Traffic Config	3 Security Parameter Config
🕀 Crea	ate 🔟 Delete		Enter t	the keyword. Q
	Proxy Mode	Local Network	Peer Network	Operation
	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.

- 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).
- 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.

Ø		3	
Basic Config Interesting Traffic Config Security Pa			er
		Config	
IKE Parameter			
* Negotiation Mode	IKEv1 Main Mode	~	
* Encryption Algorithm	AES-128 (8)	~	
* 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 Finis	sh	

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
⊖ Create 🗓 De	elete C Refresh		
Name		IP Address/Range	Address Group
VPN-remote	esubnet	192.168.100.0/24	-

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.

K Back Edit Secu	rity Policy	
Basic Info		
* Name	VPN-outbound	
Enabled State	• Enable 🔿 Disable	
* Policy Group	Default Policy Group	Add Group
Description	Enter the security policy name descrip	
Src. and Dest.		
* Src. Security Zone	any ~	
* Src. Address	VPN-localsubnet	
User/User Group	any ~	
* Dest. Security	VPN-Zone ~	
Zone		
* Dest. Address	VPN-remotesubnet ~	
Service		
Service	any ~	

< Back Edit Security Policy					
Basic Info					
* Name	VPN-inbound				
Enabled State	• Enable 🔿 Disable				
* Policy Group	Default Policy Group	• O Add Group			
Description	Enter the security policy name descrip				
Src. and Dest.					
* Src. Security Zone	VPN-Zone v	·			
* Src. Address	VPN-remotesubnet	·			
User/User Group	any	,			
* Dest. Security	any	r			
Zone					
* Dest. Address	VPN-localsubnet ~	,			
Service					
Service	any v	·			

- (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 Ro	uting
IP Туре	IPv4
* Dest. IP Range/Mask	192.168.100.0/24
Next-Hop Address	
Interface	vti1 ~
* () Priority	5
Link Detection	Link Detection \lor
Description	ipsec-route

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 Fi	eld			Enter a tunnel name.	Q
Tunnel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s) Ser	n 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 Fiel	d			Enter a tunnel name	a Q
Tunnel Name	Tunnel Status	Туре	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 <u>Figure 8-23</u>, 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.

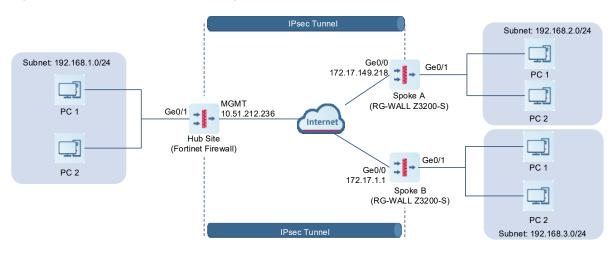


Figure 8-23 Site-to-Multisite Networking

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	2_					4
Basic Config	Authenticatio	on Config	Interes	sting Traffic C	onfig	Config Verification
	* ① Tunnel Interface * Tunnel Name	vti 2 tunnel-to-	Fortinet		8	
	* Scenario	 Point-to- 	Point) Point-to-Mu	ltipoint	
		Main	Office	Internet	Branch Of Branch Of	
	Cance	el	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.

Ø	2-			-3		4
Basic Config	Authenticatio	on Config	Interestin	g Traffic Con	fig	Config Verification
	* Peer Address	10.51.212.2	236		Ping]
	* Outbound Interface	Ge0/0		```	~	
	* Authentication Mode	• Pre-share	ed Key			
	* 🕦 Key	•••••				
	* 🕕 Confirm Key	•••••			0	
	Previous	Cancel	Nex	t		

- b After completing the configuration, click **Next**.
- (3) Interesting Traffic Configuration
 - a Click Create. Configure parameters for interesting traffic according to the following figure.
 - 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.

Create	🔟 Delete		Enter the	e keyword.	Q
Pr	oxy Mode	Local Network	Peer Network	Operation	
Sub	net-to-Su	192.168.2.0/24	192.168.1.0/24	Edit Delete	
10 ~	/ Page Total:1	I		Go to 1	1

- b After completing the configuration, click **Next**.
- (4) Verification
 - a Verify that the basic configuration, authentication configuration, and interesting traffic configuration are correct.

Ø	⊘				4
Basic Config	Authenticatio	on Config	Interesting Traffic	c Config Co	onfig Verification
	Basic Config	Edit			
	Tunnel Interface	vti2	\sim		
	Tunnel Name	tunnel-to-Fortinet			
	Scenario	Point-to-Point	 Point-to-Multip 	point 🕕	
	Authentication Config	Edit			
	Peer Address	10.51.212.236			
	Outbound Interface	Ge0/0	\sim		
	Authentication Mode	Pre-shared Key			
	① Кеу				
	Interesting Traffic Config	Edit			
	Local Network		Peerl	Network	
	192.168.2.0/24		192.16	58.1.0/24	

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.
- Set Negotiation Mode to IKEv1 Main Mode.
- Set Encryption Algorithm to AES-128.
- Set Verification Algorithm to SHA.
- o Set DH Group to GROUP5.

Advanced Settings	Fold	
* Local ID Type	IPV4_ADDRESS ~	
① Peer ID Authentication		
DPD Type	Regular Mode \vee	
DPD Detection Interval	30	Second
DPD Retry Interval	5	Second
IKE Parameter		
* ① IKE Version	✓ IKEv1 ☐ IKEv2	
* ① Negotiation Mode	IKEv1 Main Mode \sim	
* Encryption Algorithm	AES-128 🛞 🗸	
* () Verification Algorithm	SHA ®	
* DH Group	GROUP5 🛞 🗸	
* (1) SA Lifetime	86400	Second

IPsec parameters:

- Set Encryption Algorithm to AES-128.
- Set Verification Algorithm to SHA.
- Enable Perfect Forward Secrecy.
- Set DH Group to GROUP5.

≣↑ IPsec Parameter

* Protocol	ESP		~	
* Encapsulation Mode	Tunnel		\sim	
* Encryption Algorithm	AES-128 🛞		\sim	
* Verification Algorithm	SHA 🛞		~	
Perfect Forward Secrecy				
* DH Group	GROUP5		~	
* 🕕 SA Lifetime	3600			Second
① Tunnel MTU	1400			
Previous	Cancel	Finish		

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:
 - Set Template type to Hub-and-Spoke.
 - o Select Role to Hub.

VPN Creation W	Izard	
1 VPN Setup	> ② Authentication > ③ Tunnel Interface > ④ Policy & Routing > ⑤ R	eview Settings
Name Template type	tunnel-to-RJ Site to Site Hub-and-Spoke Remote Access Custom The Hub-and-Spoke VPN will be set up using auto-discovery with BGP as the routing protocol. State of the set up using auto-discovery with BGP as the routing protocol.	Hub-and-Spoke - FortiGate (Hub)
Role 🚯	Hub Spoke	This FortiGate Remote FortiGate Remote FortiGate
		< Back Next > Cancel

- 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).
 - 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.

VPN Creation Wizard				
	i wan1 (mgmt)	e Dolicy & Routing G Review Settings	Hub-and-Spoke - FortiGate (Hub)	Remote FortiGate
		< Back	Next > Cancel	

- b After completing the configuration, click Next.
- (3) Tunnel Interface Configuration

Use the default configuration for parameters on this page and click Next.

Product Cookbook

VPN Creation Wizard							
🗸 VPN Setup 🔪 🗸 A	uthentication 🔰 3 Tunnel Interface 🔪	4 Policy & Routing 5 Re	view Settings				
Tunnel IP () Remote IP/netmask ()	10.10.3.1			Hub-a	ind-Spoke - FortiG	ate (Hub)	Spoke1
				Ţ	Hub This FortiGate	Internet	Remote FortiGate
			< Back	Next >	Cancel		

- (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.
 - For **Spoke neighbor group**, click **Create**. Set **Name** and **Remote AS** as required, and select the local WAN interface **wan1(mgmt)** as the interface.

VPN Creation Wizard						
🕢 VPN Setup 🔪 🖉	Authentication > 🕢 Tunnel Interface	• 4 Policy & Routing > 5 Revie	w Settings			
Local AS	1			Hub-and-Spoke - FortiGate (Hub)	
Local interface	🖮 wan1 (mgmt) 🗙					Spoke1
Local subnets	192.168.1.0/24				[
	0			Hub		Remote FortiGate
Spoke type	Range Individual				Internet	
Spoke range prefix	192.168.0.0/24					Spoke2
Spoke neighbor group	rj 🗸			This FortiGate		
					L	
						Remote FortiGate
			< Back	Next > Cancel		
VPN Creation Wizard			Add BGP Neighbor	Group		
🕑 VPN Setup > 🖉		💊 🕘 Policy & Routing 🔪 🌀 Rev	Name	ri		
Local AS	1		Remote AS	2		
Local interface	🖮 wan1 (mgmt)		Interface	wan1 (mgmt)	×	
	+		interface	+		
Local subnets	192.168.1.0/24		Activate IPv4 🕥			
	•		Activate IPv6 🕥			
Spoke type	Range Individual					
Spoke range prefix	192.168.0.0/16					
Spoke neighbor group	· · · · · · · · · · · · · · · · · · ·				ОК	Cancel
	Q Search + Create					

b After completing the configuration, click **Next**. The **Review Settings** page is displayed.

VPN Creation Wizard	
🗸 VPN Setup 🔪 🗸	Authentication 🔪 🗹 Tunnel Interface 🔪 🕢 Policy & Routing 🔪 🕄 Review Settings
• The following set	ttings 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
	< Back Create Cancel

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 I	Monitoring								
⊘ Start	t 🛇 Stop 😋 Refresh	Custom Field						Enter a tunnel name	e. Q
	Tunnel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Received Packets (By	Operation
	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				
🚺 Export 😋 Refr	esh 🗔 Custom Field	Date 2024-08-23	to 2024-08-23	Log Level All ~ Enter a tunnel name, a peer address or a details. Q
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
	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.

+	Create New 👻 🖋 Edit 🗎 🛍 Delete 🛛 🕍 Show Matching Logs 刘 Search	Q	
	Tunnel 🗢 🛛 🔻	Interface Binding 🗢	Ref. 🗘
	📰 Hub-and-Spoke - FortiGate (Hub) ②		
	🖸 tunnel-to-RJ	🖮 wan1 (mgmt)	4

• Select the IPsec tunnel and click **Show Matching Logs** to view IPsec tunnel negotiation logs.

tunnel-to-RJ

2024/08/23 21:26:46

+Create New - 🖋 Edit	t 🗊 Delete	Let Show Matching Logs	Search	Q		
	Tunnel	I ¢	T	Interface Binding 🗘		Ref. ≑
🗄 🖽 Hub-and-Spoke - Forti	iGate (Hub) 2					
💿 tunnel-to-RJ			🗎 wan1 (mgmt)		4	4
ummary 🚯 Logs						
VPN Tunnel == tu	nnel-to-RJ 🗙 🖸	Q Search			٩	🖵 VPN Events 🗸 🕞 Memory 🗸 🔲 Det
Date/Time		Level	Action	Status	Message	VPN Tunnel
24/08/23 21:26:46			negotiate	success	negotiate IPsec phase 2	tunnel-to-RJ
24/08/23 21:26:46			negotiate	success	progress IPsec phase 2	tunnel-to-RJ
24/08/23 21:26:46			negotiate	success	progress IPsec phase 2	tunnel-to-RJ
24/08/23 21:26:46			install_sa		install IPsec SA	tunnel-to-RJ
24/08/23 21:26:46			negotiate	success	progress IPsec phase 1	tunnel-to-RJ
24/08/23 21:26:46			negotiate	success	progress IPsec phase 1	tunnel-to-RJ
24/08/23 21:26:46			negotiate	success	progress IPsec phase 1	tunnel-to-RJ

success

progress IPsec phase 1

8.25.8 Configuration Examples of IPsec VPN with NAT Traversal

negotiate

1. Applicable Products and Versions

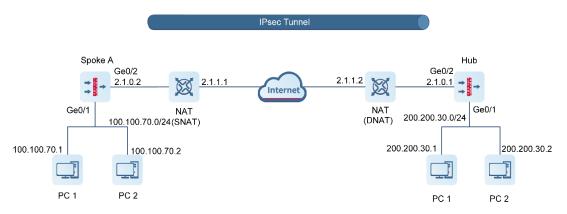
Table 8-32 Products and Versions

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.
 - 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.

1	2	3	4
Basic Config	Authentication Co	onfig Interesting Traffic Co	nfig Config Verification
	* ① Tunnel Interface	vti 100	
	* Tunnel Name	test1	
	* Scenario 🔘	Point-to-Point o Point-to-	Multipoint
		Internet Branch (
	Cancel	ext	

- c After completing the configuration, click **Next**.
- (2) Configure authentication.
 - a Configure parameters according to the following figure.

⊘ Basic Co	onfig A	wthentication	Config	Interestin	 onfig	4 Config Verification
	* Out	oound Interface	Ge0/2		\sim	
	* Authe	ntication Mode	• Pre-sł	nared Key		
		* Key	•••••	•		
		* Confirm Key	•••••	•	(\times)	
	Previous	Cancel		Next		

- b After completing the configuration, click **Next**.
- (3) Configure interesting traffic.
 - a Click Create. Configure parameters for interesting traffic according to the following figure.

\bigcirc			-	(3	4
Basic Co	onfig	Authe	ntication Config	Interesting	Traffic Config	Config Verification
	Crea	te 🔟 Delete		Enter th	e keyword.	Q
		Proxy Mode	Local Network	Peer Network	Operation	
		Auto	any	any	Edit Delete	
	10 ~	/ Page Total:1			Go to 1	1

Previous Cancel Next

- b After completing the configuration, click **Next**.
- (4) Verify configuration.
 - a After verifying the configuration, click **Finish**.

			(~)		4
Basic Config	Authenticati	on Config Interesting Traffic Cor		ffic Config	Config Verification
pe added to the custom tunnel lis	st.				
	Basic Config	Edit			
	Tunnel Interface	vti100	\sim		
	Tunnel Name	test1			
	Scenario	Point-to-Point ()	Point-to-Multi	point 🕕	
A	uthentication Config	Edit			
	Outbound Interface	Ge0/2	\sim		
	Authentication Mode	Pre-shared Key			
	Key	0000000			
Inter	resting Traffic Config	Edit			
	Local Network		Pee	er Network	
	any			any	
	Advanced Settings	Expand			
r					
	Previous	Cancel Fin	ish		

- 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.

Basic Config	Authenticat	ion Config	Interesting Tra	the conny	Config Verificatio
	* () Tunnel Interface	vti 1			
	* Tunnel Name	test1		\otimes	
	* Scenario	• Point-to-Pe	oint 🔿 Point-to-	Multipoint	
		111	Branch	Office	
		Main Office			
			Branch		
			_		
	Cancel	Next			

- $\label{eq:constraint} \mathsf{After} \ \mathsf{completing} \ \mathsf{the} \ \mathsf{configuration}, \ \mathsf{click} \ \mathbf{Next}.$
- (2) Configure authentication.
 - a Configure parameters according to the following figure.

Ø	2)	3		4
Basic Config	Authenticati	on Config	Interesting Traffic Conf	ig	Config Verification
	* Peer Address	2.1.1.2	\otimes	Ping	
	* Outbound Interface	Ge0/2	~		
	* Authentication Mode	 Pre-shared 	Кеу		
	* 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	Auther	ntication Config	Interesting	3) Traffic Config	Config \
⊖ Creat	e 🔟 Delete		Enter th	e keyword.	Q
	Proxy Mode	Local Network	Peer Network	Operation	
	Subnet-to-Sub	100.100.70.0/24	200.200.30.0/24	Edit Delete	
10 🗸	/ Page Total:1			Go to 1	1 >

Previous	Cancel	Next

- b After completing the configuration, click **Next**.
- (4) Verify configuration.
 - a After verifying the configuration, click **Finish**.

⊖ Basic Config	Authentication	Config In	teresting Traffic Cor	ıfig Co ı	4 nfig Verification
I will be added to t	he custom tunnel list.				
	Basic Config	Edit			
	Tunnel Interface	vti1	~		
	Tunnel Name	test1			
	Scenario	Point-to-Point	Point-to-Multip	oint 🕕	
	Authentication Config	Edit			
	Peer Address	2.1.1.2			
	Outbound Interface	Ge0/2	~		
	Authentication Mode	 Pre-shared Key 			
	Key	•••••			
	Interesting Traffic Config	Edit			
	Local Network		Peer Netwo	ork	
	100.100.70.0/24		200.200.30.0)/24	
	Advanced Settings	Expand			
	Previous	ncel 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:
 - o Set Interface Name to test1.
 - o 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	test1	
Security Zone	VTI ~	⊕ Add Security Zone
* Tunnel Local Address	2.1.0.1	
Tunnel Remote Address	IP O 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 test1.
- Set Enabled State to Enable.
- o Set Tunnel Interface to test1.
- Set Local Address to interface Ge0/2.
- For Authentication Mode, use the default value **Pre-shared Key**. Set both **Key** and **Confirm Key** to **ruijie123**.
- Toggle on **Reverse Route Injection** for the hub site. For **Priority**, use the default value 5. Do not configure **Next-Hop Address**.

0	3	
Basic Config Interestin	ng Traffic Config Security Parameter Config	
* Ci-		-int @
~ Scenario	Point-to-Point Point-to-Multip	
* Tunnel Name	test1	
Description	Enter Tunnel Description	
* Enabled State	• Enable 🔿 Disable	
* Tunnel Interface	test1 ~	Add Tunnel Interface
* Authentication Mode	Pre-shared Key V	
* Key	•••••	
* Confirm Key		
* Local Address	O Interface ○ IP	
	Ge0/2 ~	
* Local ID Type	FQDN V	
* Local Identity	71.com	
≣ ↑ Advanced		
Reverse Route Injection	D	
Next-Hop Address	Inter Next-Hop Address	
* Priority 5		

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 T	2) Traffic Config	3 Security Parameter Con	fig
🕒 Create	e 🔟 Delete		Enter	r the keyword.	Q
	Proxy Mode	Local Network	Peer Network	Operation	
	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.

- 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).
- 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.

⊘	⊘		3
Basic Config	Interesting Traffic Config	Secu	rity Parameter Config
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	\sim	
* Encapsulation Mode	Tunnel	~	
* Encryption Algorithm	AES-128 🛞	~	
* Verification Algorithm	SHA 🛞	~	
Perfect Forward Secrecy			
* 🕕 SA Lifetime	604800		Second
① Tunnel MTU	1400		
Previous	ancel Finish		

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		
* ① NAT Keep-Alive Interval	20	Second
① Anti-Replay Attack		
Anti-Replay Window	64 ~	
Action Specified by DF Bit	clear v	

- (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 Se	ecurity Policy		
Basic Info			
* Name	VPN-hub-outbound		
Enabled State	• Enable 🔿 Disable		
* Policy Group	Default Policy Group	~	Add Group
* Adjacent Policy	Default Policy	~	Before \lor
Description	Enter the security policy name descrip		
Src. and Dest.			
* Src. Security Zone	any	~	
* Src. Address	any	~	
User/User Group	any	~	
* Dest. Security	VTI	~	
Zone			
* Dest. Address	any	~	
Service			
Service	any	~	

< Back Create Se	curity Policy		
Basic Info			
* Name	VPN-hub-inbound		
Enabled State	• Enable 🔿 Disable		
* Policy Group	Default Policy Group	~	⊕ Add Group
* Adjacent Policy	Default Policy	~	Before \lor
Description	Enter the security policy name descrip		
Src. and Dest.			
* Src. Security Zone	VTI	~	
* Src. Address	any	~	
User/User Group	any	~	
* Dest. Security	any	~	
Zone			
* Dest. Address	any	~	
Service			
Service	any	~	

- 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:
 - o Set Interface Name to out.
 - o Add security zone VTI and set Security Zone to VTI for this interface.
 - o Set **Tunnel Local Address** to the default outbound interface address of Site A: 2.1.0.2.
 - o 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	out	
Security Zone	VTI ~	⊕ Add Security Zone
* Tunnel Local Address	2.1.0.2	
Tunnel Remote Address	• IP 🔿 Dynamic	
	2.1.1.2 🛞	
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 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.
- For Authentication Mode, use the default value Pre-shared Key. Set both Key and Confirm Key to ruijie123.

1	3	
Basic Config Interesti	ng Traffic Config Security Paramete	er
	Config	
* Scenario	Point-to-Point Point-to-Mu	Itipoint ()
* Tunnel Name	to_71	
Description	Enter Tunnel Description	
* Enabled State	• Enable 🔿 Disable	
* Tunnel Interface	out	 ✓ ⊕ Add Tunnel Interface
* Authentication Mode	Pre-shared Key	~
* Кеу	•••••	
* Confirm Key	•••••	
* Local Address	○ Interface ① ● IP ①	
	2.1.0.2	
* Peer Address	2.1.1.2	Ping
* Local ID Type	FQDN	~
* Local Identity	70.com	
Cancel	Next	

After completing the basic configuration, click $\ensuremath{\textit{Next}}.$

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.

	O Basic Config	Interesting 1	2) Traffic Config	Security Parameter Con	ıfig
🕀 Crea	ate 🔟 Delete		Ente	er the keyword.	Q
	Proxy Mode	Local Network	Peer Network	Operation	
	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.

- 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).
- 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

* P	rotocol	ESP			~	
* Encapsulation	n Mode	Tunnel			~	
* Encryption Alg	orithm	AES-128	8		~	
* Verification Alg	orithm	SHA 🛞			~	
Perfect Forward	Secrecy					
* 🕕 SA L	ifetime	604800				Second
Previous	Car	icel	Finis	h		

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		
* ① NAT Keep-Alive Interval	20	Second
 Anti-Replay Attack 		
Anti-Replay Window	64 ~	
Action Specified by DF Bit	clear ~	

- (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 G	iroup
🕀 Create 🔟 De	elete C Refresh			
Name	1	IP Address/Range	Address Group	Descr
test1_remo	te a	200.200.30.0/24	-	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	test1_out			
Enabled State	• Enable 🔿 Disable			
* Policy Group	Default Policy Group ~	Add Group		
Description	by tunnel wizard test1			
Src. and Dest.				
* Src. Security Zone	any \checkmark			
* Src. Address	test1_local ~			
User/User Group	any \checkmark			
* Dest. Security	test1 ~			
Zone				
* Dest. Address	test1_remote ~			
Service				
Service	any \checkmark			

< Back Edit Sec	curity Policy	
Basic Info	,	
* Name	test1_in	
Enabled State	• • Enable 🔿 Disable	
* Policy Group	Default Policy Group ~	Add Group
Description	by tunnel wizard test1	
Src. and Dest.		
* Src. Security Zone	test1 ~	
* Src. Address	test1_remote ~	
User/User Group	any ~	
* Dest. Security	any ~	
Zone		
* Dest. Address	test1_local ~	
Service		
Service	any ~	

- (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 Rou	iting
IP Туре	IPv4
* Dest. IP Range/Mask	200.200.30.0/24
Next-Hop Address	
Interface	out \checkmark
* ① Priority	25
Link Detection	Link Detection ~
Description	by tunnel wizard test1

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 C Refresh C Custom Field									
Tunnel Name	Tunnel Status	Туре	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 C Refresh C Stop C Refresh C Custom Field										
	Tunnel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	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

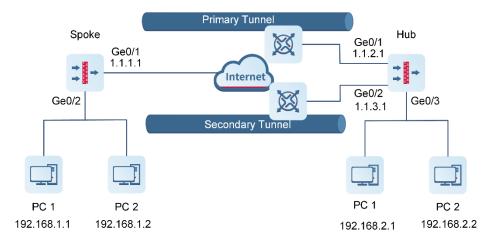
Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R6P2 or later

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
 - 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.

Ruifie Z Series Firewall	습 Home 🛛 Monitor 🕀 Net	work 🔑 Object 💿 Policy	⊕ System	L Quick Onboarding	Ø Policy Wizard	Customer Service	오 admin
Interface ~ Physical Interface	Config Wizard						
Subinterface Bridge Interface		1 Basic Config	Authentication Config Interesting Traffic Config	(4) Config Verification			
Aggregate Interface Tunnel Interface			* 🛈 Tunnel Interface vti 1				
I Zone			* Tunnel Name Primary * Scenario O Point-to-Point O Point-to-Multipoint				
⇒ SSL VPN → IPsec VPN ✓							
Tunnel Monitoring Config Wizard			Main Office				
Custom Tunnel Advanced Settings Details			Branch Office				Consult
© Link Detection							
一 団 Neinhbor Status 厚			Cancel Next				

- c After completing the configuration, click **Next**.
- (2) Configuring Authentication
 - a Configure parameters according to the following figure.

Ruijie Z Series Firewall		Network	유 Object 🖾 Policy	System				L Quick Onboarding	Ø Policy Wizard	Customer Service	ू admin
Interface ~ Physical Interface	Config Wizard										
Subinterface			Ø		·②						
Bridge Interface			Basic Config	Authentie	cation Config	Interesting Traff	fic Config	Config Verification			
Aggregate Interface				* Outbound Interface	Ge0/1						
Tunnel Interface				* Authentication Mode	 Pre-shared Key 						
図 Zone				* Key							
🖶 Routing >				" Ney							
SSL VPN				* Confirm Key							
🔄 IPsec VPN 💦 🗸											
Tunnel Monitoring											
Config Wizard											
Custom Tunnel											Consu
Advanced Settings Details											7
											-
, DHCP →											
link Detection											
H VRRP											
団 Neighbor Status 耳				Previous	Cancel	Next					

- b After completing the configuration, click **Next**.
- (3) Configuring Interesting Traffic
 - a Click Create. Configure parameters for interesting traffic according to the following figure.

Ruffe Z Series Firewall	û Home	Network	A≞ Object	Policy	System					(1 Quick Onboarding	Ø Policy Wizard	Customer Service	Q admin
D Interface Y	Config Wizard													
Physical Interface			-			-					-			
Subinterface			0)		O		3			-4			
Bridge Interface			Basic C	onfig	Auti	hentication Co	ontig	Interesting Tra	affic Config		Verification			
Aggregate Interface				• Create	Delete			Enter th	ne keyword.					
Tunnel Interface														
圆 Zone					Proxy Mode	Local Ne	rtwork	Peer Network	Operation					
🖶 Routing 💦 🔶					Auto	an	У	any	Edit Delete					
⊖ SSL VPN →				10 ~	/ Page Total:1				Go to 1 <	1 >				
IPsec VPN 🛛 🗸														
Tunnel Monitoring														
Config Wizard														2
Custom Tunnel														Consul
Advanced Settings Details														
🗊 DNS >														
📃 DHCP >														
S Link Detection														
田 Neighbor Status 写					Pr	revious	Cancel	Next						

- 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.)

A 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.

Ruijie Z Series Firewall	Home Monitor Pretwork Ar Object Policy System	L Quick Onboarding	Ø Policy Wizard	G Customer Service	Q admin
🖨 Interface 🗸 🗸	Config Wizard				
Physical Interface					
Subinterface	ØØØ				
Bridge Interface	Basic Config Authentication Config Interesting Traffic Config Con	nfig Verification			
Aggregate Interface	() The tunnel configured on the wizard will be added to the custom tunnel list.				×
Tunnel Interface	The turner compared on the wazard will be added to the custom turner list.				
関 Zone	Basic Config Edit				
🖶 Routing >	Tunnel Interface viii 🗸 🗸				
🗑 SSL VPN >	Tunnel Name Primary				
IPsec VPN 🛛 🗸					
Tunnel Monitoring	Scenario 💿 Point-to-Point 🛈 💿 Point-to-Multipoint 🛈				
Config Wizard	Authentication Config Edit				
Custom Tunnel	Outbound Interface Ge0/1				Consu
Advanced Settings Details	Authentication Mode Pre-shared Key				7
🖽 DNS >					-
🔲 рнср 💦	Кеу				

	Advanced Settings	Fold	
Physical Interface	* Local ID Type	IPV4_ADDRESS V	
	Enable Peer Identity Authentication		
	Reverse Route Injection		
	Next-Hop Address	Enter Next-Hop Address	
圆 Zone	* Priority	5	ר
	DPD Type	Regular Mode 🗸 🗸	
	DPD Detection Interval	20	Second
			second
Tunnel Monitoring	DPD Retry Interval	5	Second
Config Wizard	IKE Parameter		
	* Negotiation Mode	IKEv1 Main Mode	
	* Encryption Algorithm	AFS. 128 @	
	* Verification Algorithm	SHA ®	
	* DH Group	GROUP5 ®	
🕅 Neishhor Status 🖉	Previous	Cancel Finish	

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

Ruíjie Z Series Fire	wall		Monitor	Network P= Object				Quick Onboarding	ଡ ନ
	>	Custom	Tunnel						
	>	• Creat	e 🗊 Delete	Senable Disable	C Refresh	istom Field		Tunnel Name 🗸 E	nter a Tunnel Name. Q
	>		Tunnel Nam	e Tunnel Interface	Local Address	Peer Address	Interesting Traffic	Description	Operation
	~		Primary	vti1	Ge0/1	0.0.0.0	0.0.0.0/0-0.0.0.0/0	by tunnel wizard Primary	View Details Edit Copy Delete
Config Wizard									
Custom Tunnel									
Advanced Settings D	etails								

- 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.

Ruijie Z Series Firewall	û Home	Network	윤 Object 🛛 😨 Policy	③ System	L Quick Onboarding	Ø Policy Wizard	Customer Service	Q admin
☐ Interface →	Config Wizard							
図 Zone								
🖶 Routing >			0					
⊜ SSL VPN →			Basic Config	Authentication Config Interesting Traffic Config	Config Verification			
IPsec VPN Y				* ① Tunnel Interface vtl 2				
Tunnel Monitoring				* Tunnel Name Secondary				
Config Wizard				* Scenario O Point-to-Point O Point-to-Multipoint				
Custom Tunnel				Scenario Poneco-Pone				
Advanced Settings Details								
₿ DNS →				Branch Office				
DHCP >				Read Read				-
O Link Detection				Main Office				
H VRRP				Branch Office				onsult
📰 Neighbor Status 🔷 🗧								
æ				Cancel Next				
22								

- c After completing the configuration, click **Next**.
- (2) Configuring Authentication
 - a Configure parameters according to the following figure.

Ruffie Z Series Firewall	ය Home 🛛 Monitor 🖶 I	Network ₽= Object	SPolicy 🕲 System				L Quick Onboarding	Ø Policy Wizard	Customer Service	Q admin
Interface	Config Wizard									
2 Zone										
🖶 Routing >		\bigcirc)	2	3					
SSL VPN		Basic Co	onfig Au	thentication Config	Interesting Traf	fic Config	Config Verification			
🖾 IPsec VPN 🛛 🗸			* Outbound Int	terface Ge0/2						
Tunnel Monitoring			* Authentication	Mode O Pre-shared Key						
Config Wizard										
Custom Tunnel				* Key						
Advanced Settings Details			* Confir	rm Key						
DHCP >										
S Link Detection										
										Consult
🖾 Neighbor Status 🔷 🗧										Ť.
										-
Ē				Previous Cancel	Next					

- b After completing the configuration, click Next.
- (3) Configuring Interesting Traffic
 - a Click Create. Configure parameters for interesting traffic according to the following figure.

Ruijie Z Series Firewall	습 Home 🛛 🛇 Monit	or	,₽ ₌ Object	Policy	System				L Quick Onboarding	Policy Wizard	Customer Service	ې admin
Interface	Config Wizard											
图 Zone												
🖶 Routing >			0)			3					
Image: SSL VPN → SSL V			Basic C	Config	Auti	hentication Config	Interesting Tra	affic Config Confi	g Verification			
IPsec VPN V				• Creat	e 🔟 Delete		Enter th	he keyword. Q				
Tunnel Monitoring												
Config Wizard					Proxy Mode	Local Network	Peer Network	Operation				
Custom Tunnel					Auto	any	any	Edit Delete				
Advanced Settings Details				10 ~	/ Page Total:1			Go to 1 < 1				
🔲 ОНСР >												
link Detection												2
II VRRP												Contu
📰 Neighbor Status 🔷 🗧												Ű
					P	revious Cancel	Next					
Ē						Calleer	SVCAL					

- 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.

Ruffie Z Series Firewall	습 Home 🛛 Monitor	Network	名 Object 図 Policy	System				ĵ
☐ Interface > ☑ Zone	Config Wizard							
la conc la conc Routing →			⊘	⊘		⊘		
			Basic Config	Authentication	Config	Interesting Traffic Con	fig c	0
Tunnel Monitoring	() The tunnel config	gured on the wiza	ard will be added to the	custom tunnel list.				
Config Wizard				Basic Config	Edit			
				Tunnel Interface	vti2			
				Tunnel Name	Secondary			
EE DNS >				Scenario	Point-to-Point	nt 🕕 💿 Point-to-Multij	point ()	
DHCP >				Authentication Config	Edit			
Unic Detection				Outbound Interface				
					Ge0/2			
				Authentication Mode	 Pre-shared K 	ey		
				Key				
Ruijie Z Series Firewall	습 Home 🛛 Monitor	Network	은 Object 💿 Policy	System				
Interface				Interesting Traffic Config	Edit			
國 Zone				Local Network		Peer Networ	k	
🚔 Routing >				any		any		
SSL VPN >				Advanced Settings	Fold			
IPsec VPN V				* Local ID Type		3 ~		
Tunnel Monitoring Config Wizard			E	le Peer Identity Authentication		· · ·		
Custom Tunnel			Enab					
				Reverse Route Injection	_			
				Next-Hop Address	Enter Next-Hop	Address		
				* Priority	10		J	
				DPD Type	Regular Mode			
H VRRP				DPD Detection Interval	10		Second	
				DPD Retry Interval	5		Second	
				IKE Parameter				
				* Negotiation Mode	IKEv1 Main Mod	le v		
					AES-128 ®			
				Previous	Cancel	Finish		

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

Ruijie Z Series Firewall	ය Home 🛛 Monitor	⊕ Network	Policy System	n		Quick Onboarding	Policy Wizard Customer Service admin
Interface	Custom Tunnel						
图 Zone Routing >	🕞 Create 📋 Delete	Senable Disable	C Refresh	stom Field		Tunnel Name v Ent	er a Tunnel Name. Q
	Tunnel Nam	e Tunnel Interface	Local Address	Peer Address	Interesting Traffic	Description	Operation
Tunnel Monitoring	Primary	vti1	Ge0/1	0.0.0.0	0.0.0.0/0-0.0.0.0/0	by tunnel wizard Primary	View Details Edit Copy Delete
Config Wizard	Secondary	vti2	Ge0/2	0.0.0.0	0.0.0.0/0-0.0.0.0/0	by tunnel wizard Second	View Details Edit Copy Delete
Advanced Settings Details							

- 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.

Ruijie Z Series Firewall	🔒 Home 🛛 Monitor 🛛 🤁 Net	rork 윤 Object I Policy	© System	1 Quick Onboarding	Ø Policy Wizard	ମ Customer Service	Q admin
☐ Interface >	Config Wizard						
関 Zone							
tian → Routing		1	23				
SSL VPN		Basic Config	Authentication Config Interesting Traffic Config	Config Verification			
🖾 IPsec VPN 🛛 🗸			* (1) Tunnel Interface vti 1				
Tunnel Monitoring			* Tunnel Name Primary				
Config Wizard			* Scenario O Point-to-Point O Point-to-Multipoint				
Custom Tunnel			 scenario O Point-to-Point O Point-to-Multipoint 				
Advanced Settings Details							
III DNS >			Brack Office				
🗩 DHCP >			Liever Liever				7
Link Detection			Main Office				Consul
E VRRP			Branch Office				÷
📰 Neighbor Status 🔷 🗧							-
			Control				
匝			Cancel Next				

- c After completing the configuration, click **Next**.
- (2) Configuring Authentication
 - a Configure parameters according to the following figure.

Ruijie Z Series Firewall	습 Home 🛛 🛛 Monitor	Network	은 Object 💿 Policy	System				Quick Onboarding	Ø Policy Wizard	Customer Service	ې admin
Interface	Config Wizard										
🗓 Zone											
🖶 Routing >			⊘		-@	3-					
SSL VPN			Basic Config	Authentio	cation Config	Interesting Traf	fic Config	Config Verification			
🖬 IPsec VPN 🛛 🖂				Peer Address	1.1.2.1		Ping				
Tunnel Monitoring				* Outbound Interface	Ge0/1						
Config Wizard											
Custom Tunnel				* Authentication Mode							
Advanced Settings Details				* Key							
📾 DNS 🔷				* Confirm Key							
🔲 DHCP >											(
O Link Detection											Consult
I VRRP											Ę.
🔄 Neighbor Status 🔷 🗧											
Œ				Previou	s Cancel	Next					

- b After completing the configuration, click **Next**.
- (3) Configuring Interesting Traffic
 - a Click Create. Configure parameters for interesting traffic according to the following figure.

Ruíjie Z Series Firew	i	A: Object 🐨 Policy 🞯 System	L Quick Onboarding	Policy Wizard	Customer Service	्र admin
Interface	Config Wizard					
2 Zone						
🖶 Routing		⊘ <u></u> ⊘3_				
SSL VPN		Basic Config Authentication Config Interesting Traffic Config Confi	g Verification			
IPsec VPN		Create Delete Enter the keyword. Q				
Tunnel Monitoring		O Demoklada land Matanak Davi Matanak di K				
Config Wizard		Proxy Mode Local Network Peer Network Operation				
Custom Tunnel		Subnet-to-Subnet 192.168.1.0/24 192.168.2.0/24 Edit Delete				
Advanced Settings Deta	s - 1	10 ∨ / Page Total:1 Go to 1 < 1 >				
III DNS						
🔲 DHCP						۲
S Link Detection						Consult
URRP						Ŧ
🖾 Neighbor Status						_
		Previous Cancel Next				

- b After completing the configuration, click **Next**.
- (4) Verifying Configuration
 - a After verifying the configuration, click **Finish**.

Ruijie Z Series Firewall		⊕ Network					2 Quick Onboarding	Policy Wizard Customer Ser	오 vice admin
Interface									
Ell Interface	Config Wizard								
tool zone			0		O		-(4)		
SSL VPN			: Config	Authentication		ig Config	g Verification		
E IPsec VPN									
IPsec VPN	① The tunnel config	gured on the wizard will be a	added to the custon	n tunnel list.					×
Tunnel Monitoring Config Wizard				Basic Config	200				
Coning Wizard				-					
Advanced Settings Details				Tunnel Interface	viit 🗸				
DNS >				Tunnel Name	Primary				
圖 онся >				Scenario	Point-to-Point O Point-to-Multip	ooint 🕕			
Link Detection				Authentication Config	Edit				
III VRRP				Peer Address					Contul
Neighbor Status									
				Outbound Interface					
				Authentication Mode	 Pre-shared Key 				
				Key					
Ruíjie Z Series Firewall		Object					L Quick Onboarding	O Policy Wizard Oustomer Sen	A A A A A A A A A A A A A A A A A A A A
							and a formula	Customer Sen	
Interface				Local Network	Peer Networ	k			
🗓 Zone				192.168.1.0/24	192.168.2.0/2	4			
Heating >				Advanced Settings					
IPsec VPN 🗸				* Local ID Type	IPV4_ADDRESS V				
Tunnel Monitoring			Enable Pee	r Identity Authentication					1
Config Wizard Custom Tunnel				DPD Type	Regular Mode \sim				
Custom Junnel				DPD Detection Interval	30	Second			
DNS >				DPD Retry Interval	5	Second			
S Link Detection				IKE Parameter					
URRP				* Negotiation Mode	IKEv1 Main Mode V				Consul
Neighbor Status				* Encryption Algorithm	AES-128 🛞 🗸				
				* Verification Algorithm	SHA ®				
				* DH Group	GROUPS ®				
				* 🕕 SA Lifetime	86400	Second			
-				Previous	Cancel Finish				
드									
									_
Ruffe Z Series Firewall		● Network ^A Object					L Quick Onboarding	O Policy Wizard Customer Server	vice admin
☐ Interface >	Custom Tunnel								
2 Zone	castom runner								
⇔ Routing >	🕑 Create 🔟 Delete	e 🕢 Enable 🚫 Disable	e 🖸 Refresh [Custom Field		Tunnel Name		inter a Tunnel Name.	
SSL VPN	Tunnel Nan	ne Tunnel Interface	Local Address	Peer Address	Interesting Traffic	Desc	ription	Operation	
IPsec VPN V									
Tunnel Monitoring	Primary	vti1	Ge0/1	1.1.2.1	192.168.1.0/24-192.168.2.0/24	by tunnel w	izard Primary	View Details Edit (Delete	Сору
Config Wizard									
Custom Tunnel									
Advanced Settings Details									
B DNS >									
Д рнср >									
C Link Detection									
									Consult
🖅 Neighbor Status >									

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 **vti1** 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.

Ruifie Z Series Firewall	ය Home 🛛 🖯 Monitor	Network	A≘ Object 🛛 🖾 Policy	System			(L) Quick Onboarding	Ø Policy Wizard	Customer Service	Q admin
☐ Interface >	IPv4 IPv6									
圆 Zone	• Create 🛅 Delet	e Refresh					vt(
Static Routing	Dest. IP Ra	nge/Mask	Next-Hop Address	Interface	Priority	Link Detection	Description		Operation	
Intelligent Routing	192.16	1.2.0/24		vti1	5		by tunnel wizard Prima	ary	Edit Delete	

- Configuring the Secondary 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.

Ruffe Z Series Firewall	습 Home 🛛 🛛 Monitor	Network	An Object 🛛 Policy	System			Quick Onboarding	Policy Wizard	Customer Service	Q admin
Interface	Config Wizard									
図 Zone										
🛗 Routing 💦 🔶			0		2	3				
⊜ SSL VPN →			Basic Config	Authenti	cation Config	Interesting Traffic Con	fig Config Verification			
🖻 IPsec VPN 🛛 🗸				* () Tunnel Interface	vti 2					
Tunnel Monitoring				* Tunnel Name	Secondary					
Config Wizard										
Custom Tunnel				* Scenario	Point-to-Point	Point-to-Multipoint				
Advanced Settings Details										
B DNS >						- Same				
関 рнср >					anter Internet	Branch Office				
O Link Detection					Main Office	- Stan				Consult
H VRRP						Branch Office				nsult
🖾 Neighbor Status 💦 🗧										
æ					Cancel Nex					

- c After completing the configuration, click Next.
- (2) Configuring Authentication
 - a Configure parameters according to the following figure.

Ruffie Z Series Firewall	G Home G Monitor ⊕ Network	A₂ Object 🖾 Policy	System				Quick Onboarding	Ø Policy Wizard	Customer Service	<u>)</u> admin
Interface	Config Wizard									
🗓 Zone										
⊟ Routing →		Ø		2	3					
SSL VPN		Basic Config	Authentio	ation Config	Interesting Tra	ffic Config	Config Verification			
🖾 IPsec VPN 🛛 🗸			* Peer Address	1.1.3.1		Ping				
Tunnel Monitoring			* Outbound Interface	Ge0/1						
Config Wizard			* Authentication Mode							
Custom Tunnel										
Advanced Settings Details			* Key							
III DNS >			* Confirm Key							
同 DHCP >										
O Link Detection										Consult
I VRRP										aute
😰 Neighbor Status 💦 🗧										-
					-					
歪			Previous	Cancel	Next					

- b After completing the configuration, click **Next**.
- (3) Configuring Interesting Traffic
 - a Click Create. Configure parameters for interesting traffic according to the following figure.

Ruijie Z Series Firewall	ය Home 🛛 Monitor	Network	A₂ Object	Policy	System				L Quick Onboarding	Ø Policy Wizard	Customer Service	오 admin
Interface	Config Wizard											
2 Zone												
🖶 Routing >			\oslash)			3		(4)			
♥ SSL VPN >			Basic Co	onfig	Auther.	ntication Config	Interesting Tra	ffic Config Con	fig Verification			
IPsec VPN 🗸				• Create	e 🔟 Delete		Enter the	e keyword. Q				
Tunnel Monitoring												
Config Wizard					Proxy Mode	Local Network	Peer Network	Operation				
Custom Tunnel					Subnet-to-Subnet	192.168.1.0/24	192.168.2.0/24	Edit Delete				
Advanced Settings Details				10 ~	/ Page Total:1			Go to 1 < 1 >				
🗏 DHCP >												
O Link Detection												Contu
URRP												nut
☑ Neighbor Status >												
ē					Previo	ious Cancel	Next					

- b After completing the configuration, click **Next**.
- (4) Verifying Configuration
 - a After verifying the configuration, click **Finish**.

Ruijie Z Series Firewall	ය Home ම Monitor ව Network ළ Object ල Policy ම System	🔝 🤗 Quick Onboarding Policy V		
Interface >	Config Wizard			
図 Zone				
🖶 Routing 💦 🗧	\odot \odot \odot			
🗐 SSL VPN 💦 🗧 🗧	Basic Config Authentication Config Interesting Traffic Config	Config Verification		
🖬 IPsec VPN 🛛 🗸	① The tunnel configured on the wizard will be added to the custom tunnel list.		×	
Tunnel Monitoring	The talmet configured on the means will be added to the coston talmet mat.			
Config Wizard	Basic Config Edit			
Custom Tunnel	Tunnel Interface vii2			
Advanced Settings Details	Tunnel Name Secondary			
DNS >	Scenario 🤄 Point-to-Point 🕥 💿 Point-to-Multipoint 🤇	0		
DHCP >			6	
O Link Detection	Authentication Config Edit			💽 contu
III VRRP	Peer Address 1.1.3.1			ş.
🖾 Neighbor Status 🔷 🗧	Outbound Interface Geore			-
	Authentication Mode 💿 Pre-shared Key			
	Key			

□ Interface >				
田 Zone	Local Network	Pe	eer Network	c .
Bouting	192.168.1.0/24	19	2.168.2.0/24	ŧ.
	Advanced Settings	Fold		
IPsec VPN Y	* Local ID Type	IPV4_ADDRESS		
Tunnel Monitoring	Enable Peer Identity Authentication			
Config Wizard	DPD Type	Regular Mode		
Custom Tunnel	DPD Detection Interval	30		Second
Advanced Settings Details	DPD Retry Interval	5		Second
ink Detection	IKE Parameter			
VRRP	* Negotiation Mode			
Neighbor Status >	* Encryption Algorithm	AES-128 ®		
	* Verification Algorithm	SHA ®		
	* DH Group	GROUP5 ®		
	* 🕕 SA Lifetime	86400		Second
Œ	Previous	Cancel Finish		

Ruffe Z Series Firewall	⊜ Ho	ome 🤤	Monitor	Object Network	t 🞯 Policy 🛞 Syste	em		Quick Onboarding	Policy Wizard Customer Service adm
	Cu	stom Tu	unnel						
	C	Create	📋 Delete	Senable Disat	le 🔉 Refresh 🕅 C	custom Field		Tunnel Name 🗸 🖉	inter a Tunnel Name. Q
		т	unnel Name	Tunnel Interface	Local Address	Peer Address	Interesting Traffic	Description	Operation
			Primary	vti1	Ge0/1	1.1.2.1	192.168.1.0/24-192.168.2.0/24	by tunnel wizard Primary	View Details Edit Copy Delete
Config Wizard Custom Tunnel	(Secondary	vti2	Ge0/1	1.1.3.1	192.168.1.0/24-192.168.2.0/24	by tunnel wizard Second	View Details Edit Copy Delete
Advanced Settings Details									

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.)

A 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.

Ruijie Z Series Firewall	습 Home	Monitor	Network	ி Object இ Policy	System			Quick Onboarding Po	ြ Customer Service	ې adm
Interface	IPv4	IPv6								
i Zone i Routing ∽	🕤 Crea	te 📋 Delete	C Refresh					vti		
Static Routing		Dest. IP Rar	nge/Mask	Next-Hop Address	Interface	Priority	Link Detection	Description	Operation	
Intelligent Routing		192.168	2.0/24	-	vti1	5	-	by tunnel wizard Primary	Edit Delete	
Egress Load Balancing Address Library Route		192.168	2.0/24		vti2	5	-	by tunnel wizard Second	Edit Delete	

Curre Z Series Firewall	û Home	Network P= Object	S Policy 8	🕄 Systen
☐ Interface >	Back Edit Static Ro	outing		
图 Zone	ІР Туре	Pv4		
Static Routing	* Dest. IP Range/Mask	192.168.2.0/24		
Intelligent Routing	Next-Hop Address	5		
Egress Load Balancing	Interface	vti2		
Address Library Route	* ① Priority	10		
OSPF Routing Table	Link Detection	Link Detection		~
Routing Policy	Description	by tunnel wizard Seco	ondary	
SSL VPN >				h
🖾 IPsec VPN 🛛 🗸				
Tunnel Monitoring				
Config Wizard				
Custom Tunnel				
Advanced Settings Details				
A DHOP				

After the modification, the following static route configuration is displayed.

Ruijie Z Series Firewall	☆ Home	Monitor Monitor	etwork 🔑 Object 🐨 Policy 💿	l System			L Quick Onboarding	Policy Wizard Customer Set	Q rvice admin
Interface	IPv4	IPv6							
👿 Zone 📛 Routing 🛛 🗸	⊕ Creat	te 🛅 Delete 😋	Refresh				vti		
Static Routing		Dest. IP Range/M	lask Next-Hop Address	Interface	Priority	Link Detection	Description	Operation	
Intelligent Routing		192.168.2.0/24	-	vti1	5		by tunnel wizard Primar	y Edit Delet	e
Egress Load Balancing Address Library Route		192.168.2.0/24	-	vti2	10	-	by tunnel wizard Seconda	ary Edit Delet	ie -

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.

o Checking the Tunnel Status of the Hub Site

Ruijie Z Series Firewall	🛆 Home	Monitor	Network	A₂ Object 🛛 Policy	System				▲	ရ Customer Ser	ې rvice adr
☐ Interface >	I Tunnel	Monitoring									
I Zone ⊟ Routing →	🕑 Sta	irt 🚫 Stop	C Refresh	Custom Field					Enter a tunnel nan	10.	
SSL VPN		Tunr	nel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re Op	eration
Tunnel Monitoring		×	Primary		Point-to-Multipoint	0.0.0.0					
Config Wizard			Primary	 Established 	Instance Link	1.1.1.1	192.168.2.0/24->192.168.1.0/24	3076	0		Stop
Custom Tunnel		Sec	ondary		Point-to-Multipoint	0.0.0.0		-			
Advanced Settings Details											
ee dns >											

o Checking the Tunnel Status of the Spoke Site

Ruijie Z Series Firewall	ය Home ා ල Me	onitor	우 Object ⓒ Policy ③	System				Onboarding Policy Wizard	Customer Service	ې adm
Interface	Tunnel Mon	itoring								
👿 Zone	Start S	Stop Refresh	Custom Field							
🛱 Routing >	o our									
		Tunnel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re Operati	ion
Tunnel Monitoring		Primary	 Established 	Point-to-Point	1.1.2.1	192.168.1.0/24->192.168.2.0/24	2525	0	Stop	2
Config Wizard		Secondary	 Not established 	Point-to-Point	1.1.3.1	192.168.1.0/24->192.168.2.0/24	0	0	Star	t
Custom Tunnel										

• 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.

o Checking the Tunnel Status of the Hub Site

Ruffie Z Series Firewall	🛆 Home	G Monitor	Network	A₂ Object 🖾 Policy	System				Diboarding Policy Wizard	G Customer Service	ر adi
	I Tunne	l Monitorin	g								
	0	tart 🚫 Stop	Defresh	Custom Field							
	00	unt Goop	C rencon	Eg ousion rick							
		Tur	nel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re Operat	ion
IPsec VPN 🗸			Primary		Point-to-Multipoint	0.0.0.0					
Tunnel Monitoring			erimary	-	Point-to-Multipoint	0.0.0.0	-	-	-		
Config Wizard		~	Secondary	-	Point-to-Multipoint	0.0.0.0		-	-		
	0		Secondary	 Established 	Instance Link	1.1.1.1	192.168.2.0/24->192.168.1.0/24	3524	0	Stop	p

o Checking the Tunnel Status of the Spoke Site

Ruffe Z Series Firewall	습 Home 🛛 M	lonitor	유 Object 🐨 Policy 😒	System				Onter Onter Onter Onter Onter Onter Onter Onter	Customer Service	오 admin
Interface	Tunnel Mon	itoring								
☑ Zone ⊟ Routing >	⊘ Start	Stop C Refresh	Custom Field					Enter a tunnel nam	e.	
SSL VPN		Tunnel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re Operati	on
IPsec VPN ~		Primary	 Not established 	Point-to-Point	1.1.2.1	192.168.1.0/24->192.168.2.0/24	0	0	Starl	t.
Config Wizard		Secondary	 Established 	Point-to-Point	1.1.3.1	192.168.1.0/24->192.168.2.0/24	3476	0	Stop	
Custom Tunnel										

- Verifying Tunnel Switchback After the Primary Link Recovers
 - o Checking the Tunnel Status of the Hub Site

Ruíjie Z Series Firewall	🛆 Home	Monitor	Network	A≘ Object 🔄 Policy	System				Onboarding Policy Wizard	G Customer Se	ervice admi
	I Tunne	I Monitorin	g								
	⊘ st		Defect	Custom Field							
	() st	art Stop	G Refresh	Ut Custom Field							
		Tun	nel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re	peration
🔚 IPsec VPN 🛛 🗸			Primary		Point-to-Multipoint	0.0.0.0					
Tunnel Monitoring		, v	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
		Se	condary		Point-to-Multipoint	0.0.0.0		-	-		

o Checking the Tunnel Status of the Spoke Site

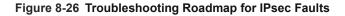
Ruijie Z Series Firew	rall	습 Home	S Monitor	Network	ද Object ල Policy	3 System				Diboarding Policy Wizard	Customer Service	ې adr ء
	>	Tunnel	Monitoring	1								
		0.00		Distant	Custom Field							
	>	Star	rt 🕔 Stop	G Refresh	Custom Field							
	>		Tuni	nel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re Operat	tion
IPsec VPN	~								2525			
Tunnel Monitoring			P	rimary	 Established 	Point-to-Point	1.1.2.1	192.168.1.0/24->192.168.2.0/24	2525	0	Sto	.p
Config Wizard		•	Sei	condary	 Not established 	Point-to-Point	1.1.3.1	192.168.1.0/24->192.168.2.0/24	0	0	Sta	irt

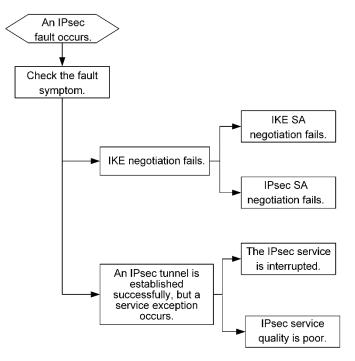
8.25.10 Common Faults and Troubleshooting Roadmaps

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.





1. IKE Negotiation Failure

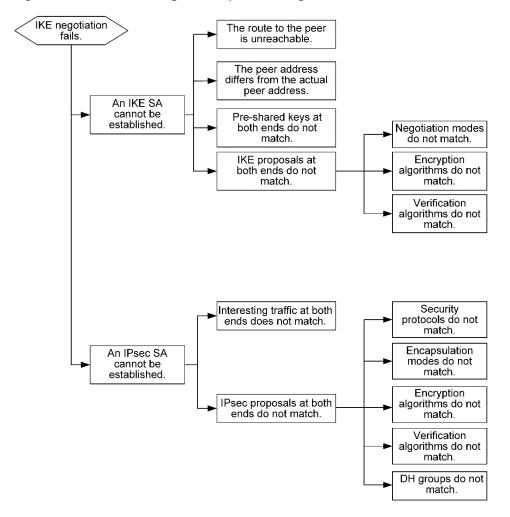


Figure 8-27 Troubleshooting Roadmap for IKE Negotiation Failures

2. IPsec Service Exception

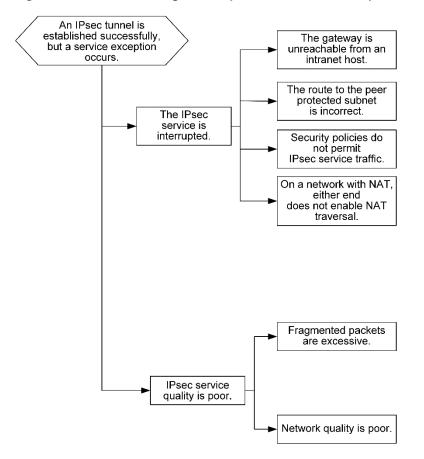


Figure 8-28 Troubleshooting Roadmap for IPsec Service Exceptions

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:

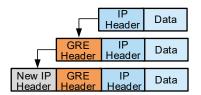
- Load protocol: Packet protocol before encapsulation, that is, the innermost tunnel protocol. IPv4 and IPv6 protocols are generally used as load protocols. For a GRE tunnel, the load protocol can be IPv4, IPv6, or MPLS.
- Carrier protocol: Encapsulation protocol, which is used for secondary encapsulation 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

Transport	Encapsulation/	Passenger
Protocol	Carrier Protocol	Protocol
Delivery Header	GRE Header	Payload Packet

GRE encapsulates packets layer by layer based on the protocol stack. As shown in <u>Figure 8-30</u>, 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
	Cross-region IPv4 communication over IPv4 GRE tunnels
IPv4 over IPv4	Key configurations:
GRE tunnel	• 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.
	Cross-region IPv6 communication over IPv4 GRE tunnels
IPv6 over IPv4	Key configurations:
GRE tunnel	• 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
	Meeting both GRE networking and tunnel security requirements
	Key configurations:
GRE over IPsec	 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 <u>Figure 8-31</u>, 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.

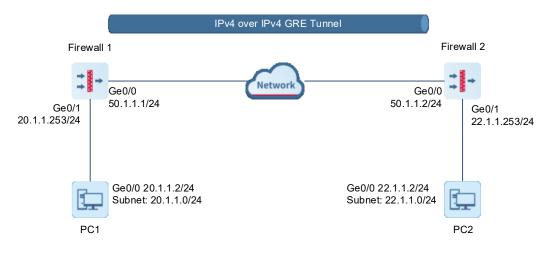


Figure 8-31 Topology of an IPv4 over IPv4 GRE Tunnel

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	greipv4	
Description		
Interface Config		
* Interface Type	GRE V	
* Security Zone	trust ~	
① Tunnel Interface Address	IPv4 IPv6	
IP/Mask		
Tunnel Encapsulation Address		
* 🕕 Src. IPv4	50.1.1.2	
* 🕕 Dest. IPv4	50.1.1.1	
 Advanced Settings 		
 Tunnel Validity Check 		
① Tunnel Key Value	123	
① Keepalive		
① Keepalive Interval	10	S
Retransmission Times Transmission Times	3	
① Tunnel MTU Access Management	1500	
-	🗸 https 🔽 ping 🔽 SSH	
remit		
		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 Туре	IPv4	
* Dest. IP Range/Mask	22.1.1.0/24	
Next-Hop Address		
Interface	greipv4 v	
* ① Priority	5	
Link Detection	Link Detection V	
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		
* ① 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	greipv4		
Enabled State	• Enable 🔿 Disable		
* Policy Group	Default Policy Group \checkmark \odot Add Group		
Description			
Src. and Dest.			
* Src. Security Zone	any \vee		
* Src. Address	greipv4 \lor		
User/User Group	any 🗸		
* Dest. Security	any 🗸		
Zone			
* Dest. Address	greipv4-peer		
Service			
Service	any 🗸		
Арр			
Арр	any 🗸		
Time Range			
Time Range	any \checkmark \odot Add One-Off Time Plan \odot		
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		

- 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 Sec	urity Policy	
Basic Info		
* Name	greipv4-peer	
Enabled State	• Enable O Disable	
* Policy Group	Default Policy Group \lor \odot Add Group	
Description		
Src. and Dest.		
* Src. Security Zone	any 🗸	
* Src. Address	greipv4-peer 🗸	
User/User Group	any 🗸	
* Dest. Security	any 🗸	
Zone * Dest. Address		
	greipv4 V	
Service		
Service	any	
Арр		
Арр	any 🗸	
Time Range		
Time Range	any \checkmark \odot Add One-Off Time Plan \odot .	
Action Settings		
Action Option	Permit O Deny	
Content Security		
Intrusion Prevention	 ○ Enable ● Disable ● Add Intrusion Prevention Template 	
Virus Protection	 ○ Enable ● 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	greipv4	
Description		
Interface Config		
* Interface Type	GRE ~	
* Security Zone	trust ~	
① Tunnel Interface Address	ΙΡν4 ΙΡν6	
IP/Mask		
Tunnel Encapsulation Address		
* () Src. IPv4	50.1.1.2	
* () Dest. IPv4	50.1.1.1	
 Advanced Settings 		
1 Tunnel Validity Check		
1) Tunnel Key Value	123	
① Keepalive		
 Keepalive Interval 	10	s
① Retransmission Times	3	
① Tunnel MTU	1500	
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		
ІР Туре	IPv4	
* Dest. IP Range/Mask	20.1.1.0/24	
Next-Hop Address		
Interface	greipv4 v	
* ① Priority	5	
Link Detection	Link Detection V	
Description		
	là.	

- 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 Addre	ess Object
Basic Info	
* Name	greipv4
Description	
IP Address/Range	
* 🕕 IP Address/Range	22.1.1.0/24
	li.

- $\label{eq:constraint} c \quad \mbox{After completing the configuration, click $ Save. $}$
- d Click Create. On the page that is displayed, add a remote address object.

< Back Edit IPv4 Addre	ess Object
Basic Info	
* Name	greipv4-peer
Description	
	<i>k</i>
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 Sec	urity Policy
Basic Info	
* Name	greipv4
Enabled State	Enable Disable
* Policy Group	Default Policy Group \lor \odot Add Group
Description	
Src. and Dest.	
* Src. Security Zone	any ~
* Src. Address	greipv4 \sim
User/User Group	any ~
* Dest. Security	any ~
Zone	
* Dest. Address	greipv4-peer ~
Service	
Service	any \checkmark
Арр	
Арр	any 🗸
Time Range	
Time Range	any \lor \odot Add One-Off Time Plan \odot Add Cyclic Time Plan
Action Settings	
Action Option	Permit O Deny
Content Security	
Intrusion Prevention	Enable Disable Add Intrusion Prevention Template
Virus Protection	C Enable Disable Add Virus Protection Template
URL Filtering	C Enable O Disable O Add URL Filtering
Keyword Filtering	C Enable O Disable O Add Keyword Filter
Advanced	Settings
	Save

- 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.

K Back Edit Secu	irity Policy
Basic Info	
* Name	greipv4-peer
Enabled State	• Enable O Disable
* Policy Group	Default Policy Group \lor \odot Add Group
Description	
Src. and Dest.	
* Src. Security Zone	any \lor
* Src. Address	greipv4-peer \checkmark
User/User Group	any \checkmark
* Dest. Security	any \lor
Zone	
* Dest. Address	greipv4 ~
Service	
Service	any \checkmark
Арр	
Арр	any \lor
Time Range	
Time Range	any · · · · · · · · · · · · · · · · · · ·
Action Settings	
Action Option	• Permit O Deny
Content Security	
Intrusion Prevention	○ Enable • Disable • Add Intrusion Prevention Template
Virus Protection	○ Enable
URL Filtering	C Enable O Disable O Add URL Filtering
Keyword Filtering	 Enable O Disable O Add Keyword Filter
Advanced	Settings
	Save

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 Int	erface GRE I	nterface ER	SPAN Interface						
🕑 Crea	ate 🗓 Delete 🔇	Refresh							
	Interface Name	Security Zone	Interface Type	Interface Status	Tunnel Interface Address	Tunnel Local Ad dress	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.

VTI In	terface GRE	Interface ER	SPAN Interface						
🕑 Cre	ate 🛅 Delete 🕏	C Refresh							
		c			Tunnel Interface	Tunnel Local Ad	Tunnel Remote		
	Interface Name	Security Zone	Interface Type	Interface Status	Address	dress	Address	Description	Operation
	greipv4	trust	gre	UP	Address	dress 50.1.1.2	Address 50.1.1.1	Description -	Operation 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=0.061 ms
64 bytes from 22.1.1.2: icmp_seq=5 ttl=64 time=0.059 ms
66 bytes from 22.1.1.2: icmp_seq=5 ttl=64 time=0.059 ms
67 bytes from 22.1.1.2: icmp_seq=5 ttl=64 time=0.059 ms
68 bytes from 22.1.1.2: icmp_seq=5 ttl=64 time=0.059 ms
69 bytes from 22.1.1.2: icmp_seq=5 ttl=64 time=0.059 ms
64 bytes from 22.1.1.2: icmp_seq=5 ttl=64 time=0.050 ms
64 bytes from 22.1.1.2: icmp_seq=5 ttl=64 time=0.050 ms
64 bytes from 22.1.1.2: icmp_seq=5 ttl=64 time=0.050 ms
64
```

Checking Interface Traffic Statistics

Choose Monitor > Traffic Monitoring > Interface Traffic > Interface Traffic Details and check detailed interface traffic statistics.

terface 1	Traffic Statistics					
rface Traff	fic Statistics Interface Traffic	c Details				
Export	C Refresh					
	Interface \Rightarrow	Interface Status 👙	Zone 💠	IP 💠	Uplink ‡	Downlink \$
	Ge0/0	m	trust	172.17.123.48/26	510bps	11.91Kbps
	Ge0/1		trust	50.1.1.2/24	1.91Kbps	3.03Kbps
	Ge0/2		trust	60.1.1.2/24	Obps	924bps
	Ge0/3		trust	22.1.1.253/24 3011::1/64	Obps	345bps
	greipsec		trust		Obps	0bps
	greipv4		trust		672bps	672bps
	greipv6	m	trust		Obps	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 <u>Figure 8-32</u>, 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.

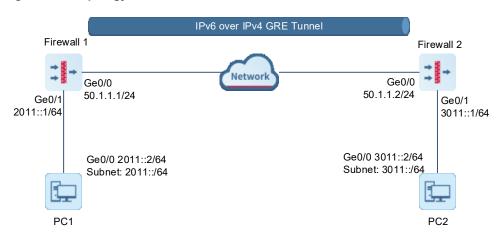


Figure 8-32 Topology of an IPv6 over IPv4 GRE Tunnel

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.

< Back Edit GRE Interface		
Basic Info		
* Interface Name	greipv6	
Description		
Interface Config		
* Interface Type	GRE ~	
* Security Zone	trust ~	€ Add Security Zone
 Tunnel Interface Address 	IPv4 IPv6	
 IPv6 Protocol 	Z Enable	
① IP/Mask		
Tunnel Encapsulation Address		
* ① Src. IPv4	50.1.1.1	
* ① Dest. IPv4	50.1.1.2	
▲ Advanced Settings		
① Tunnel Validity Check		
1 Tunnel Key Value	124	
① Keepalive		
() Keepalive Interval	10	S
① Retransmission Times	3	
① Tunnel MTU	1500	
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 > IPv6.
 - b Click **Create.** On the page that is displayed, add a static route.

< Back Edit Static Rou	iting
ІР Туре	IPv6
* Dest. IP Range/Mask	3011::/64
Next-Hop Address	
Interface	greipv6 v
* ① 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 Addre	ess 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 Addre	ess 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 Sect	urity Policy	
Basic Info		
* Name	greipv6	
Enabled State	• Enable 🔿 Disable	
* Policy Group	Default Policy Group ~	⊙ Add Group
Description		
Src. and Dest.		
* Src. Security Zone	any ~	
* Src. Address	greipv6 ~	
User/User Group	any \checkmark	
* Dest. Security	any ~	
Zone * Dest. Address	grainut poor	
	greipv6-peer V	
Service		
Service	any \vee	
Арр		
Арр	any ~	
Time Range		
Time Range	any \lor	
Action Settings		
Action Option	• Permit 🔿 Deny	
Content Security		
Intrusion Prevention	○ Enable	ion Prevention Template
Virus Protection	○ Enable	Protection Template
URL Filtering		ltering
Keyword Filtering	○ Enable Disable Add Keyword	ord Filter
Advanced	Settings	
		Save

- 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 Sec	urity Policy	
Basic Info		
* Name	greipv6-peer	
Enabled State	• Enable 🔿 Disable	
* Policy Group	Default Policy Group V	
Description		
Src. and Dest.		
* Src. Security Zone	any \vee	
* Src. Address	greipv6-peer V	
User/User Group	any \lor	
* Dest. Security	any \vee	
Zone		
* Dest. Address	greipv6 ~	
Service		
Service	any \lor	
Арр		
Арр	any \vee	
Time Range		
Time Range	any \vee	
Action Settings		
Action Option	• Permit 🔿 Deny	
Content Security		
Intrusion Prevention	○ Enable • Disable • Add Intrus	ion Prevention Template
Virus Protection	○ Enable ● Disable ● Add Virus	Protection Template
URL Filtering	○ Enable	iltering
Keyword Filtering	○ Enable • Disable • Add Keywo	ord 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.

Back Edit GRE Interface			
Basic Info			
* Interface Name	greipv6		
Description			
Interface Config			
* Interface Type	GRE V		
* Security Zone	trust ~		
① Tunnel Interface Address	IPv4 IPv6		
IPv6 Protocol	Z Enable		
① IP/Mask			
Tunnel Encapsulation Address			
* () Src. IPv4	50.1.1.2		
* 🕕 Dest. IPv4	50.1.1.1		
▲ Advanced Settings			
1) Tunnel Validity Check			
Tunnel Key Value	124		
() Keepalive			
() Keepalive Interval	10	s	
① Retransmission Times	3		
① Tunnel MTU	1500		
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 > IPv6.
- b Click **Create.** On the page that is displayed, add a static route.

< Back Edit Static Rou	uting
IP Туре	IPv6
* Dest. IP Range/Mask	2011::/64
Next-Hop Address	
Interface	greipv6 v
* ① Priority	5
Description	
	h.

- 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 Addre	Back 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 Addr	ess 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.

Basic Info * Name Enabled State	greipv6	
Enabled State		
	• Enable 🔿 Disable	
* Policy Group		Add Group
Description		
Src. and Dest.		
* Src. Security Zone	any \checkmark	
* Src. Address	greipv6	
User/User Group		
	any ~	
* Dest. Security Zone	any 🗸	
* Dest. Address	greipv6-peer 🗸	
Service		
Service	any 🗸	
Арр		
Арр	any \checkmark	
	uny	
Time Range	anv	
	any 🗸 🕤	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 Prov	tection Template
URL Filtering	○ Enable	ing
Keyword Filtering	○ Enable O Disable O Add Keyword	Filter
Advanced	Settings	

- 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 Sec	urity Policy
Basic Info	
* Name	greipv6-peer
Enabled State	Enable Disable
* Policy Group	Default Policy Group 🗸 💿 Add Group
Description	
Src. and Dest.	
* Src. Security Zone	any \checkmark
* Src. Address	greipv6-peer 🗸
User/User Group	any ~
* Dest. Security	any
Zone	
* Dest. Address	greipv6 \lor
Service	
Service	any
Арр	
Арр	any
Time Range	
Time Range	any \checkmark \odot Add One-Off Time Plan \odot Add Cyclic
Action Settings	
Action Option	Permit O Deny
Content Security	
Intrusion Prevention	Enable Disable Add Intrusion Prevention Template
Virus Protection	
URL Filtering	
Keyword Filtering	
Advanced	Settings
Auvaliced	seconds
	Save

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 Int	erface GRE I	nterface ER	SPAN Interface						
Create Delete C Refresh Enter a name.									
	Interface Name	Security Zone	Interface Type	Interface Status	Tunnel Interface Address	Tunnel Local Ad dress	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.

Product Cookbook

VTI Int	erface GRE In	nterface ER	SPAN Interface						
🕑 Crea	te 🔟 Delete 🕄	Refresh							
	Interface Name	Security Zone	Interface Type	Interface Status	Tunnel Interface Address	Tunnel Local Ad dress	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	
64 bytes from 3011::2: icmp_seq=2 ttl=64 time=0.123	
64 bytes from 3011::2: icmp_seq=3 ttl=64 time=0.094	
64 bytes from 3011::2: icmp_seq=4 ttl=64 time=0.094	
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 Traffic Statistics									
Interface Traffic Statistics Interface Traffic Details									
2 Export C Refresh									
	Interface \Leftrightarrow	Interface Status 💠	Zone 😄	IP \$	Uplink ¢	Downlink ¢			
	Ge0/0			172.17.123.12/24	10.81Kbps	33.10Kbps			
	Ge0/1		untrust	50.1.1.1/24	1.36Kbps	1.66Kbps			
	Ge0/2	m	trust	60.1.1.1/24	Obps	345bps			
	Ge0/3	m	trust	20.1.1.253/24 2011::1/64	Obps	924bps			
	erspan1		trust		Obps	0bps			
	greipsec		trust		Obps	0bps			
	greipv4		trust		Obps	Obps			
	greipv6		trust		672bps	672bps			

8.26.6 Configuring GRE over IPsec

1. Applicable Products and Versions

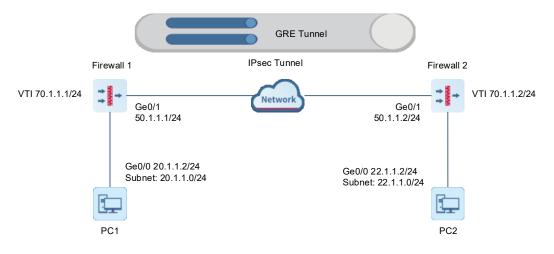
Table 8-36Products and Versions

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. <u>Figure 8-</u> <u>33</u> 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.
 - a Choose Network > Interface > Tunnel Interface > VTI Interface.
 - b Click Create. On the VTI configuration page, configure the following parameters:
 - o Set the interface name to vti1.
 - o Set the IP address to 70.1.1.1/24.

Back Edit VTI Interfa	ace	
Basic Info		
* Interface Name	vti1	
* Enabled State	• Enable 🔿 Disable	
Security Zone	trust ~	€ Add Security Zone
Description		
Address		
IP	70.1.1.1/24	
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:

- Set the tunnel name to **ipsec-gre**.
- o Set Enabled State to Enable.
- Associate with the tunnel interface vti1. Set the local address to interface Ge0/1 and set the remote address to 50.1.1.2.
- For the authentication mode, use the default value **Pre-shared Key**. Enter the key **test123** and then enter it again for confirmation.

(1)	
Basic Config	nteresting Traffic Config Security Parameter Confi
* Scenario	Point-to-Point Point-to-Multipoint
* Tunnel Name	ipsec-gre
Description	
* Enabled State	• Enable O Disable
* Tunnel Interface	vti1 ~
* Local Address	Add Tunnel Interface Interface O IP O Ge0/1 V
* Peer Address	50.1.1.2 Ping
* Authentication Mode	Pre-shared Key V
* () Key	•••••
* () Confirm Key	•••••
* Local ID Type	IPV4_ADDRESS ~
Peer ID Authentication	
⊒ ↓ Advanced	
Car	Next

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:

- 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

		⊘ Basic Config	2 Interesting Traffic Config	3 Security Parameter Config	
🕑 Create 📋 D	Delete				
	Proxy Mode		Local Network	Peer Network	Operation
	Host-to-Host		70.1.1.1	70.1.1.2	Edit Delete
10 V / Page	Total:1				Go to 1 🔨 1

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.

- 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.

Ø			3
Basic Config	Interesting Traffic Config	Security	Parameter Config
≣ ↑ IKE Paramete	r		
* ① IKE Versio	n 🔽 IKEv1 🔽 IKEv2		
* (i) Negotiation Mod	e IKEv1 Main Mode	\sim	
* Pseudo-Random Algorithr	m SHA-256 🛞		
* Encryption Algorithr	M AES-128 🖲		
* (i) Verification Algorithm	n Sha 🗷		
* DH Grou	GROUP5 ®		
* 🛈 SA Lifetim	e 86400		Second
≣ ↑ IPsec Paramete	r		
* Protoco	ESP ESP		
* Encapsulation Mod	e Tunnel		
* Encryption Algorithr	M AES-128 🛞		
* Verification Algorithm	n SHA ®		
Perfect Forward Secred	у		
* 🕕 SA Lifetim	e 3600		Second
Tunnel MT	U 1400		
Previous	Cancel Finish		

Click Finish to create the IPsec tunnel.

- Configuring Firewall 2
- (1) Configure a VTI.
 - a Choose Network > Interface > Tunnel Interface > VTI Interface.
 - b 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 Interfa		
Basic Info		
* Interface Name vti1		
* Enabled State 🥑 Enable 🔷 Disable		
Security Zone	trust \lor	€ Add Security Zone
Description		
Address		
IP	IP 70.1.1.2/24	
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:

- Set the tunnel name to **ipsec-gre**.
- o Set Enabled State to Enable.
- Associate with the tunnel interface **vti1**. Set the local address to interface Ge0/1 and set the remote address to 50.1.1.1.
- For the authentication mode, use the default value **Pre-shared Key**. Enter the key **test123** and then enter it again for confirmation.

0	2	3
Basic Config Ir	nteresting Traffic Config Security	Parameter Conf
* Scenario	Point-to-Point () Point-to-Multip	oint 🕕
* Tunnel Name	ipsec-gre	
Description		
* Enabled State	• Enable 🔿 Disable	
* Tunnel Interface	vti1 ~	
	Add Tunnel Interface	
* Local Address	Interface IP	
	Ge0/1 ~	
* Peer Address	50.1.1.1	Ping
* Authentication Mode	Pre-shared Key \sim	
* () Key	•••••	
* 🛈 Confirm Key	•••••	
* Local ID Type	IPV4_ADDRESS ~	
 Peer ID Authentication 		
≣ ↓ Advanced		
Can	Next	

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

		Ø	2	3		
		Basic Config	Interesting Traffic Config	Security Parameter Config		
🕑 Create 🔲 Del	lete					
	Proxy Mode		Local Network	Peer Network	Operatio	n
	Host-to-Host		70.1.1.2	70.1.1.1	Edit Dele	ete
10 V / Page To	otal:1				Go to 1 <	1

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.

 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. 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.

Ø	Ø	3
Basic Config	Interesting Traffic Config	Security Parameter Config
≣ ↑ IKE Paramet	er	
* () IKE Versi	on 🗹 IKEv1 🔽 IKEv2	
* ① Negotiation Mo	de IKEv1 Main Mode	~
* Pseudo-Random Algorith	SHA-256 💌	\sim
* Encryption Algorith	AES-128 🖲	~
* ① Verification Algorith	SHA 💌	~
* DH Gro	GROUP5 🛞	~
* (i) SA Lifetir	ne 86400	Second
≣r IPsec Paramet	er	
* Protoc	col ESP	~
* Encapsulation Mo	de Tunnel	~
* Encryption Algorith	AES-128 🛞	~
* Verification Algorith	SHA 🛞	~
Perfect Forward Secre	cy	
* 🕕 SA Lifetin	ne 3600	Second
① Tunnel M [*]	TU 1400	
Previous	Cancel Finish	

Click **Finish** to create the IPsec tunnel.

6. Configuring GRE

- 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.

🛕 Caution

The MTU of the GRE tunnel must be the same as that configured for IPsec.

< Back Edit GRE Interface		
Basic Info		
* Interface Name	greipsec	
Description		
Interface Config		
* Interface Type		
* Security Zone	trust ~	
① Tunnel Interface Address	IPv4 IPv6	
① IP/Mask		
Tunnel Encapsulation Address		
* () Src. IPv4	70.1.1.1	
* 🕦 Dest. IPv4	70.1.1.2	
▲ Advanced Settings		
① Tunnel Validity Check		
 Tunnel Key Value 	123	
① Keepalive		
① Keepalive Interval	10	s
 Retransmission Times 	3	
① Tunnel MTU	1400	
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 Edit Static Routing		
ІР Туре	IPv4	
* Dest. IP Range/Mask	22.1.1.0/24	
Next-Hop Address		
Interface	greipsec v	
* () Priority	5	
Link Detection	Link Detection \checkmark	
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 Addre	Back Edit IPv4 Address Object		
Basic Info			
* Name	greipv4		
Description			
IP Address/Range			
* 🕕 IP Address/Range	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.

< Back	Edit IPv4 Addro	ess Object
	Basic Info	
	* Name	greipv4-peer
	Description	
	IP Address/Range	
* (IP Address/Range	22.1.1.0/24
* (-	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.

K Back Edit Secu	urity Policy
Basic Info	
* Name	greipv4
Enabled State	• Enable O Disable
* Policy Group	Default Policy Group V O Add Group
Description	
Src. and Dest.	
* Src. Security Zone	any \sim
* Src. Address	greipv4 ~
User/User Group	any \checkmark
* Dest. Security	any \checkmark
Zone	
* Dest. Address	greipv4-peer V
Service	
Service	any \vee
Арр	
Арр	any \lor
Time Range	
Time Range	any \lor \odot Add One-Off Time Plan \odot Add Cyclic Time f
Action Settings	
Action Option	• Permit O Deny
Content Security	
Intrusion Prevention	○ Enable O Disable O 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

- 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 Secu	rity Policy
Basic Info	
* Name	greipv4-peer
Enabled State	• Enable 🔿 Disable
* Policy Group	Default Policy Group \lor \odot Add Group
Description	
Src. and Dest.	
* Src. Security Zone	any \vee
* Src. Address	greipv4-peer \lor
User/User Group	any \checkmark
* Dest. Security Zone	any \lor
* Dest. Address	greipv4 ~
	greipv4
Service Service	
	any 🗸
Арр	
Арр	any 🗸
Time Range	
Time Range	any v S Add One-Off Time Plan S Add Cyclic T
Action Settings	
Action Option	• Permit O Deny
Content Security	
Intrusion Prevention	Enable O Disable O Add Intrusion Prevention Template
Virus Protection	Enable Disable O Add Virus Protection Template
URL Filtering	C Enable Disable Add URL Filtering
Keyword Filtering	C 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.

A Caution

The MTU of the GRE tunnel must be the same as that configured for IPsec.

Basic Info		
* Interface Name	greipsec	
Description		
Interface Config		
* Interface Type	GRE ~	
* Security Zone	trust \lor	
① Tunnel Interface Address	ΙΡν4 ΙΡν6	
① IP/Mask		
Tunnel Encapsulation Address		
* () Src. IPv4	70.1.1.2	
* 🕕 Dest. IPv4	70.1.1.1	
▲ Advanced Settings		
 Tunnel Validity Check 		
 Tunnel Key Value 	123	
① Keepalive		
() Keepalive Interval	10	s
Retransmission Times	3	
 Tunnel MTU 	1400	
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	ack Edit Static Routing							
	ІР Туре	IPv4						
*[Dest. IP Range/Mask	20.1.1.0/24						
	Next-Hop Address							
	Interface	greipsec	\sim					
	* 🕕 Priority	5						
	Link Detection		\sim					
	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 Addr	ess Object
Basic Info	
* Name	greipv4
Description	
IP Address/Range	A
* () 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 Addr	ess 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.

Basic Info	
* Name	greipv4
Enabled State	• Enable 🔿 Disable
* Policy Group	Default Policy Group \lor \odot Add Group
Description	
Src. and Dest.	
* Src. Security Zone	any ~
* Src. Address	greipv4 \checkmark
User/User Group	any
* Dest. Security	any
Zone	
* Dest. Address	greipv4-peer 🗸
Service	
Service	any 🗸
Арр	
Арр	any \checkmark
Time Range	
Time Range	any \checkmark \odot Add One-Off Time Plan \odot Add Cyclic
Action Settings	
Action Option	• Permit 🔾 Deny
Content Security	
ntrusion Prevention	○ Enable • Disable • Add Intrusion Prevention Template
Virus Protection	○ Enable O Disable O Add Virus Protection Template
URL Filtering	○ Enable O Disable O Add URL Filtering
Keyword Filtering	○ Enable • Disable • Add Keyword Filter
Advanced	Settings

- 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 Secu	rity Policy	
Basic Info		
* Name	greipv4-peer	
Enabled State	• Enable 🔿 Disable	
* Policy Group	Default Policy Group \lor	
Description		
Src. and Dest.		
* Src. Security Zone	any \checkmark	
* Src. Address	greipv4-peer V	
User/User Group	any \lor	
* Dest. Security	any \lor	
Zone		
* Dest. Address	greipv4 V	
Service		
Service	any \lor	
Арр		
Арр	any \vee	
Time Range		
Time Range	any \lor	
Action Settings		
Action Option	• Permit 🔿 Deny	
Content Security		
Intrusion Prevention	Enable O Disable 🟵 Add Intrus	ion Prevention Template
Virus Protection	Enable O Disable O Add Virus	Protection Template
URL Filtering	🔿 Enable 💿 Disable 🟵 Add URL F	iltering
Keyword Filtering	⊖ Enable 💿 Disable ⊙ Add Keyw	ord Filter

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 Int	terface GRE	Interface ER	SPAN Interface						
📀 Crea	ate 🛅 Delete	C Refresh							
	Interface Name	Security Zone	Interface Type	Interface Status	Tunnel Interface Address	Tunnel Local Ad dress	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.

/TI Int	erface GRE I	nterface ER	SPAN Interface						
🕑 Crea	te 🗓 Delete 🔇	Refresh							
	Interface Name	Security Zone	Interface Type	Interface Status	Tunnel Interface Address	Tunnel Local Ad dress	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 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=0.061 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.

terface 1	Traffic Statistics					
erface Traf	fic Statistics Interface	Traffic Details				
Export	C Refresh					
	Interface ≑	Interface Status 🗘	Zone 🗘	IP ‡	Uplink 🗘	Downlink 🗘
	Ge0/0	m	trust	172.17.123.48/26	25.90Kbps	18.36Kbps
	Ge0/1		trust	50.1.1.2/24	1.86Kbps	2.44Kbps
	Ge0/2		trust	60.1.1.2/24	Obps	230bps
	Ge0/3		trust	22.1.1.253/24 3011::1/64	0bps	230bps
	greipsec	m	trust		672bps	672bps
	greipv4	m	trust		0bps	0bps
	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.

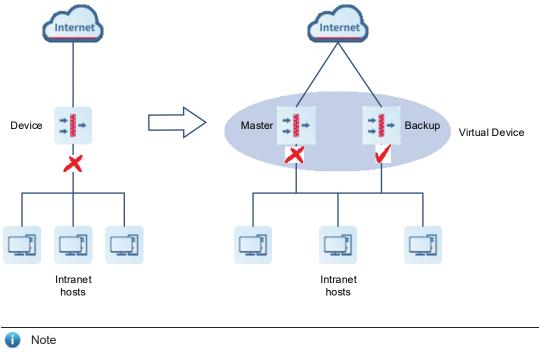
8.27 VRRP

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.



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.

RRP VRRP Log					
VRRP Group Name VRRP Priority	Role	Deployment Interface	Interface IP	Virtual IP	Operating Status
			No Data		

(3) Configure the parameters of the VRRP group.

< Back Add VRRP Gro	ир	
Basic Info		
* VRRP Group Name	Enter the VRRP group name. Range	
① Priority	100	
* () Deployment Interface	Select a deployment interface. \sim	
* 🕕 Virtual IP	Enter a virtual IP address.	
 Monitoring Interface 	Select a monitoring interface. \checkmark	
≣ ↑ Advanced		
 Preemption Delay 	1	Second
 Advertisement Interval 	1	Second
Authentication		
1 Plain Text Authentication		

Save

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
AdvertisementInterval in seconds at which the master device sendsAdvertisementVRRP messages. All devices within the same VRRPIntervalgroup must be configured with the same advertisementinterval.		[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.

VRRP VRRP Log	
C Refresh	Time 2023-05-25 to 2023-05-25 Enter the keyword.
Time	Details
	No Data

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.

The firewall provides a built-in portal service. After obtaining the user's username password, the portal service authenticates the user's identity information. After pathe authentication, the user can access specific resources or perform specific operations.	
Local portal authentication Configuration notes: Set Local Portal Authentication to Enabled. Set the authentication template name to Local Portal in authentication polic configuration. Toggle on WEBAUTH in authentication domain configuration. Configure User Location in authentication domain configuration. To authenticate user information using a firewall, configure Only Lo Info or Prefer Local Info. To authenticate user information using an external RADIUS server, configure Only Info on Server or Prefer Info on Server.	cy

Scenario	Description			
External portal authentication	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.			
	 Configuration notes: 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. Note: An RG-WALL 1600-Z series firewall cannot act as an external RADIUS server. 			
Real-name user information synchronization	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. PC/Access Berver Firewall Berver Berver Content Berver			
	 Configuration notes: 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

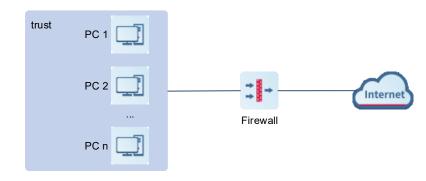
Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS1.0R6 or later

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**.

User Management						
Default Authentication Domain $\ \lor$						
User Structure =	User Group Membe	rs				
⊕ Create User Group	Add 🗸 🛅 Delet	e 🛛 Enable 🚫 Disable	S Refresh More 🗸			Enter a name. Q
All Groups	User lame	Group	Account Expiry Date	Source	Description	Operation
			No E	Data		

- c Configure user information for Internet access.
- o Login Username: test
- o Parent Group: *Idefault*. In this example, the predefined default user group is selected. In actual configuration, you can select a custom user group as required.
- o Password: test@123

< Back Add User		
Basic Info		
* Login Username	test	
Enabled State	• Enable 🔿 Disable	
Displayed Username	Enter the displayed username.	
* Parent Group	/default ~	
Description	Enter user description.	
Password		
* ① Password	•••••	
* Confirm Password	••••••	
E 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	default		
	Enabled State	• Enable 🔿 Disable		
	Description	Enter authentication domain description.		
	* Scenario			
	SSL VPN Access	• •		
	User Location	Only Local Info V		
	WEBAUTH	• •		
	User Location	Only Local Info V		
🗐 Advan	ced 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.
 - 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.

Product Cookbook

Local Portal	Custom Portal	Real-Name User Info Reception	Allowlist
Local Portal A	Authentication 🔵		
() Authe	entication Port 8081		
Redirection upon A	Authentication 💿 No I	Redirection	
	Red	rect to Previous Web Page	
	Redi	rect 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	on Policy
* Name	test
Enabled State	• Enable 🔿 Disable
Description	test_policy
* Src. Security Zone	trust \lor
* Src. Address	any
Authentication Action	• Authentication O Authentication-free
* Authentication Template Name	Local Portal v

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.

	//		English 🗸
Dear user, Welcome to the Web Authentication System	Usersame*	Login	
	Passord * ©		

(3) Upon successful login, the authentication success page is still displayed.

1 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.

		English 🗸
Dear user,	•	
Welcome to the Web Authentication System	Login succeeded. You have logged in successfully and can now access the Internet.	
	Username test IP 192.168.1201	
	Online Duration 00:03:39	
	Change Password Log Out	

(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 8-38Products and Versions

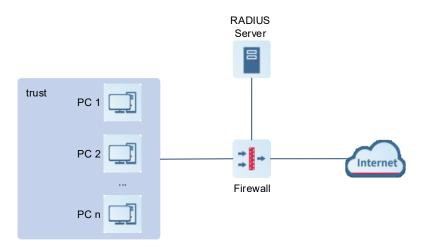
Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS1.0R6 or later

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	test_radius
* Shared Password	••••••
Active Authentication Server IP	
* IP	192.168.50.1
 Authentication Port 	1812
① Accounting Port	1813
Tx Interface	Select an interface.
Standby Authentication Server IP	
IP	Enter an IP address.
 Authentication Port 	Enter the port number.
① Accounting Port	Enter the port number.
Tx Interface	Select an interface.
≣ ↑ Advanced Settings	
Retransmission Times	3 ~
Unit	Byte 🗸
Response Timeout	5 ~
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.

Basic Info			
basic into			
* Name	default		
Enabled State	• Enable 🔿 Disable		
Description	Enter authentication domain description.		
* Scenario			
SSL VPN Access	• •		
User Location	Only Local Info	~	
WEBAUTH	•		
User Location	Only Info on Server	\sim	
Authentication Server	test radius	~	Add RADIUS Server

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.
- 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.

Product Cookbook

Portal Authentication							③ Create
Portal Authentication Template 1							Delete
Basic Info							
* Portal Authentication Template 1 Name	portal1						
* ① Portal Server URL	http://10.51.210.97/sn	p/commonauth					
URL Config Result	http://10.51.210.97/smp	/commonauth					
① NAS Configuration	🔿 Default 🛛 ip	 Interface 					
ET Custom URL Parameters							
User IP Field	Field Name	Enter the field name.	Encryption Mode	Select an encryption mode. \sim			
MAC Field	Field Name	Enter the field name.	Encryption Mode	Select an encryption mode. \sim			
	Address Forma	XX-XX-XX-XX-XX-XX					
NAS-IP Field	Field Name	Enter the field name.	Encryption Mode	Select an encryption mode. \sim			
URL Field	Field Name	Enter the field name.	Encryption Mode	Select an encryption mode. \sim			
Hostname Field	Field Name	Enter the field name.	Encryption Mode	Select an encryption mode. \sim			
Custom Parameter1	Parameter Name	Enter a parameter name.	Parameter Value Enter a	value. Encryp	tion Mode	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.)
- 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.
- 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.
- Escape: If this function is enabled, user Internet access is not affected when the server goes Down. This function is disabled in this example.
- 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	10.51.210.97	Port	50100	
* (1) Shared Key	•••••			
① Sending Source	• Default O Interface			
MAB				
ET Advanced Settings				
Server Detection				
Server Detection Protocol Type	icmp ~]		
 Detection Interval 	30			
① Detection Retries	3			
Escape	If the portal server goes down after t requests.	nis fun	ction is enabled, sp	pecific network access permissions can be granted to users to support basic network access
Listening Port				
① Listening Port	2000			

- 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.
 - Authentication Action: Authentication
 - o Authentication Template Name: Select the external portal authentication template name **portal1** configured in the previous section.

< 返回 Edit Authentication	n Policy	
* Name	test	
Enabled State	• Enable 🔿 Disable	
Description	test_policy	
* Src. Security Zone	trust \vee	
* Src. Address	any \checkmark	
Authentication Action	• Authentication O Authentication-fr	ree
* Authentication Template Name	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.

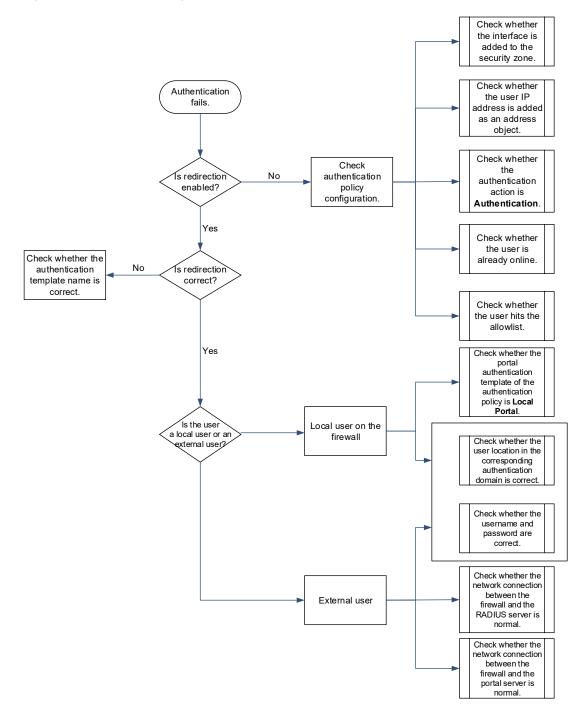


Figure 8-36 Troubleshooting Roadmap of Web Authentication

- 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 unter the overload protection function.

Overl	oad Protection
c	f data CPU usage or system memory usage is too high, you can enable system overload protection. After this function is enabled, the default action is Permit, and the system will not perform security detection on received packets.
l I	f the action is set to Block, the system denies traffic that fails security detection.
	Overload Protection
	Save

(3) Configure the action to be taken on traffic when overload is detected.

Overload Protection	
 If data CPU usage or system memory usage is too high, yo detection on received packets. If the action is set to Block, the system denies traffic that factors 	
Overload Protection	
Action on Traffic for System O Permit O Block Overload	
Save	

(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.

- A 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.

o F	Push		
9 Pu	ish 💽		
0	onfig Info Settings	Il to Defaults	Info Push Type All
	Name	Description	Operation

(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.

< Back Config Info Settings		
 O Create ☑ Delete ☑ Refresh 		
Name	Image	Operation
default_image_red.png	۲	Edit
default_image_blue.png	۹	Edit
default_image_white.png		Edit

(4) Click Create.

Back Config Info Settings		
⊖ Create Delete Create		
Name	Image	Operation
default image red.png	•	Edit
0 _ 1 0		
default_image_blue.png	۹	Edit

(5) Add a logo image. The image format must be PNG or JPEG, and the image size cannot exceed 32 KB.

Add Config	g Info		\otimes
* Name	Enter the name.		
① Image		+	
	Confirm	Cancel	

(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 I	Push		
Info Pu	ısh 💽		
1 c	onfig Info Settings	faults Refresh	Info Push Type All
	Name	Description	Operation
	URL-based Blocking Page	Updated HTML for the URL-based blocking page	Edit
	Antivirus-based Blocking Page	Updated HTML for the antivirus-based blocking page	Edit

(3) Click Edit in the Operation column.

Info	Push		
Info P	ush 🗾		
1	onfig Info Settings	ults C Refresh	Info Push Type All v
	Name	Description	Operation
	URL-based Blocking Page	Updated HTML for the URL-based blocking page	Edit
	Antivirus-based Blocking Page	Updated HTML for the antivirus-based blocking page	Edit

(4) Configure the push text.

	view
	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	proper reason to access this specific website, please contact your network administrator for help.
Edit Info Push * Title	proper reason to access this specific website, please contact your network administrator for help.

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 C	onfigure l	Info Push for URL-based Blocking Page
Inf	fo Push Pre	view
		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
Ed	lit Info Push	1
	* Title	Web Access blocked
* [Description	According to the network control policy, you have no privilege to visit this web page. If you have proper reason to access this specific web: administrator for help.
		Restore Defaults Cancel Save

Follow-up Procedure

- Select push pages and click **Export** to export the push page information to the local device.
- Click **Restore All to Defaults** to restore the default configurations on a page, including the logo and text.
- Click **Refresh** to obtain the latest push information.
- Select **Common**, **All**, or **Revised** from the **Info Push Type** drop-down list to view information on corresponding traffic blocking pages.

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

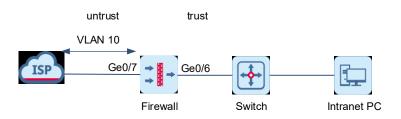


Table 8-40 Configuration Description

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 subinterface 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.

Ruije Z Series Firewall	습 Home	€ Network	ତ Policy	@ System
🕒 Interface 🗸 🗸	1 Subinterface			
Physical Interface				
Subinterface 2	⊕ Create	Enable Disable	C Refresh	
	Interface Name	Description	Zone	Link Type
				No Data
Tunnel Interface				No Data

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**.

< Back Add Subinterfa	ace
Basic Info	
* Physical Interface	Ge0/7 ~
Interface Type	WAN ~
* VLAN ID	Ge0/7. 10
Description	VLAN 10 to ISP
Zone	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**.

Address				
IP Туре IPv4 IPv6				
* Connection Type 🔘 Static Address	DHCP	O PPPoE	O No IP Address	

- (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.
 - 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.
 - 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	sec_1							
Enabled State	• Enable 🔿 Disable							
* Policy Group	Default Policy Group	⊕ Add Group						
* Adjacent Policy	allow_all ~	Before 🗸						
Description	Enter the security policy name desc							
Src. and Dest.								
* Src. Security Zone	trust ~							
* Src. Address	any \checkmark							
* Dest. Security	untrust \vee							
Zone								
* Dest. Address	any \lor							

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

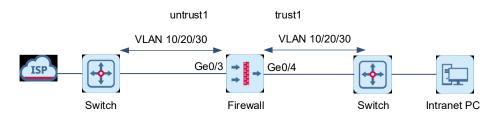
Device Type	Device Name	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	All versions

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.

Ruijie Z Series	Firewall	_ ☐ Home	Network	줄 Policy ۞ System	Network
Interface	>	Zone			
😨 Zone			D = 1 = 1		
		⊕ Create 🛅 Delete	C Refresh		
		Name	Descri	ption	Interface List
		trust	Trust 2	ione.	Ge0/0,Ge0/1,Ge0/2
		untrust	Lintas	t Zone.	Ge0/3,Ge0/7
					000/0,000/7
뗅 VRRP		DMZ	Demil	tarized Zone.	-

b Create the security zone trust1 and click Save.

< Back Add Security Z	one	
* Name	trust1	
Description		
Interface	To-be-selected (6) Select All	Selected (0) Clear
	Enter the keyword.	Enter the keyword.
	Interface	
	Name	
	Ge0/4	
	Ge0/5	
	Ge0/6	
	Ge0/8	
	TenGe0/0	
		Save

- c Repeat the previous steps to create the security zone ${\it untrust1}.$
- (2) Creating a Bridge Interface
 - a Choose Network > Interface > Bridge Interface and click Create to create the bridge interface br1.

Ruíjie Z Series Firewall	습 Home 🛛 🛛 Monitor	Network P Object	ত্ত Policy (ই System	ا Network D
	Bridge Interface			
Subinterface	(i) Member interfac	es are interfaces configured v	vith the transparent mode.	
Bridge Interface	⊕ Create 🗊 Delet	te 🖸 Refresh 🥥 Enable	e 🛇 Disable	
	Bridge Interfa	ace Member I	nterface Connection Type	IP
	Dr0		0/3, Ge0/4 0/6, Ge0/8 DHCP	-
00 DNS				

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.

< Back Add Bridge Interface
Basic Info
* Interface Name br1
Connection Status 🧿 Enable 🔿 Disable
Member Interface Select ~
Address
Connection Type 🔘 Static Address 💿 DHCP
Src. MAC Consistency
Check
① Src. MAC Consistency
Check
Access Management
Permit 🗌 HTTPS 📄 PING 📄 SSH
Save

- 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	Ge0/4						
Description							
Connection Status	• Enable 🔿 Disable						
Mode	 Routing Mode Transparent Mode 	Off-Path Mode					
* Bridge Interface	br1 v	Add Bridge Interface					
* Zone	trust1 ~	Add Security Zone					
Interface Type	O WAN Interface O LAN Interface						
Advanced							
① MTU	1500						
MAC	00:d0:f8:22:37:0d	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.
 - Set Src. Security Zone to trust1.
 - Set Src. Address to any, indicating packets with all IP addresses in the source security zone are permitted.
 - Set Dest. Security Zone to untrust1.
 - Set **Dest. Address** to **any**, indicating that a user is allowed to access resources with all IP addresses in the destination security zone.
 - Set Action Option to Permit.

< Back Create Security Policy								
Basic Info								
* Name	sec_1							
Enabled State	• Enable 🔿 Disable							
* Policy Group	Default Policy Group \sim	③ Add Group						
* Adjacent Policy	allow_all ~	Before 🗸						
Description	Enter the security policy name desc							
Src. and Dest.								
* Src. Security Zone	trust1 ~							
* Src. Address	any \vee							
* Dest. Security	untrust1 ~							
Zone								
* Dest. Address	any \vee							

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.
--

Ruijie Z Series Firewall	습 Home 🛛 Monitor	Networ	rk 욘 Obje	ct 🖾 Policy	🕀 Sys	tem		Netwo	nk Discovery	🔕 Network Mgm	₤ t Quick Onboarding	Ø Policy Wizard	ဂြ Customer Service	ز adi e
Security Policy ~	Security Policy												69 Simulation	Space
Policy Config Wizard Security Policy	Policy Group	•	Create	Delete 🔗	Enable	O Disable	C Refresh	More ~		Type All		Enter a key	vord.	
Policy Optimization	 Add Policy Group 		Priorit	y Name	Addr	Service	App	Time Rang e	Action	Content Sec urity	Hit Count	Hit Session	Operatio	'n
Policy Life Cycle	Keyword Q		Default Poli	icy Group										
Traffic Learning	BE (5) Default		1	sec_2	ny	any	any	any	Perm		2612 Clear	View Details	Ed	
🛱 NAT Policy >			2	sec_1	ny	any	any	any	Perm		5076 Clear	View Details	Ed	
Blocklist and Allowlist			3	allow_trus	. ny	any	any	any	Perm	l	0 Clear	View Details	Delete	
SSL Praxy >			4	allow_all	ny	any	any	any	Perm		0 Clear	View Details	Delete	
			5	Default Po.	. ny	any	any	any	Den		0 Clear	View Details	Edit Del	lete

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

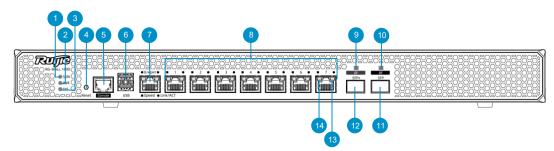


Table 9-1	Components on the Front Panel
-----------	-------------------------------

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

No.	Component	Description
		It is used to connect to the console for device maintenance and
		diagnosis.
_		Note:
5	Console port	 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	MONT	It is used to access the device management page upon first
7	MGMT port	login.
8	10/100/1000BASE-T ports	Ports 1 to 7, which are used to connect Ethernet cables.
		Steady green: The port is connected.
9	10GE SFP + port LED	• Blinking green: The port is receiving or sending data.
		Off: The optical port is incorrectly connected.
		• Steady green: The port is connected.
10	1GE SFP port LED	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 <u>Table 1-5</u> .
		Port 0F. For details about optical modules that support this port,
12	10GE SFP+ port	see <u>Table 1-5</u> .
	Link/ACT status LEDs	 Steady green: The port is connected.
13	(square) of	 Blinking green: The port is receiving or sending data.
	10/100/1000BASE-T ports	 Off: The port is incorrectly connected.
	Speed LEDs (round) of	Stoody orange: Chit/s part apod
14	10/100/1000BASE-T ports	 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.

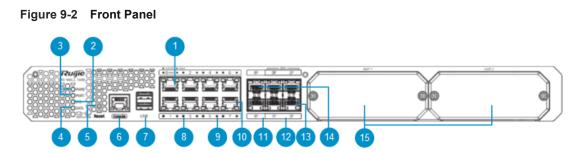


Table 9-2 Components on the Front Panel

No.	Component	Description
1	MGMT port	It is used to access the device management page upon first login.
2	System status LED (SYS)	 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)	 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	 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: 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	 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	Solid orange: Gbps port speedOff: 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	Solid green: The port is connected.Blinking green: The port is receiving or sending data.
12	10GE SFP + port LEDs	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.

Device H	ardware Monit	oring					
Device Ha	rdware Usage						
C Refresh						Display Cycle	Recent 1 Hour 🗸 🗸
CPU Us	age						
100%							
80%							
60%							
40%				· · · · · · · · · · · · ·			
20%							
0%	09:20	09:30	09:40	09:50	10:00	10:10	

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



The hard disk usage is displayed only when a hard disk is installed on the device.



Follow-up Procedure

Item	Description
CPU Usage	In normal cases, the CPU usage should be lower than 80%. If the CPU usage is too high for a long time, check the device and analyze the causes. The possible causes for high CPU usage are as follows:
	 App protection or DDoS protection is enabled. Too many connections are created, many of which are initiated by attackers.
Memory Usage	In normal cases, the memory usage should be lower than 80%. If the memory usage is too high for a long time, check the device and analyze the causes.
Hard disk Usage	In normal cases, the hard disk usage should be lower than 90%. If the remaining hard disk space is too small for a long time, check the device and clear the hard disk space.

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.

System Log									
Unhandled Handled									
Set to Handled [1 Expor	t 😋 Refresh								
Date	2023-12-14	to 🗎 2023-12-14	Security Level	All ~	Enter the keyword.	Q			
Security Level \ddagger	Log Type 👙	Time 🌲	Details		Operati	ion			
No Data									

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

Field	Description
Security Level	Security level of a system log.
Log Туре	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.

Securi	ity Log					
🚺 Exp	port 😋 Refre	sh 🚺 Export All		2Q Search Criteria Enter an IP a	address or a p	ort number. Q
Searcl	h Criteria: Time: 3	2023-12-14 00:00:00 2023-12	2-14 23:59:59 Severity: Hi	ligh,Medium,Low × Clear	Action	
No.	Severity 🗘	Security Event $\mbox{$\ddagger$}$	Dest. Address 😄	© App ‡		Operation ≡~
				No Data		

Field	Description
Severity	Severity level of a problem marked in the security log.
Security Event	Description of a security event recorded in the log.
Log Туре	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.

Keyword Filter Log										
	Lagrandian Export Refresh External Enter an IP address or a port number. C Search Criteria Time: 2023-12-14 00:00:00 2023-12-14 23:59:59 Clear Clear									
Time ≑	User 🌲	Application P rotocol ‡	Directio n ‡	Matching Keyword Se t ‡	Src. Address 💲	Dest. Addre ss 🌲	③ App ≑	Action ‡	Matching Policy	
					No Data					

🚺 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.

URL Analysis	IM	Search Engine	Email	Forum_Weibo	File						
🚺 Export	Refresh	Custom Field				EQ Search	n Criteria	Enter an IP	address or a j	port n	Q
Search Criteria	Time: 2023-12-	14 00:00:00 2023-12-14	23:59:59 Cle	ear							
No.	Time ≑	U	ser ≑	URL Category ≑		URL \$	Src. Ad	ddress ≑	Dest. Add	Operat	ion
							No Data				

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.

Export	Search Cri	Iteria Custom Fiel			-12-14	Start Tim	e © 11:00:00) End	Time © 1	1:59:59	Enter a	an IP address (or a port numl	ber. Q
Log Recor d Time 🗢	Session D uration	Src. Address 🖨	Dest. Add ress \$	Src. Port	Dest. Port ≑	Protocol ‡	① App \$	User ≑	Forward Packets	Forward Bytes 🗘	Reverse P ackets \$	Reverse B ytes ¢	Security P olicy \$	Operatio
2023-12	12Second	10.51.210.92	10.51.21	59607	161	UDP	Applicati	10.51.21	3	240	-	-	_visit_lo	View Det
2023-12	12Second	10.51.212.212	10.51.21	58649	58649	ICMP	Echo-re	10.51.21	1	84	1	84	_visit_lo	View Det
2023-12	12Second	10.51.212.212	172.30.4	58648	58648	ICMP	Echo-re	10.51.21	1	84	1	84	_visit_lo	View De
2023-12	42Second	10.51.212.210	10.51.21	37652	22	ТСР	SSH	10.51.21	43	5269	34	4734	visit_lo	View De
2023-12	2Second	10.51.212.212	10.51.21	48752	53	UDP	UDP-DNS	10.51.21	1	61	1	301	_visit_lo	View De
2023-12	2Second	10.51.212.212	172.30.4	40687	53	UDP	UDP-DNS	10.51.21	1	61	1	77	visit_lo	View De
2023-12	11Second	10.51.210.92	10.51.21	59602	161	UDP	Applicati	10.51.21	3	240	-	-	_visit_lo	View De
2023-12	11Second	10.51.212.212	172.30.4	58647	58647	ICMP	Echo-re	10.51.21	1	84	1	84	visit_lo	View De
023-12	11Second	10.51.212.212	10.51.21	58646	58646	ICMP	Echo-re	10.51.21	1	84	1	84	_visit_lo	View De
2023-12	11Second	10.51.212.212	10.51.21	40752	22	TCP	SSH	10.51.21	12	2330	12	2333	_visit_lo	View De

1 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 😋 I	Refresh				2	Q Search Criteria	Enter an IP address.	Q
Search Criteria :	Time Range: 2024-01-15 (00:00:00 2024-01-15 23:59:59	Admin: All Users Source: All Type	sClear				
Admin ‡	Host IP 🌲	Operation Object	Operation 🗘	Operation Time	Source	Desci	ription	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

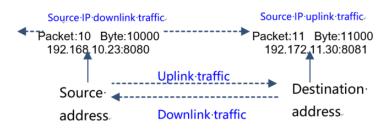
Application Scenario

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.

Interface Traffic Statistics Interface Traffic Details Interface:All WAN Interfaces 1bps	Uplink	Interface Downlink	All WAN Interfaces 🛞 🗸	Display Cycle	Real-Time	~
	 Uplink 	Downlink				
1bps						
0.8bps						
0.6bps						
0.4bps						
0.2bps						
0Bytes	13:55		13:56	13:57		13:58
10,24	10.00		10.00	13:57		15.56

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

Interface	Traffic Statistics					
Interface Tra	ffic Statistics	e Traffic Details				
🚺 Export	C Refresh				Enter an i	nterface name. Q
	Interface ≑	Interface Status 💠	Zone ≑	IP ‡	Uplink ≑	Downlink ≑
	Ge0/0		trust	10.51.212.212/24	9.46Kbps	3.18Kbps
	Ge0/1	m	zone1	10.10.10.1/24 2000:10::1/64	2.82Mbps	47.89Kbps
	Ge0/2		zone2	20.20.20.1/24 2000:20::1/64	50.44Kbps	2.79Mbps
	Ge0/3	m			Obps	Obps
	Ge0/4	m	test3		Obps	Obps
	Ge0/5	m	zone4	42.194.197.1/24	Obps	Obps
	Ge0/6	m	trust		Obps	Obps
	Ge0/7	m	untrust		Obps	Obps
	TenGe0/0	m	monitor		Obps	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 O to enable real-time traffic statistics.

Real-Time Traffic	
① Real-Time Traffic	

(3) Set the traffic range for statistics collection. Traffic statistics can be collected based on the source IP address, application, and user.

1 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.

• Set **Type** to **Src. IP** to display top 5 source IP addresses with the highest traffic and corresponding traffic information.

Real-Time Traffic		
Real-Time Traffic	Interface All WAN Interfaces • V Type Src	. IP V Query Time Range Recent 24 Hours V Query Range TOP5 Traffic Distribution ③
InterfacesAll WAN Interfaces B.00Mbps 6.00Mbps 4.00Mbps	Uptick Opworlink	100.100.213.16 31.86%
2.00Mbps 0Bytes 18:00 19:00 20:00 21:00 22:00 23:00		100.100.127.124 32.21%

 Set Type to App Name to display top 5 applications with the highest traffic and corresponding traffic information.

Real-Time Traffic	
Real-Time Traffic	Interface All WAN Interfaces: Type App Name Query Time Range Recent 24 Hours Query Range TOP5 Traffic Distribution ③
Interface:All WAN Interfaces 8.00Mbps 6.00Mbps	Uplink Downlink SYN_ACK 0.01% Tumble 31.86% Assemble 35.92%
4.00Mbps	
2.00Mbps 0Bytes 18:00 19:00 20:00 21:00	11STREET 32.21%

• Set Type to Username to display top 5 users with the highest traffic and corresponding traffic information.

eal-Time Traffic		
 Real-Time Traffic 		
	Interface All WAN Interfaces ® V Type U:	ername V Query Time Range Recent 24 Hours V Query Range TOP5 V
Traffic Trend		Traffic Distribution 🕕
Interface:All WAN Interfaces	Uplink Downlink	10.0.0.44 19.41%
400.00Mbps MMM	1	
200.00Mbps 200.00Mbps	A	10.0.39 19.42% 10.0.0.61 20.04%
100.00Mbps		10.0.0.55 19.6%
0Bytes 12:00 13:00 14:00 15:00	16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 00:00 01:00 02:00 03:00 04:0	05:00 06:00 07:00 08:00 09:00 10:00 11:00

(4) Click the line chart to view the traffic ranking list.

Real-Time Traffic						
 Real-Time Traffic 						
	Interface All WAN Interfaces ®	√ Туре	Username \vee	Query Time Range	Recent 24 Hours V Query Rang	e TOP5
Traffic Trend	2023-12-13 15:18:56 10.0.053: ↑1.33Mbps , ↓5.93Mbps			Traffi	c Distribution ()	
Interface:All WAN Interfaces	10.0.0.18: 11.82Mbps , ↓ 5.12Mbps 10.0.0.34: 11.68Mbps , ↓ 5.22Mbps 10.0.0.47: 12.10Mbps , ↓ 4.67Mbps 10.0.032: 11.33Mbps , ↓ 5.24Mbps Other: 1128.55Mbps , ↓ 327.43Mbps	link			10.0.0.32 19.07%	10.0.0.53 21.08%
400.00Mbps 300.00Mbps 200.00Mbps	Click to view details.				10.0.0.47 19.66%	10.0.0.18 20.15%
100.00Mbps 0Bytes					10.0.0.34 20.04%	
12:00 13:00 14:00 15:00 1	6:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 0	00:00 01:00 02:00 03	:00 04:00 05:00 06:00 07:00 08:00	09:00 10:00 11:00		

< Back Ranking Lis

Ranking Username Type Username Center a username. Center a username. Separate VPN and Non-VPN Traffi 1 10.0.58 20.785/0 153.443/0 174.228/0 2 10.0.33 51.902/0 104.611/0 156.513/0	🚺 Export
Ranking Username (Forward/Suppress) (Forward/Suppress) (Forward/Suppress) 1 10.0.58 20.785/0 153.443/0 174.228/0	
2 10.0.33 51.902/0 104.611/0 156.513/0	
3 10.0.78 39,744/0 82.008/0 121.752/0	
4 10.0.41 14.649/0 106.752/0 121.401/0	
5 10.0.32 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.

< Back 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 v Type Username v Enter a username.					d Non-VPN Traffic	
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(kb ps) (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

Keak Ranking List							
The current interface is All WAN Interfaces. Uplink traffic: traffic sent from the interface. Downlink traffic: traffic received by the interface. X							
Time : 2023-12-13 15:23:56 Query Range TOP5 v Type Username v Enter a username. Q 🖬 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(kb ps) (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 **O** to enable traffic statistics.

Traffic Statistics						
① Traffic Statistics						
O Uplink Traffic O Downl	link Traffic 🛛 💿 Total Traffic					

(3) Set search criteria to view information about specific traffic.

Traffic Statistics				
O Traffic Statistics				
Uplink Traffic O Downlink Traffic	Total Traffic Type App Name V	Query Time Range Recent 1 Hour V	Enter an application name.	n
		No data		
Traffic Ranking List				
Query Range TOP20 \lor			🔃 Custom Field 🚺 Export	Consult
Ranking 🗘 App Name 🗘	Uplink Traffic 🗘	Downlink Traffic 👙	Total Traffic 🗘	
		No Data		

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. <u>Configuring the New Session Limit</u>.

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.

Session Number Monitoring			
		Enter an IP address.	Q
IP	New Session Number Limit/s		
	No Data		

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 \otimes
Are you sure you want to enable real-time session statistics?
When this function is enabled, the device performance is greatly affected.

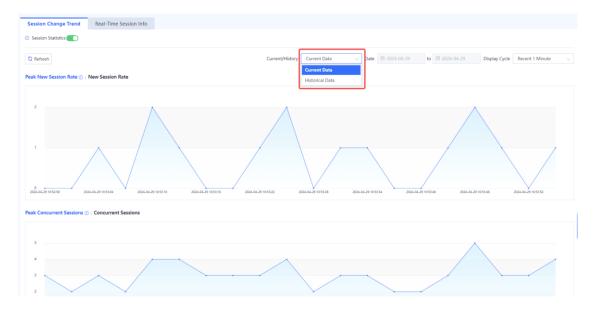
(4) You can query current or historical data:

OK

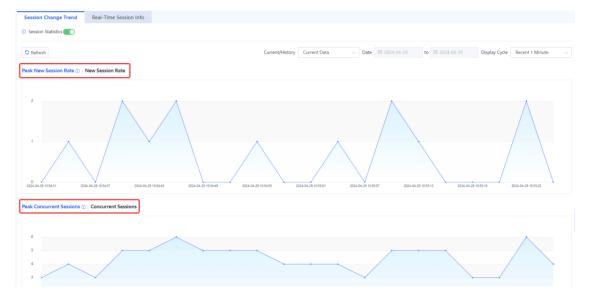
o Current Data: displays trends in new and concurrent sessions over the last 24 hours.

Cancel

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.

Sessi	on Change Trend	Real-Time Session Info								
	ock 🕄 Search Criteria	Custom Field C Refresh							Refresh Inter	val 30s
earc	h Criteria: Session Creation	Time: 60Minute × Clear								
	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	О Арр	Security Policy	Operation
	2023-07-28 17:42:19	29Minute58Second	172.17.97.28	10.51.212.212	53302	443	TCP	HTTPSprotocol	visit_local	Block View Details
	2023-07-28 17:42:19	29Minute58Second	172.17.97.28	10.51.212.212	53304	443	TCP	HTTPSprotocol	visit_local	Block View Details
	2023-07-28 17:32:42	28Minute14Second	10.52.24.249	10.51.212.212	10863	22	TCP	SSH	visit_local	Block View Details
	2023-07-28 17:42:19	29Minute58Second	172.17.97.28	10.51.212.212	53303	443	TCP	HTTPSprotocol	visit_local	Block View Details
	2023-07-28 17:28:56	22Minute19Second	100.100.121.50	200.200.116.196	56419	443	TCP	Global New	L7	Block View Details
	2023-07-28 17:42:19	29Minute58Second	172.17.97.28	10.51.212.212	53306	443	TCP	HTTPSprotocol	_visit_local_	Block View Details
	2023-07-28 17:34:45	25Minute57Second	100.100.44.200	200.200.160.243	50197	443	TCP	NBC News	L7	Block View Details
	2023-07-28 17:30:17	29Minute58Second	10.51.212.212	34.111.156.117	34854	5683	TCP	HTTPSprotocol	visit_local	Block View Details
	2023-07-28 17:32:38	29Minute1Second	10.51.212.212	47.104.206.152	44440	25857	TCP	HTTPSprotocol	_visit_local_	Block View Details
	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

 \otimes

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 Inbound Interface:Ge0/7 Forward Packets:7 Reverse Packets:4 Security Policy:Iocal

App:HTTPSprotocol
Outbound Interface:lo
Forward Bytes:816
Reverse Bytes:320

Session State:connection being closed and connection resources being reclaimed

Disable

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

Sessi	on Change Trend	Real-Time Session Info								
A BI	ock 🔄 Search Criteria h Criteria: Session Creation	Custom Field Refresh							Refresh Inte	rval 30s
	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	① Арр	Security Policy	Operation
	2023-07-28 17:43:19	2Second	10.52.24.249	10.51.212.212	4894	443	TCP	HTTPSprotocol	_visit_local_	Block View Details
	2023-07-28 17:32:42	27Minute16Second	10.52.24.249	10.51.212.212	10863	22	TCP	SSH	_visit_local	Block View Details
	2023-07-28 17:28:56	21Minute21Second	100.100.121.50	200.200.116.196	56419	443	TCP	Global New	L7	Block View Details
	2023-07-28 17:43:19	2Second	172.17.97.28	10.51.212.212	54171	443	TCP	HTTPSprotocol	visit_local	Block View Details
	2023-07-28 17:34:45	24Minute59Second	100.100.44.200	200.200.160.243	50197	443	TCP	NBC News	L7	Block View Details
	2023-07-28 17:30:17	30Minute0Second	10.51.212.212	34.111.156.117	34854	5683	TCP	HTTPSprotocol	_visit_local_	Block View Details
	2023-07-28 17:32:38	29Minute27Second	10.51.212.212	47.104.206.152	44440	25857	TCP	HTTPSprotocol	visit_local	Block View Details
	2023-07-28 17:41:20	30Minute0Second	100.100.213.16	200.200.107.6	53791	443	TCP	Tumblr	L7	Block View Details
	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
	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.

Sessi	on Change Trend	Real-Time Session Info								
A Bl	ock Search Criteria ch Criteria: Session Creation	Time: 60Minute × Clear							Refresh Inte	30s
	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	① Арр	Security Policy	Operation
	2023-07-28 17:42:49	30Minute0Second	172.17.97.28	10.51.212.212	53741	443	ТСР	HTTPSprotocol	_visit_local_	Block View Details
	2023-07-28 17:32:42	27Minute46Second	10.52.24.249	10.51.212.212	10863	22	ТСР	SSH	_visit_local_	Block View Details
	2023-07-28 17:28:56	21Minute51Second	100.100.121.50	200.200.116.196	56419	443	ТСР	Global New	L7	Block View Details
	2023-07-28 17:34:45	25Minute29Second	100.100.44.200	200.200.160.243	50197	443	TCP	NBC News	L7	Block View Details
	2023-07-28 17:30:17	29Minute30Second	10.51.212.212	34.111.156.117	34854	5683	TCP	HTTPSprotocol	_visit_local_	Block View Details
	2023-07-28 17:32:38	29Minute57Second	10.51.212.212	47.104.206.152	44440	25857	TCP	HTTPSprotocol	_visit_local_	Block View Details
	2023-07-28 17:41:20	30Minute0Second	100.100.213.16	200.200.107.6	53791	443	TCP	Tumblr	L7	Block View Details
	2023-07-28 17:42:33	29Minute59Second	10.51.212.210	10.51.212.212	40046	22	ТСР	SSH	_visit_local_	Block View Details
	2023-07-28 17:42:38	29Minute49Second	10.51.212.212	10.51.213.10	45144	22	ТСР	SSH	visit_local	Block View Details
	2023-07-28 17:42:49	2Second	172.17.97.28	10.51.212.212	53740	443	ТСР	HTTPSprotocol	_visit_local_	Block View Details

(5) (Optional) Click **Custom Field** to set the session fields to be displayed on the page.

Sessi	on Change Trend	Real-Time Session Info								
A B	cock 🤄 Search Criteria	Time: 60Minute × Clear							Refresh Inte	30s v
	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	① App	Security Policy	Operation
	2023-07-28 17:43:19	2Second	10.52.24.249	10.51.212.212	4894	443	TCP	HTTPSprotocol	_visit_local_	Block View Details
	2023-07-28 17:32:42	27Minute16Second	10.52.24.249	10.51.212.212	10863	22	TCP	SSH	_visit_local	Block View Details
	2023-07-28 17:28:56	21Minute21Second	100.100.121.50	200.200.116.196	56419	443	TCP	Global New	L7	Block View Details
	2023-07-28 17:43:19	2Second	172.17.97.28	10.51.212.212	54171	443	TCP	HTTPSprotocol	_visit_local_	Block View Details
	2023-07-28 17:34:45	24Minute59Second	100.100.44.200	200.200.160.243	50197	443	TCP	NBC News	L7	Block View Details
	2023-07-28 17:30:17	30Minute0Second	10.51.212.212	34.111.156.117	34854	5683	TCP	HTTPSprotocol	visit_local	Block View Details
	2023-07-28 17:32:38	29Minute27Second	10.51.212.212	47.104.206.152	44440	25857	TCP	HTTPSprotocol	visit_local	Block View Details
	2023-07-28 17:41:20	30Minute0Second	100.100.213.16	200.200.107.6	53791	443	TCP	Tumblr	L7	Block View Details
	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
	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.

Ruijie Z Series Firewall	습 Home 😌 Monitor 🔀 Network 🔑 Object 😳 Policy	(i) System	M S E Network Discovery Network Mgmt Quick Onboarding	Policy Wizard Customer Service admin
Security Cookpit Security Cookpit Security Cookpit Log Monitoring Netligence Overview Traffic Monitoring Y	I Intelligence Overview Hit Distribution by Intelligence Type	Intelligence Hit Trend		Cycle Recent 1 Day 🗸
Session Monitoring Traffic Monitoring	No data	0	0000	
	Hit Src. IP Ranking	Hit Dest. IP Ranking	Hit Domain Name Ranking	
	No data	No data	No	data a
Ξ				

(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.

ltem	Description
Hit Distribution by Intelligence Type	Displays hit distribution by intelligence type in a pie chart. This information allows administrators to master major threats in the current network environment so that they can intensify protection accordingly. Move the pointer over this area to view the number of hits of each intelligence type and the proportion.
Intelligence Hit Trend	Displays the number of hits of threat intelligence in various periods within the statistical cycle in a line chart. This information helps administrators find periods with high occurrence of attack threats or check whether protection measures are effective. Move the pointer over the line chart to view the number of hits over each period.

Hit Src. IP Ranking	Displays the ranking of source IP addresses with threat intelligence by the number of hits. This information helps administrators analyze the threat source and then develop corresponding protection measures to block the traffic from these source IP addresses. Click an IP address to switch to the security log page. Security logs of this source IP address are automatically filtered out.
Hit Dest. IP Ranking	Displays the ranking of destination IP addresses with threat intelligence by the number of hits. This information helps administrators analyze addresses of compromised hosts on the botnet or IP addresses attacked by malicious programs and then develop corresponding protection measures to protect these hosts. Click an IP address to switch to the security log page. Security logs of this destination IP address are automatically filtered out.
Hit Domain Name Ranking	Displays the ranking of domain name addresses with threat intelligence by the number of hits. This information helps administrators analyze malicious domain names and then develop corresponding protection measures to block and protect the traffic from these domain names. Click a domain name to switch to the security log page. Security logs of this domain name are automatically filtered out.

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 multichannel protocol is used for data transmission.

Procedure

(1) Choose Policy > NAT Policy > ALG.

Ruíjie Z Series Firewall	A Home @ Monitor @ Network & Object Characterization @ System Characterization @ System Characterization @ System Section &
	I ALG
	O Select the protocols for which you want to enable the ALG function.
	After this function is enabled for a multi-channel protocol, packet filtering and NAT can be performed on the ports that are temporarily negotiated in the protocol.
	Select All
	S FTP(TCP, port number: 21)
	TFTPIUDP, port number: 69)
ALG	 DNS-UDP(UDP, port number: 53)
Address Pool	
	SIP-TCP(TCP, port number: 5060)
	SIP-UDP(UDP, port number: 5060)
	Save
	- 50YC

(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.

11.1 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.

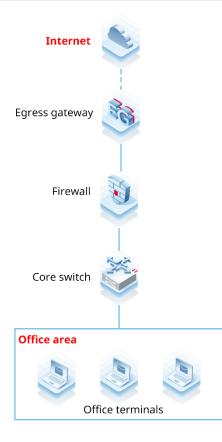
11.2 Firewall Deployment

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:

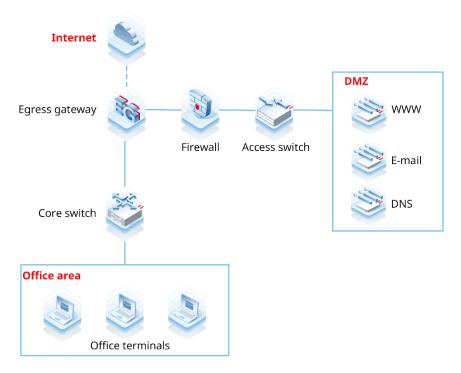
Transparent mode - office network egress link - single-in single-out

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.



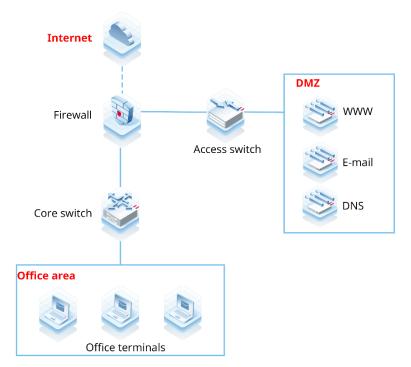
• Transparent mode – area boundary - single-in single-out

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.



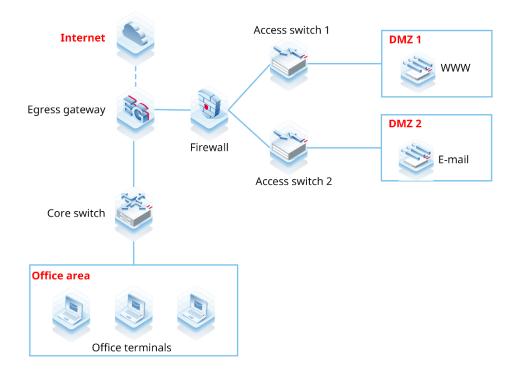
• Gateway mode - single ISP access

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.

Ruijie Z Series Firewall	습 Home I Monitor
Admin >	Web SSH Advanced Settings
System Config ~ System Time	* SSH Port 22
SNMP Service Parameters	* Allowed Consecutive 3 Login Failures
Authorization Management	* Lockout Period (min) 1
Fault Diagnosis > Cloud Management Platform	Save Restore Defaults
Signature Library Upgrade	
Ø System Maintenance →	

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.

Ruijie Z Series Firewall	≙ Home	nitor	A Object	@ Policy	⊖ Syste	m				Netwo	M ork Discovery	🔕 Network Mgmt	(Quick Onboarding	Policy Wizard	G Customer Ser	Q vice admin
	policies to be optimiz traffic exceptions to b ndled		Ruijie 23200-5	0/		1 2	3	4	5		7 OF View Devic	e Details>>				1.6% ard Disk

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.

terface Traffic Statistics Interface Traffic	Details		Interface All WAN In	terfaces 🛞 \vee Display Cycle Real-Time	
Interface:All WAN Interfaces		Uplink Downlink			
0.00Mbps 0.00Mbps	~~~~	~~~~~	\sim	\bigwedge	~
00Mbps 00Mbps	^				
00Mbps 00Mbps			\sim	\sim \sim \sim	
Obps				16:14	

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.

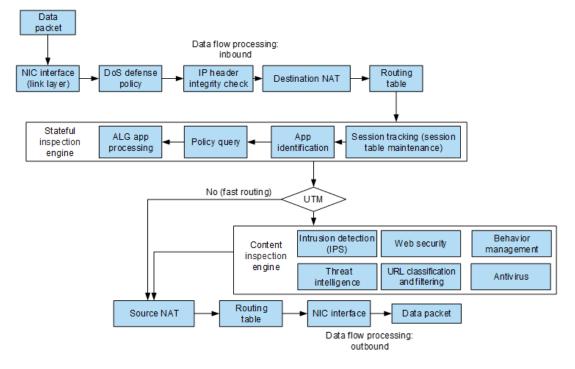
The data flow direction is determined by the source security zone and destination security zone, while the source address, destination address, service, and time range can directly reference defined objects.

- (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:
 - 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 proxybased 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.

- 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:
 - 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.
 - 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.
 - 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.
 - URL classification and filtering: URL classification and filtering are performed on network traffic based on the URLs carried in the traffic.
 - 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.

Diagnosti	c Center		
Go to Diagno	ose Based on Issue		
Ô	Network connectivity is normal. View Historical Diagnostic Record Last Diagnosis Time: 2024-03-20 11:46:46	Diagnose	
Ô	IPsec VPN Diagnosis View Historical Diagnostic Record Last Diagnosis Time: 2024-03-12 11:16:30	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 Conne	Network Connectivity Diagnosis					
Diagnos	tic Parameter Settings					
N		ange to achieve a better dia	gnostic result. If the diagnostic range i	Jetection, packet tracing, and traffic receiving and forwarding detection. is too large, only 1000 flows will be obtained. Packet tracing only displays the		
* () Src. Address	Enter the source address.	 Src. Port 	Enter the source port number.			
① Dest. Address	输入目的地址	 Dest. Port 	Enter the destination port numbe			
Inbound Interface	Select ~	* Protocol	Select ~			
① Src. MAC	例: d8:9e:f3:3f:d5:64	① Dest. MAC	Example: d8:9e:f3:3f:d5:64			
	Diagnose					

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

Network Connectiv	vity Diagnosis					Exit
Fault Diagnosis Tracing						
Diagnostic Parameters:	Src. Address:172.20.37.124	Src. Port:any	Dest. Address:any	Dest. Port:any Inbound Interface:	Protocol:TCP Src. MAC: any Des	st. MAC: any
23%			2			
c Receiving Detection ompleted within 23Second		Basic Co	nfig Detection	Pause Network Diag	Packet Tracing	Traffic Forwarding Detection
Diagnostic Result						
				No data		
Et Result Details						

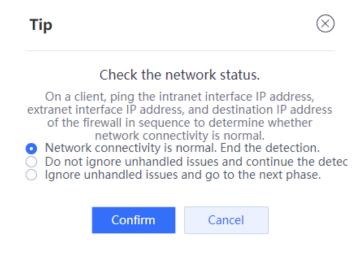
(5) After the diagnosis is complete, the diagnostic result and diagnostic details are displayed in the lower part of the page. After you troubleshoot the fault based on the diagnostic details, click **I have handled the problem**.

Network Connectivity Diagnosis			Ex		
Fault Diagnosis Tracing Diagnostic Parameters: Src. Address:192.168.1.44 Src. Portany Dest. r	ddress:114.114.114.114 Dest. Portany Inbound Interfa	exGe0/0 Protocolap Src. MAC: any Dest.	MAC: any		
Receiving Detection Basic Config D	Participant Partic	- 😟	Traffic Forwarding Detection		
The f Diagnostic Result	ollowing 1 errors have been found. Please handle ther	according to suggestions.			
Result	Suggestion	Operation			
interfacemodule: The interface has not obtained an IPv4 address.[Ge0/1]					
interfacemodule: The interface has not obtained an IPv4 address.(Ge	Check interface configuration and connections.	Troubleshooting Ope	eration Ignore		
interfacemodule: The WAN interface is not added to an untrust zone	The interface is not added to the corresponding see whether a LAN interface is added to the trust zone, N interface is added to the untrust zone.				
interfacemodule: The interface is Up, but no configuration is perform	Configure a static IP address, DHCP, or PPPoE for the terface.	e corresponding in			
The NAT module passes the check.					
The security policy module passes the check. O					
The DNS module passes the check.					
The DHCP module passes the check.					

(6) In the **Tip** dialog box, select **Network connectivity is normal.** and click **Confirm**. The firewall continues to check the next item.

Note

If the fault is not rectified, select **Do not ignore unhandled issues and continue the detection.** The firewall performs the detection again.



(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 Diagno	ose Based on Issue				
8	Network connectivity is normal. View Historical Diagnostic Record Last Diagnosis Time: 2024-03-20 11:46:46	Diagnose			
Ŕ	IPsec VPN Diagnosis	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	c Center	
Go to Diagno	ose Based on Issue	
Ô	Network connectivity is normal. View Historical Diagnostic Record Last Diagnosis Time: 2024-03-20 11:46:46	Diagnose
Ś	IPsec VPN Diagnosis C 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					
Diagnosti	Diagnostic Parameter Settings				
Diagnosis Type	 Tunnel Negotiation Error 	 Tunnel Forwarding Error 			
* Tunnel	Select				
Remote IP	Enter				
* 🕕 Diagnosis	30	Second			
Duration					
	Diagnose				

IPsec VPN Diagnosis						
Diagnosti	Diagnostic Parameter Settings					
Diagnosis Type	O Tunnel Negotiation Error • Tunnel Forwarding Error					
* Tunnel	Select					
Remote IP	Enter					
* 🕕 Src. Address	Enter the source address.					
* () Dest. Address	Enter the destination address.					
Protocol	Select ~					
🛈 Src. Port	Enter the Dest. Port number					
🕕 Dest. Port	Enter the Src. Port number.					
* 🕕 Diagnosis	30 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.

IPsec VPN Diagnosis		Exit
Fault Diagnosis Parameters Diagnostic Parameters: Tunnel Nameguoruo Remote IP:1.1.1.1		
Diagnostic Result		
Session ID Time Remote IP Current Status	Diagnostic Result Handling Suggestion	Operation
10 √ / Page Total:0	No Data	Go to 1 < 1 >
	Diagnosing To be completed within 26Second Stop Diagnosis	

(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**.

Psec VPN	Diagnosis					Exi
Diagnostic Pa			e IP:1.1.1.1	Rediagnose 2		
Session ID	Time	Remote IP	Current Status	Diagnostic Result	Handling Suggestion	Operation
Session ID	Time 2024-04-12 17:34:38	Remote IP	Current Status Waiting for the respon	Diagnostic Result No response received from peer	Handling Suggestion Possible reasons: 1.Network failure 2.Inconsistent ne	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 Diagno	Go to Diagnose Based on Issue		
Ś	Network connectivity is normal. View Historical Diagnostic Record Last Diagnosis Time: 2024-03-20 11:46:46	Diagnose	
Ô	IPsec VPN Diagnosis View Historical Diagnostic Record Last Diagnosis Time: 2024-03-12 11:16:30	Diagnose	

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 Diagno	se Based on Issue	
Ô	Network Connectivity Di No diagnostic records	agnosis Diagnose
Ô	IPsec VPN Diagnosis No diagnostic records	Diagnose
Ø.	SSL VPN Diagnosis No diagnostic records	Diagnose

(3) Set diagnostic parameters and click **Diagnose**. The firewall checks tunnel connectivity.

SSL	VPN	Diagn	osis
		Plagin	0010

Diagnostic Parameter Settings			
Select	~		
 Login Failure 	Resource Access Failure		
Select			
https://			
Diagnose			
	Select Cogin Failure Select https://		

SSL VPN Diagnosis				
Diagnostic Parameter Settings				
Select	~			
O Login Failure	• Resource Access Failure			
Select				
Enter				
Select	~			
Enter				
Diagnose				
	c Parameter Settir Select O Login Failure Select Enter Select			

Item	Description	Remarks			
Login Failure	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 F	ailure				
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]			

		ТСР
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.

SSL VPN Diagnosis	;		Exit
Fault Diagnosis Parame Diagnostic Parameters :	Gateway:chptest Diagnosis Type:Login Failure	Usernamechp Gateway Addresschttps://1.1.1	
	Basic Environment Check To be completed within SSecond	Packet-based Diagnosis	
Diagnostic Result:		• ·	
		No data	

(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.

SSL VPN Diagnos	is		Exit
Fault Diagnosis Param Diagnostic Parameters:	Gateway:chptest Diagnosis Type:Login Failure Username:chp Gat	eway Address:https://1.1.1.1 Packet-based Diagnosis	
Diagnostic Result:	The following 1 errors have been found. Pl	ease handle them according to suggestions.	
Time	Diagnostic Result	Handling Suggestion	Operation
2024-06-07 14:06:26	The login address is inconsistent with the gateway configuratio	It is recommended to enter the correct gateway login aaddress 1	Configure
2024-06-07 14:06:26	The gateway can be logged in without a domain name 🛛	-	Cons
2024-06-07 14:06:26	Sufficient license capacity 🛛	•	Ę
10 V / Page Tota	l:3	Go to	1 (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	c Center
Go to Diagno	ose Based on Issue
Ø	Network Connectivity Diagnosis No diagnostic records Diagnose
\bigotimes	IPsec VPN Diagnosis No diagnostic records Diagnose
Ø.	SSL VPN Diagnosis View Historical Diagnostic Record Last Diagnosis Time: 2024-06-07 14:06:26

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.

Ruijie Z Series Firewall	습 Home 🛛 Monitor	Network	우 Object	Policy	System		Retwork Discovery	🕲 Network Mgmt	1 Quick Onboarding	Policy Wizard	Customer Service	ې admi
Admin >	Packet Obtaining	Tool										
♦ System Config →												
🗑 Fault Diagnosis 🛛 🗸	Start 🔟 Delete											
Diagnostic Center												
Device Self-Test	Packet obtaining state	us:Packet obtain	ing is stopped.	L.								
Ping	🗌 Name 🗢					Interface	÷	Size 🔅			Operation	
Tracert	2023-03-10_15	5-55-55.Ge0_3.p	cap			Ge0/3		78.0 K	В	Viev	Download Del	lete
Packet Obtaining Tool												
One-Click Collection												
Cloud Management Platform												
🗒 Signature Library Upgrade												

Packet Obtaining Option

 \otimes

You are advised to enter the complete source MAC address, destination MAC address, source IP address (port number), destination IP address (port number) to improve packet obtaining efficiency. An unspecified item is set to any.

* Interface	Select an inte	erface.	\sim
Packet			
Obtaining Rule			
Layer 2 Protocol	oany 🔿 I	IP 🔿 ARP	
①Src. MAC			
①Dest. 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.
 - o 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.
 - o 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

<u> </u>	r), destination IP address (por	rce MAC address, destination MAC address, s number) to improve packet obtaining efficie	
* Interface	Ge0/0	~	
Packet			
Obtaining Rule			
ayer 2 Protocol	🔿 any 💿 IP 🔿 ARP		
ayer 2 Protocol ayer 3 Protocol		q	
		0~65535	
ayer 3 Protocol	oany oTCP oU		
ayer 3 Protocol	oany oTCP oU	0~65535	

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

 \otimes

(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	Ge0/0	~
Packet Obtaining Rule		
Layer 2 Protocol	oany oIP ARP	
Layer 3 Protocol	🔾 any 💿 TCP 🔷 UDP	
OSrc. IP (Port)	192.168.1.1	0~65535
①Dest. IP (Port)	192.168.23.100	80
OSrc. MAC		
①Dest. MAC		
	Start Car	ncel

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.

Note

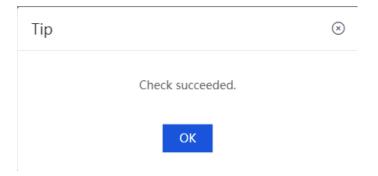
The device self-test function is supported from NTOS1.0R3. If your version is lower than NTOS1.0R3, upgrade it to NTOS1.0R3 or higher.

Procedure

- 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.

Device Self-Test Self-Test Score 93 Self-Test Score Self-Test Score Self-Test Details			
Export Check Log System Basic Info Check	System Basic Status	Log Status Check	-2points
Device Model:23200 Device Handware SNMACCWWM320001 Device Software SNM01024708192022 Device Software Venion:NGFW_NTOS Trunk, Release(02201901) Unable to obtain the version recommended by the cloud server.	44.5% 33.3% CPU Usage Memory Usage	OWhether Hard Dick is AvailableYies OWhether Systeg Server is set. The log store requirement may not be met.	age time
Management Mode Check -5points	Authorization Status Check	Policy Check	
S5H Login Failure Limit Admin Timeout Period: The login timeout period is long, and Fix scuthy final setist. Web Login Failure Limit	Attribute License: Not installed. Antivirus (AV): Trial license. Performance License: Not installed.	Policy Check	

(3) After device self-test is complete, in the dialog box that is displayed, click OK.



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

Device Self-Test Hardware Self-Test Self-Test Score Start Check Salf-Test Score Last Check Time:2023-12-14 10:19:25 Self-Test Details Y Export Check Log			
System Basic Info Check	System Basic Status	Log Status Check -2points	
Device Model/2320-5 Device Hardware SNMACCLHI/232511 Device Software SNMACCLHI/2325023 Once: Software Version/NGV/NTOS 1.0R7, Release(0)240501) Unable to obtain the version recommended by the cloud server.	23.2% 54.4% CPU Usage Memory Usage	Whether Hard Disk is Available/Yes Whether Syidog Server is Set. The log storage time requirement may not be met.	Consult
Management Mode Check -10points S5H Login Failure Limit Admin Timeout Period : The login timeout period is long, and security risks exist. Web Login Failure Limit	Authorization Status Check - 5points If threat Intelligence (DAS-Security): Not installed. Performance License: Not installed. ()	Policy Check	

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

- 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

Device Self-Test	Hardware Self-Test	
\bigcirc	Start Check Last Check Time:No data	
Self-Test Details		
🚺 Export Check Log		
No.	Check Item	Result
		No Data

(3) After the self-test is complete, a dialog box is displayed. Click **OK**.

Тір		(\times)
	Check succeeded.	
	ОК	

(4) If any item is abnormal, contact Ruijie Networks technical support.

Device Self-Test	Hardware Self-Test		
\bigcirc	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.

Ruffe Z Series Firewall	습 Home	Ø Monitor	Network	₽_ Object	중 Policy	System		M Network Discovery	⊗ Network Mgmt
& Admin →	One-Cli	ick Collectio	on						
♦ System Config >									
🕲 Fault Diagnosis 🛛 🗸		(i) One-clic	k collection is a	complete. You	can downloa	ad collected in	formation or perform collectio	n again.	
Diagnostic Center		Last Collection	Time2023-03-	11 13:40:28					
Device Self-Test		One-Click Co		Download					
Ping		One-Click CC	Direction	Download					
Tracert									
Packet Obtaining Tool									
One-Click Collection									
Cloud Management Platform									
🗐 Signature Library Upgrade									
Ø System Maintenance →									

- (2) Click One-Click Collection and wait for 3 to 5 minutes until information collection is complete.
- (3) Click **Download** to download the collected fault information to the PC for fault analysis.

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-suppo	rt fp exec stats
==== interface stats:	
lo-vr0 port:65534	
_eth0-vr0 port:65534	
_eth1-vr0 port:65534	
_eth2-vr0 port:65534	
Ge0_0-vr0 port:65534	
ifs_ipackets:124720	>Number of packets received by the interface
ifs_ibytes:14454713	>Number of bytes in the packet received by the interface
ifs_opackets:23430	>Number of packets sent by the interface
ifs_obytes:29152694	>Number of bytes in the packet sent by the interface
TenGe0_0-vr0 port:65534	
ifs_opackets:739	
ifs_obytes:33994	
br0-vr0 port:65534	
ifs_ipackets:306	
ifs_ibytes:18360	
==== global stats:	
fp_dropped:11053053	
fp_dropped_excp:14155	
fp_dropped_ether:326	

fp_dropped_bridge:2 fp_dropped_npf:11038563 --->Total number of lost service packets in the flow platform. The data will be used with statistical analysis of the flow platform later. fp_dropped_system:6 ==== exception stats: LocalFPTunExceptions:253437 ExceptionByModule: fp_exception_ether:199272 fp_exception_bridge:734 fp_exception_ip:37548 fp_exception_ipv6:15883 LocalExceptionClass: FPTUN EXC SP FUNC:206764 FPTUN_EXC_ETHER_DST:28299 FPTUN_EXC_IP_DST:15196 FPTUN_EXC_ICMP_NEEDED:687 FPTUN_EXC_NDISC_NEEDED:2491 LocalExceptionType: FPTUN_IPV4_OUTPUT_EXCEPT:2491 FPTUN_ETH_INPUT_EXCEPT:250946 FPTUN ETH SP OUTPUT REQ:2444 ExcpDroppedFpToLinuxUserExcSendtoFailure:102 ==== IPv4 stats: IpForwDatagrams:1648056613 IpInReceives:1648056613 ==== arp stats: arp unhandled:168695 ==== IPv6 stats: ==== TCP stats: total packets received:6758 # of packets not managed by MCORE_SOCKET:6758 ==== UDP stats: ==== vlan stats: ==== dsa stats: DsaDroppedInOperative:1 ==== bridge stats: L2ForwFrames:251334551 BridgeDroppedNoOutputPort:2 ==== ebtables stats: ==== pppoe stats:

2. cmd debug-support npf exec stats

This command is used to display statistics of various services in the flow platform.

firewall> cmd debug-support npf exec stats					
Policy action:	>Statistical summary of a security policy				
1008 Policy permit	> Number of flows permitted by the security policy				

	0 Policy deny	> Number of flows blocked by the security policy
Packe	ts dropped:	>Total number of lost service packets in the flow platform
	0 RPF check drop	
	0 Connection create	•
	0 Connection instal	
	0 Connection thresh	
	0 Connection invali	•
	0 Invalid connectior	drop
	0 Do SNAT drop	
	0 Do DNAT drop	
	0 NAT transition dro	p
	0 Do ALG drop	
	624879 Route error	drop
	0 thd-event mlist ful	l drop
	0 thd-event error dr	p
	0 Prepend failed dr	q
	0 Header too short	drop
	0 Fragment failure	lrop
	0 Invalid IP drop	
Wrong	packets dropped:	
	0 Interface error	
	0 lp header error	
	0 Frament packet	
	0 IP header hl error	
	0 TCP header error	
	0 UDP header error	
	0 ICMP header erro	r
	0 ICMP packet erro	r
	0 ICMP6 header en	or
	0 ICMP6 packet err	or
	0 checksum error	
	0 lpv6 header error	
	0 lpv6 extension he	ader error
Conne	ection entries:	
	625887 Connection	allocations
	0 Connection revers	Se la
	625886 Connection	release
	625884 Connection	destructions
	0 Connection refres	h conflict
	0 Connection alloca	tion failures
	0 Connection ID lim	it
	0 Connection ID inv	alid
	0 Connection ID no	entry
NAT e	ntries:	
	0 NAT entry allocati	ons
	0 NAT entry destruc	tions

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 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]rns 0 [2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp fast ip input pre routing: mbuf=0x18ad669c0

[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp fast ip output post routing: mbuf=0x18ad669c0 [2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp ether output: mbuf=0x18ad669c0, ifp=Ge0 1 port=65534 [2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]; fp_if_output: mbuf=0x18ad669c0, ifp=eth0, port=0 [2022/02/17 11:24:39]Feb 17 11:23:51 firewall uwsgi[2445]: <190>1 2022-02-17T03:23:51.525503Z firewall web 2445 - [operationLog@4881 ip="192.168.1.100" operator="<E7><AB><AF><E5><8F<8F><A3><E6><98><A0><E5><80><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><8<81><E7><94><A8><E7><AB><AF><E5><8F><A3><E6><98> <A0><E5><B0><84><E6><88><90><E5><8A><9F>" timestamp="1645068231" admin="admin"] [2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: [2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: fp ether input(ifp=eth0 port=0) [2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: sbuf data at [0x18e60ab82], len=78 [2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: 00000000 30 0D 9E 41 D8 D1 22 22 22 22 22 24 C0 10 00 00 [2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: 00000010 08 00 45 00 00 3C 3E 34 00 00 40 01 31 70 05 00 [2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: 00000020 40 35 AC 12 19 D6 08 00 19 14 00 01 34 47 61 62 [2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: 00000030 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 [2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: 00000040 73 74 75 76 77 61 62 63 64 65 66 67 68 69 [2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: fp_ether_input(ifp=Ge0_1 port=65534) [2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: fp ether input one(ifp=Ge0 1 port=65534) [2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: fp_ip_input_bulk_check: mbuf=0x18e60a900 [2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: npf packet handler: mbuf=0x18e60a900, npf mode=0 [2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: npf_packet_handler, 1029: conn 662 is expired, drop the mbuf 0x18e60a900!packet m=0x18e60a900 dropped at npf packet handler():1030 [2022/02/17 11:24:39]Feb 17 11:23:53 firewall fp-rte[1339]; flow-log 1230 send: src 83902517 sport 16374 dst 1964509311 dport 80 natsrc 3232261378 natsport 9278 natdst 1964509311 natdport 80 proto 6 direct 1 sendbytes 415 recvbytes 410 sendpkts 8 recvpkts 2 srcif Ge0 1 dstif Ge0 6 appid 0-0-0-0 policy allow all action 0 module reason time 1645068232 [2022/02/17 11:24:39]Feb 17 11:23:53 firewall fp-rte[1339]: flow-log 662 send: src 83902517 sport 1 dst 2886867414 dport 1 natsrc 3232261378 natsport 458 natdst 2886867414 natdport 458 proto 1 direct 1 sendbytes 54068232 [2022/02/17 11:24:39]Feb 17 11:23:53 firewall fp-rte[1339]: flow-log 710 send: src 83902517 sport 12345 dst 660748687 dport 8000 natsrc 3232261378 natsport 8959 natdst 660748687 natdport 8000 proto 17 direct 1 sendbytes 205 recvbytes 0 sendpkts 1 recvpkts 0 srcif Ge0 1 dstif Ge0 6 appid 0-0-0-0 policy allow all action 0 module reason time 1645068232

[2022/02/17 11:24:39]Feb 17 11:23:53 firewall fp-rte[1339]: flow-log 138 send: src 83902517 sport 61509 dst 2567170222 dport 8000 natsrc 3232241498 natsport 8326 natdst 2567170222 natdport 8000 proto 17 direct 1

sendbytes 1170 recvbytes 70 sendpkts 6 recvpkts 1 srcif Ge0_1 dstif Ge0_7 appid 0-0-0-0 policy allow_all action 0 module reason time 1645068233 [2022/02/17 11:24:39]Feb 17 11:23:53 firewall fp-rte[1339]: Connection 662 is destroyed

(2) cmd trace [level EMERG | ALERT | CRIT | ERR | WARNING | NOTICE | INFO | DEBUG] [max-number line] [timeout seconds] [type-off "all"] [type-on "NFP BASIC "]

This command is used to set the output level of debugging logs, the maximum number of rows in a log, maximum record timeout period (in seconds), and module enabling/disabling log.

- o **max-number**: Specifies the maximum number of rows in a printed log.
- **timeout:** Specifies the time when the log is printed.

1 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 (<u>https://secloud1.ruijie.com.cn</u>), click **Version Upgrade**, and select an applicable version to download it.

Zuijie	•	Library Upgrade	Version Upgrade	Device Authorization	Validity Period Que	IY SSLVPN					은 test
Version I	nfo Patch Info										
-	ownload software packag		Software Version. Otherworduct Series Select 1		Model Sele	ect a model.	 Software Version 	Select a softwa	re version. V		
No.	File Name	Version Number	Release Date	File Size (MB)	MD5	Applicable Model	Hardware Version A	pplicable Software Version	Version Description	Operation	
1	NGFW_NTOSTrun	NGFW_NTOS Tru	2023-01-05	163.74	4C8772E66DC4A	Z8620,Z8680	1.00	Universal	hjqtest: z8600-20	🛓 Download 🖹 View Version	
2	NGFW_NTOSTrun	NGFW_NTOS Tru	2023-01-04	163.69	5FA916C58951B8	Z8620,Z8680	1.00	Universal	hjqtest: z8600-20	± Download 🗈 View Version	
3	NGFW_NTOSTrun	NGFW_NTOS Tru	2022-12-29	167.41	a7277983ee08653	Z8620,Z8680	1.00	Universal	lyftest1	± Download 🗎 View Version	
4	NGFW_NTOSTrun	NGFW_NTOS Tru	2022-12-28	127.76	07bee08c49f3c121	Z5100	1.00	Universal	lyftest1	🛓 Download 🖻 View Version	

 Method 2: Log in to the web page of the firewall and choose Home > View Device Detail > Version Info or System > System Maintenance > System Upgrade.

Ruijie Z Series Firewall	Home @ Monitor @ Network & Object @ Policy @ System Network Discovery Network Mgmt Quick Onboarding Policy Wizard Customer Service admin
🔑 Admin 🗸 🗸	I System Upgrade
Admin	
Admin Role	① You can perform an upgrade online or visit Ruijje Secure Cloud Platform at https://secloud1.uujje.com.cn On the platform, access the Software Version page and download the latest system upgrade file. Then, perform the upgrade locally. Do not close or refresh this page during the upgrade process.
♦ System Config →	Otherwise, the upgrade may fall.
	Note: The file name cannot contain any Chinese or full-width character. Before the upgrade, verify that the target version matches the device model.
Cloud Management Platform	Version Info
🗐 Signature Library Upgrade	Current Version NGFW_NTOS 1.0R5, Release(03151320)
🗐 System Maintenance 🛛 🗸	Version Rollback. You can roll back toNGFW_NTOS 1.0R4, Release(03151401)
Device Info	Version Rollback
Device Positioning	Online Upgrade
Config Backup	Recommended Version Failed to connect to the server or obtain the version.
System Upgrade	Peconimience version Failed to connect to the server of opdam the version.
Patch Installation	Local Upgrade
Restart	Download Download Linkhttps://sectoud.rulije.com.cn
Defaults Restoration	Import Select an upgrade file. Browse Upgrade Now

(2) Check whether signature libraries (app identification signature library, IPS signature library, virus protection signature library, ISP address library, threat intelligence signature library) are of the latest version.

Ruffic Z Series Firewall	습 Home ④ Monitor ④ Network 유 Object ③ Policy ④ System	N	n c c c c c c c c c c c c c c c c c c c
Agdmin ∽	Signature Library Upgrade		
Admin Admin Role	Enable Auto Upgrade		
♦ System Config >	Upgrade Time:Daily 6 \lor Hour 4 \lor Minute		
Fault Diagnosis	Signature Library Select All App Identification Signature Library Threat Intelligence Signature Library	ep Scan) 🗾 Virus Protection Signature Library (Quick Scan) 🗾 Intrusion Preventi	on Signature Library 🗾 ISP Address Library
Signature Library Upgrade System Maintenance	Save		
	Signature Library Type		
	O Upgrade All (Upgrade all signature libraries online simultaneously.)		
	App Identification Signature Library	Virus Protection Signature Library (Deep Scan)	Virus Protection Signature Library (Quick Scan)
	Current Version/20230217.1245 Last Upgrade Time-	Current Version- Last Upgrade Time-	Current Version/20230309.0218 Last Upgrade Time-
	Latest Version: Unable to obtain the latest version.	Latest Version.Unable to obtain the latest version.	Latest Version: Unable to obtain the latest version.
	Version State-	Version State:	Version State:-
	Activation State:Activated	The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded	Activation State Activated
	Online Upgrade Local Upgrade system.versionRollback	Online Upgrade Local Upgrade	Online Upgrade Local Upgrade
	Intrusion Prevention Signature Library	ISP Address Library	Threat Intelligence Signature Library
	Current Version:20221026.1141	Current Version:20221202.1005	Current Version:20230308.1608
	Last Upgrade Time:2023-03-13 11:53:03 Latest Version:Unable to obtain the latest version.	Last Upgrade Time:- Latest Version Unable to obtain the latest version.	Last Upgrade Time:- Latest Venion Unable to obtain the latest version
	Version State:-	Version State:-	Version State:-
	Activation State Activated		Activation State Expired
đ	Online Upgrade Local Upgrade system versionRollback	Online Upgrade Local Upgrade	Online Upgrade Local Upgrade

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.

Ruffe Z Series Firewall	
🗐 Interface 🗸 🗸	Mode 🧿 Routing Mode 🔗 Transparent Mode 🔗 Off-Path Mode
Physical Interface	* Zone untrust \lor \odot Add Security Zone
Subinterface	Interface Type O WAN Interface O LAN Interface
Bridge Interface	Address
Aggregate Interface	
👰 Zone	IP Type IPv6
Harring >	Connection Type 🔿 Static Address 🔹 DHCP 🔿 PPPoE
🛅 SSL VPN >	Line Bandwidth
DNS	Uplink Select V
DHCP >	Downlink Select ~
link Detection	
L VRRP	Access Management
	Permit 🗹 HTTPS 🗹 PING 🗹 SSH
	Advanced
	ISP Address Library V
	① MTU 1500
	MAC 00:d0:f8:22:37:10 Restore Default MAC
	Link Detection V
프	Save
1	

- (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.

Ruijie Z Series Firewall	습 Home ਓ Monitor ⊕ Network ♀ Object ☞ Policy
Admin ∽	Web SSH Advanced Settings
Admin Role	Device Name RG-WALL * HTTPS Port 443
System Config System Time	* Login Timeout Period 1440
SNMP	(min)
Service Parameters Authorization Management	* Allowed Consecutive 6 Login Failures
In the second secon	* Lockout Period (min) 3
Cloud Management Platform	Verification Code 🔘 Enable 💿 Disable
🗐 Signature Library Upgrade 🕲 System Maintenance 🛛 🔿	Save Restore Defaults

• Limit on administrator login failures

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

Ruffe Z Series Firewall	습 Home 🛛 Monitor	•	₽_ Object	ନ୍ତ୍ର Policy	System	
🄏 Admin ∽	Web SSH	Advanced S	Settings			
Admin Admin Role	Device		ALL			
♦ System Config ✓	* HTTP					
System Time SNMP	* Login Timeout	Period 1440 (min)				
Service Parameters	* Allowed Conse	ecutive 6				
Authorization Management	Login F	ailures				
In a provide the second se	* Lockout Period	d (min) 3				
Cloud Management Platform	Verification	n Code 🔘 Enabl	e 🧿 Disa	ble		
🗑 Signature Library Upgrade 🔞 System Maintenance 🛛 >		Save	Restore	e Defaults		

(3) Management host settings

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

Ru	líjie ∣ ℤ Series Firewa	all	61	Home 🛛	Monitor	Network	ය ළ Object	C Policy	System			M Network Discovery	🚷 Network Mgmt	(L) Quick Onboarding	@ Policy Wizard	Customer Service	오 admir
	Security Policy $ ightarrow$	L	ocal	Defense													
	Port Scan Traffic Learning		Cre	eate 🔟 D	Delete	Enable	S Disable	Move	Z Local De	fense					Enter the	keyword.	
	NAT Policy >			Priority	Name		Src. Security	Zone Si	rc. Address	Dest. Address	Service	Action		Description		Operation	
	Security Defense~ DoS/DDoS Attack Defe			1	limit_loca	1	any	ar	vy	any	local_service,icmp,i.	permit		o the local device, b to 1500 pps per ho		Edit Delete	
	ARP Attack Defense			2	deny_all		any	ar	ıy	any	any	deny	Block all tra	ffic to the local devi	ce.	Edit Delete	
	Local Defense Threat Intelligence																
	Blocklist and Allowlist																
	Reputation Center SSL Proxy																

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.)

Ruíjie Z Series Firewall	🛆 Home	G Monitor	Network	,ዶ= Object	Policy	System			M Network Discovery	🚷 Network Mgmt	1 Quick Onboarding	Policy Wizard	Customer Service	오 admin
Security Policy ~	Policy Optin	nization												
Policy Config Wizard Security Policy Policy Optimization	Polic	y analysis intelligi	ently identifies polic	cy issues to prov	ride policy op	imization suggestions.	Analyze Policy Last analysis time:2023-03-1	3 19:32:48						
Policy Life Cycle Port Scan M Traffic Learning	Issue Policies		ies					Sele	ct the issue level.	∽ Select t	he issue type. $~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~$	Enter a p	olicy name.	
B NAT Policy >	Issue	Level		Issu	e Type 🔅				描述				Operation	
Ag Blocklist and Allowlist	🗌 🗸 all	ow_all											Ignore Handle	
 Reputation Center SSL Proxy > 	Majo	r Issue		f	王意权限		该策略允)	午任何源到任何	可目的数据包转发,权	限过大				
egy ssc Proxy 7														

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.
 - o The UTM security function is enabled.
 - o Abnormal traffic from attackers such as DDoS and broadcast storm exists.
- The possible causes for high memory usage are as follows:
 - o The output of the top command indicates that some processes consume high memory.
 - o 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.

Ruijie Z Series Firewall	습 Home 🛛 Monitor	letwork 🔑 Object	⊠ Policy	ම Syste	ም Network Discovery
∕⊗ Admin >	System Time				
♦ System Config × System Time	System Time Settings				
SNMP	Date	2023-03-14			
Service Parameters	Time	[©] 23:04:50			
Authorization Management	Time Zone	(UTC+08:00) Shangh	nai, Beijing, He	ong 🗸	
 Fault Diagnosis Cloud Management Platform 	Synchronization Settings				
🗐 Signature Library Upgrade		Auto Sync with Inter- Auto Sync with Inter-	ernet Time Se	rver	
⊗ System Maintenance >	Time Server			(time servers of the system: ntp.ntsc.ac.cn and ntp1.aliyun.com)
		Save			

(2) Check the license status to confirm that the purchased license for the upgrade service is still valid.

Ruijie Z Series Firewall		Monitor 4	Network		Policy ③ System		Net	work Discovery	🔕 Network Mgmt	Quick Onboarding	Policy Wizard	Customer Service	ad
🄏 Admin →	Authorizat	tion Mana	gement										
🗇 System Config 🛛 🗸													
System Time		cense Config	-										
SNMP						tform athttps://secloud1.ruijie.com.cn. On fal.)		Device Authoriza	tion page, and gen	erate a license file. The	account of this p	latform is	
Service Parameters	2.1	Select an activi	ation mode based	d on device connect	tion status.For threat in	telligence, only online activation is supp	orted.						
Authorization Management		Activate C	Online				You can cho	oose to perform	n manual activat	ion.			
⑦ Fault Diagnosis →		Activate	e Now				Activate	Manually				•	
D Cloud Management Platform													
🗑 Signature Library Upgrade	De	evice SN:MA	CC932672666	Сору									
System Maintenance	16	cense Info									How to Obtain	License	
		Performan	ce License								How to obtain	License	
												- 3G/3G	
	Av	vailable Perform	nance:3G(Basic Pe	erformance:1G+Add	ded New Performance:2	G) Performance to Be Added:0G							
		1 SSL VPN Li	icense										
	Ma	ax. Concurrent	License Sessions	25(25 concurrent fr	ee license sessions + 0 o	oncurrent purchased license sessions)							
	ê	Security Ca	apability Licens	e									
		No.	Security Ca	apability Name		Description	Lie	ense Type		5	tatus		
		1	App Ident	tification (APP)	It provid	es upgrade services for app identific ation signature libraries.	For	mal License		Activated (Expiry	Time:2024-03-	07)	
Ŧ		2	Intrusion P	Prevention (IPS)	It provid	es upgrade services for IPS signatur e libraries.	For	mal License		Activated (Explry	Time:2024-03-	07)	

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

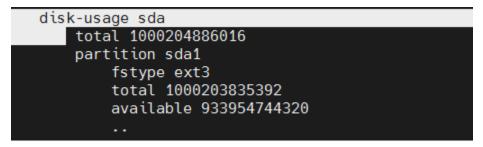
- Confirm that the customer has purchased a hard disk.
- If no hard disk is available, the Syslog server is configured.

Method

- (1) Check whether a hard disk is available.
- Log in to the web management page and choose **Monitor > Device Monitoring > Device Hardware Monitoring**.

Ruffie Z Series Firewall		G Monitor	Network					M Network Discovery	🚱 Network Mgmt	(Quick Onboarding	Ø Policy Wizard	ဂ Customer Service	오 admin
Security Cockpit	Device	Hardware	Monitoring										
Log Monitoring > Intelligence Overview	Device	Hardware U	sage										
Traffic Monitoring	🖸 Refr	esh								D	splay Cycle	Recent 1 Hour	~
Device Monitoring		Usage											
	100%												
	80%												
	40%				<u> </u>								
	20%												
	0%						22.42						
		22:10		2	2:20	22:30	22:40		22:50		23:00		

• Run the firewall> show state system linux command in the CLI.



(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**.

Ruijie Z Series Firewall		(۹۹) Network Discovery	😡 Network Mgmt	
l Security Cockpit	Syslog Server			
➡ Log Monitoring × System Log Security Log	① The syslog protocol can be used to send firewall logs to a third-party log analysis platform for unified storage, analysis, and processing.Note:When the fast sys bandwidth and affect existing network services. Please operate with caution.			
URL Log	Fast Syslog Forwarding			
Operation Log SSL VPN Log	Syslog Server1 Syslog Server2			
Session Log	* Server IP Enter an IP address.			
Syslog Server	* Port 514			
Traffic Monitoring >	* public.stand • rfc3164			
@ Device Monitoring >	rsion			
	启用该Syslog服务器的日志类型 Create * 日志类型 Select a syslog log type.			
	Save			

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.

Ruffe Z Series Firewall	습 Home 🛛 Monitor 🌐 Network 🔑 Object 🖾 Policy 😟 System
Admin >	Ping
♦ System Config > I ault Diagnosis >	Diagnostic Parameters
Diagnostic Center	Src. Type 💿 Src. IP 🔷 Src. Port
Device Self-Test	Src. IP Enter the source IPv4 or IPv6 address.
Ping	* Dest. IP/Domain Name Enter the destination IPv4 or IPv6 addre:
Tracert	Ping CountEnter the count. Range: 1–10.
Packet Obtaining Tool One-Click Collection	Packet Length Enter the packet length. Range: 0–1500.
Cloud Management Platform	Diagnose
🗐 Signature Library Upgrade	Diagnostic Result
囫 System Maintenance →	$\overline{\mathbb{C}}$

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.