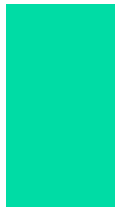
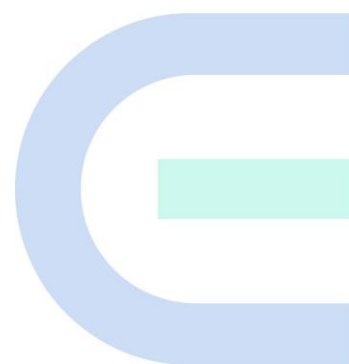


RG-WALL 1600-Z-S Series Cloud-Managed Firewall

FAQs



Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

Without the prior written consent of Ruijie Networks, any organization or individual shall not reproduce, extract, back up, modify, or propagate the content of this document in any manner or in any form, or translate it into other languages or use some or all parts of the document for commercial purposes.

 ,  ,  and other Ruijie network logos are trademarks of Ruijie Networks.

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

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to the content of this document.

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

This manual is designed merely as a user guide. Ruijie Networks has tried its best to ensure the accuracy and reliability of the content when compiling this manual, but it does not guarantee that the content of the manual is completely free of errors or omissions, and all the information in this manual does not constitute any explicit or implicit warranties.

Preface

Intended Audience

This document is intended for:

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

Technical Support

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

Conventions

1. Signs

This document also uses signs to indicate some important points during the operation. The meanings of these signs are as follows:

Warning

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

Caution

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

Note

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

Specification

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

2. Instruction

This manual provides installation steps, troubleshooting, technical specifications, and usage guidelines for cables and connectors. It is intended for users who want to understand the above and have extensive experience in network deployment and management, and assume that users are familiar with related terms and concepts.

Contents

Preface	1
1 Product Overview	3
1.1 What Is the Hardware Architecture of the RG-WALL 1600-Z-S Series Firewall?	3
1.2 What Firewall Deployment Modes Are Supported?	3
2 Device Management	7
2.1 Can the Z Series Firewalls Be Managed on Ruijie Reyee App?	7
2.2 What Are the Restrictions of Port MGMT?	7
2.3 Can 10GE Optical Ports on the Firewalls Be Connected to GE Optical Ports on Other Devices?	7
2.4 Can GE Optical Port and 10GE Optical Port Form a Bridge?	7
3 Function Configuration	8
3.1 What Are the Principles of Security Policies?	8
3.2 What Are the Key Configuration Points of Security Policies?	8
3.3 What Are the Application Scenarios of the Simulation Run of Security Policies? How to Configure Simulation Run?	9
3.4 How Is Source NAT Implemented?	9
3.5 Does the Firewall Support Link Detection?	9
3.6 Does the Z-S Series Firewall Block TCP Sessions in the Secondary Traversal Scenario? ...	10
3.7 Does the Firewall Support Port Aggregation?	10
3.8 How Do I View the CPU, Memory, and Hard Disk Information of the Firewall?	10
3.9 How Do I View the Interface Traffic of the Firewall?	10
3.10 Is IPsec VPN Supported?	10
3.11 What Is Traffic Learning? What Functions Does It Provide?	10

3.12 What Is Port Scan? What Functions Does It Provide? Are Ports Using IPv6 Addresses Supported?	11
3.13 What Is Diagnostic Center? What Functions Does It Provide?.....	11
4 Product License.....	12
4.1 Does the Product License Have a Validity Period? How Long Is the Validity Period? How to Calculate It?	12
4.2 Is There Any Compensation for Expired Licenses? What Is the Compensation Mechanism? What Are the Specific Operations?	13
5 Troubleshooting.....	15
5.1 The Firewall Goes Online Through Quick Onboarding, but Is Not Displayed on Ruijie Reyee App.....	15
5.2 What Can I Do If I Fail to Log In to the Web Page?	15
5.3 What Can I Do If I Fail to Log In to the System Through SSH?	16
5.4 Why Is the Threat Intelligence Function Enabled, but the Status Is Unauthorized?.....	16
5.5 Session Logs of the Z-S Series Firewall Are Not Displayed	16

1 Product Overview

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 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.

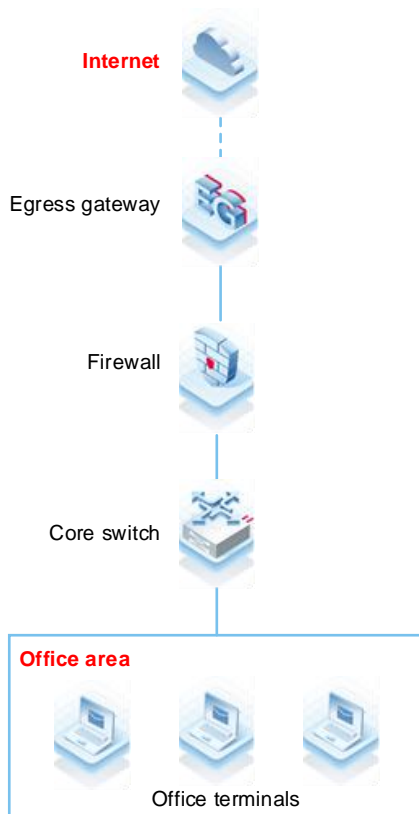
The overall hardware design adopts the area-based power solution to avoid whole machine restart caused by short circuit of the USB drive or optical module.

1.2 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:

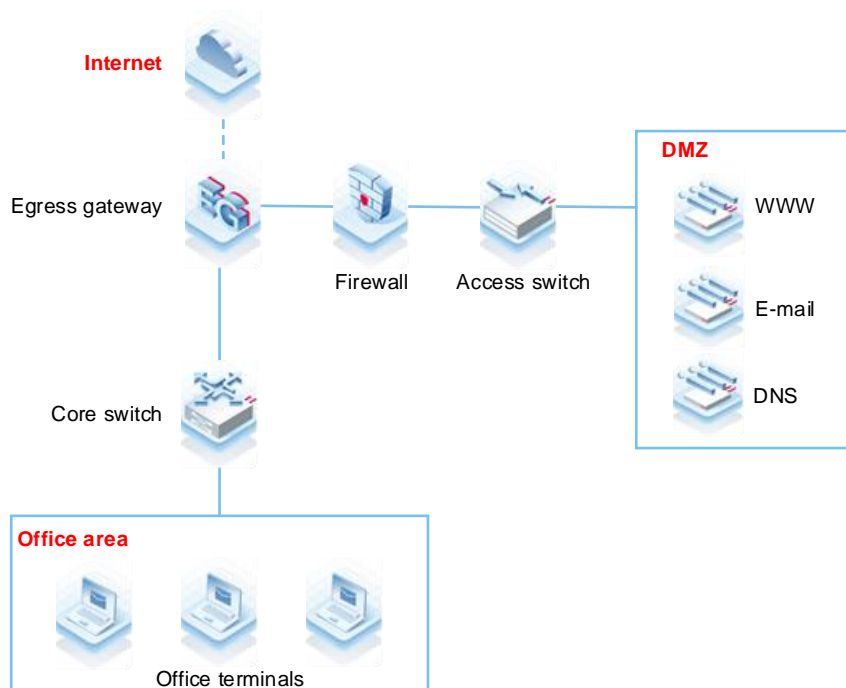
- Transparent mode - office network egress link - single-in single-out

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.



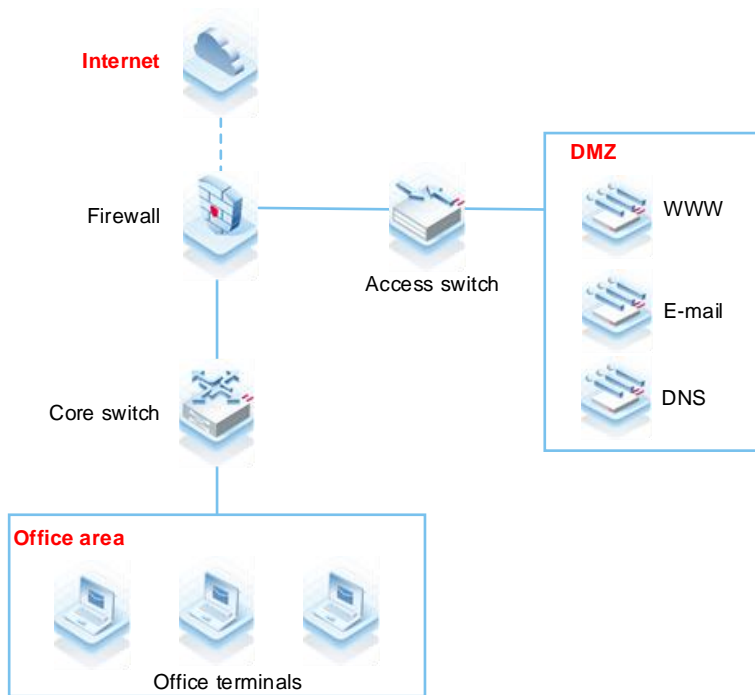
- Transparent mode – area boundary - single-in single-out

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.



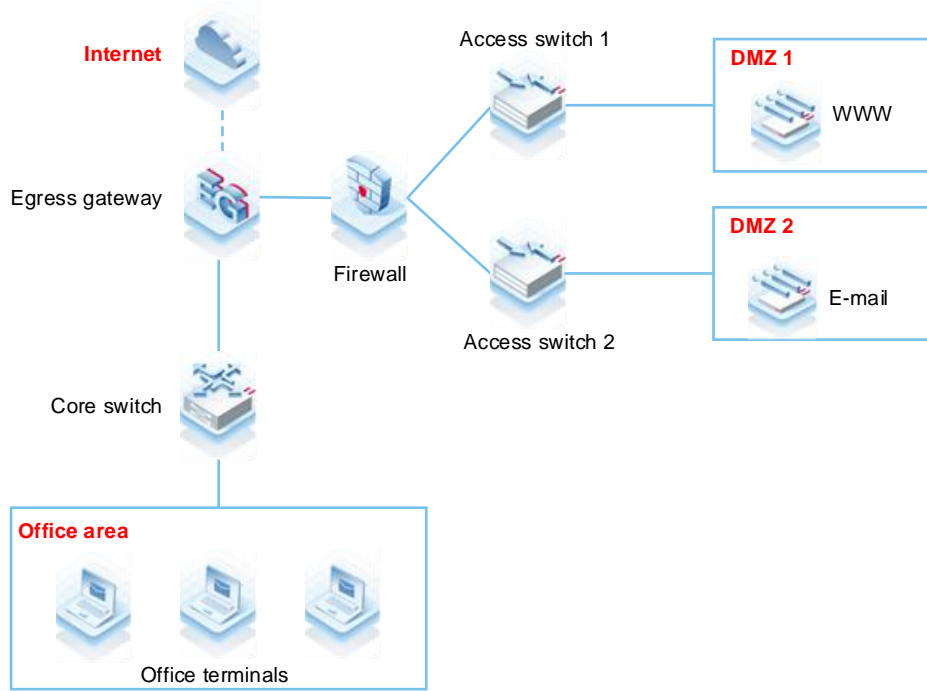
- Gateway mode - single ISP access

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

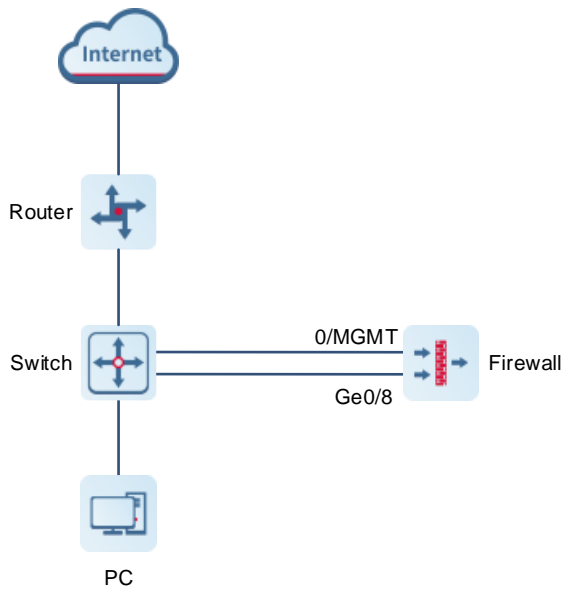
Scenario overview: The firewall is transparently deployed on the network. It connects to the LAN areas through multiple ports and connects to the Internet through the same WAN port to provide services to external users.



- Off-path mode

Scenario overview: The firewall is connected to the switch in off-path mode, and traffic of the switch is mirrored to the off-path interface on the firewall for detection. In this mode, the firewall can monitor the security of a customer network without changing the network structure or affecting data forwarding.

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



2 Device Management

2.1 Can the Z Series Firewalls Be Managed on Ruijie Reyee App?

Ruijie Reyee App only supports the management of the Z-S series firewalls of NGFW_NTOS 1.0R3 or later. Currently, the app only supports the topology and interface information display of the Z-S series firewalls. In the future, more firewall O&M functions on Ruijie Reyee App will be updated in later versions.

2.2 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.

2.3 Can 10GE Optical Ports on the Firewalls Be Connected to GE Optical Ports on Other Devices?

In NGFW_NTOS 1.0R3 and earlier versions, 10GE optical ports are not backward compatible and cannot be connected to GE optical ports, and the rates of ports on both ends must be the same.

In NGFW_NTOS 1.0R4 and later versions, 10GE optical ports are backward compatible.

2.4 Can GE Optical Port and 10GE Optical Port Form a Bridge?

The GE optical port and 10GE optical port can form a bridge.

3 Function Configuration

3.1 What Are the Principles of Security Policies?

- (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 application layer service processing on the permitted data flows.
- (3) Application layer 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.

3.2 What Are the Key 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.

3.3 What Are the Application Scenarios of the Simulation Run of Security Policies? How to Configure Simulation Run?

Application Scenario

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

Z-S series firewalls provide a virtual space of policy simulation run for O&M personnel to verify and test policy modifications. This space does not affect the services in the real network environment. That is, the security policies in the simulation space will not permit or block real service traffic.

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

Procedure

- (1) Choose **Policy > Security Policy > Security Policy**.
- (2) Click **Simulation Space** in the upper right corner of the operation area.
- (3) Select the policy for which simulation run will be performed, and click **Start Simulation**.
- (4) On the **Set Simulation Duration** page, set the duration of simulation run.
- (5) Click **Start Simulation**.

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.

3.4 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.

3.5 Does the Firewall Support Link Detection?

The firewalls running NGFW_NTOS1.0R3 and later versions support link detection.

3.6 Does the Z-S Series Firewall Block TCP Sessions in the Secondary Traversal Scenario?

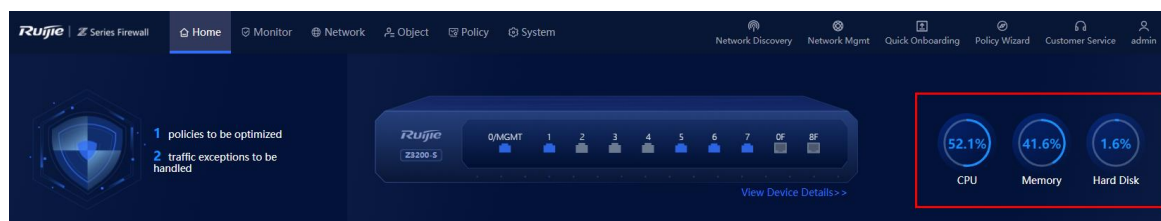
No. However, if the same packet flow traverses the firewall for a second time, secondary authentication of SYN-Cookie will be triggered if SYN flood attack defense (DDoS attack defense) is enabled, causing TCP connection setup failure.

3.7 Does the Firewall Support Port Aggregation?

The firewalls running NGFW_NTOS1.0R4 and later versions support port aggregation.

3.8 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.



3.9 How Do I View the Interface Traffic of the Firewall?

Log in to the web management page, choose **Monitor > Traffic Monitoring > Traffic Monitoring > Interface Traffic Statistics**, and view the interface traffic.

3.10 Is IPsec VPN Supported?

Currently, the firewalls do not support IPsec VPN. In V5.2-NGFW_NTOS1.0R5 and later versions, SSL VPN is supported.

3.11 What Is Traffic Learning? What Functions Does It Provide?

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.

3.12 What Is Port Scan? What Functions Does It Provide? Are Ports Using IPv6 Addresses Supported?

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.

Currently, ports using IPv6 addresses are not supported.

3.13 What Is Diagnostic Center? What Functions Does It Provide?

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.

4 Product License

4.1 Does the Product License Have a Validity Period? How Long Is the Validity Period? How to Calculate It?

All licenses for the RG-WALL 1600-Z-S series firewalls have a validity period. The licenses can be divided into perpetual licenses and licenses with an expiry date.

- Perpetual license: After purchasing a license, you can activate it at any time. The corresponding functions are permanently available after the license is activated.
- License with an expiry date: After purchasing a license, you need to activate it before the license activation deadline (within 1 year from the license delivery date). Otherwise, the days will be deducted from the validity period.

For licenses with an expiry date, the formula for calculating the license validity period is as follows: $V = M \times 365 - N$.

- V: Remaining validity period (day)
- M: Number of licenses of the same type
- N: Duration deducted from the validity period (day). If the license is activated before the activation deadline, $N = 0$ (that is, no time is deducted). If it is activated after the activation deadline, $N = \text{Actual activation date} - \text{Activation deadline}$.

 Note

For licenses of different types, the validity periods need to be calculated separately.

The following describes four cases.

Case 1: One License for One Device

- License type: RG-WALL 1600-Z3200-S-AV-LIS-1Y (virus protection license for the RG-WALL 1600-Z3200-S that provides virus protection and one-year AV signature library upgrade service per license)
- License validity period: 1 year

Type	Quantity (M)	Activation Deadline	Actual Activation Date	Deducted Validity Period (N) (Actual Activation Time – Activation Deadline)	Remaining Validity Period (V)
AV	1	2023-05-01	2023-10-01	153 days	$1 \times 365 - 153 = 212$ days

Case 2: Licenses of One Type for One Device

- Licensed type: RG-WALL 1600-Z3200-S-AV-LIS-1Y (purchased quantity: 3)
- License validity period: 1 year

Type	Quantity (M)	Activation Deadline	Actual Activation Date	Deducted Validity Period (N) (Actual Activation Time – Activation Deadline)	Remaining Validity Period (V)
AV	3	2023-04-01	2023-10-01	N1 = 183 days	3 x 365 – Max(N1,N2,N3) = 912 days
AV		2023-04-01	2023-10-01	N2 = 183 days	
AV		2023-05-01	2023-10-01	N3 = 153 days	


 Caution

If multiple licenses are of the same type, the maximum value among all deducted validity periods should be used for calculation.

Case 3: Licenses of Multiple Types for One Device

- Licensed type: RG-WALL 1600-Z3200-S-AV-LIS-1Y (purchased quantity: 2); RG-WALL 1600-Z3200-S-IPS-LIS-1Y (purchased quantity: 2)
- License validity period: 1 year

Type	Quantity (M)	Activation Deadline	Actual Activation Date	Deducted Validity Period (N) (Actual Activation Time – Activation Deadline)	Remaining Validity Period (V)
AV	2	2023-04-01	2023-10-01	N1 = 183 days	2 x 365 – Max(N1,N2) = 547 days
AV		2023-05-01	2023-10-01	N2 = 153 days	
IPS	2	2023-03-01	2023-10-01	N3 = 214 days	2 x 365 – Max(N3,N4) = 516 days
IPS		2023-04-01	2023-10-01	N4 = 183 days	

 Caution

If multiple licenses are of the same type, the maximum value among all deducted validity periods should be used for calculation.

Case 4: Multiple Licenses for Multiple Devices

The validity period of the license for each device is calculated separately in the same way as for a single device.

4.2 Is There Any Compensation for Expired Licenses? What Is the Compensation Mechanism? What Are the Specific Operations?

There is no compensation for expired licenses. If you have any questions, please contact Ruijie technical support.

For details on how to calculate the validity period, see 4.1 Does the Product License Have a Validity Period?
How Long Is the Validity Period? How to Calculate It?.

5 Troubleshooting

5.1 The Firewall Goes Online Through Quick Onboarding, but Is Not Displayed on Ruijie Reyee App

Possible Causes

- The firewall fails to deliver the security policy.
- An exception occurs on Ruijie Cloud.
- A network error occurs.

Troubleshooting Procedure

- (1) After quick onboarding, the firewall automatically delivers a security policy **allow_trust_to_untrust**. Log in to the firewall web page, and choose **Policy > Security Policy > Security Policy**. On the page that is displayed, check whether the policy has been generated and enabled.
- (2) Ping the domain name of Ruijie Cloud to check whether Ruijie Cloud is working properly. If so, log in to the firewall web page, and choose **Network > DNS**. On the page that is displayed, check whether the address of the DNS server of the firewall is 8.8.8.8. If not, the firewall cannot resolve the domain name of Ruijie Cloud and fails to go online.
- (3) If the network connection between the firewall and Ruijie Cloud is interrupted, you need to troubleshoot the network error hop by hop. If the firewall can connect to Ruijie Cloud, but other devices connected to the firewall cannot connect to Ruijie Cloud, check whether firewall interfaces, security zones, security policies, NAT policies, and other configurations are correct.

5.2 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.

Troubleshooting Procedure

- (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.

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

Possible Causes

The SSH port number is incorrect.

Troubleshooting Procedure

- (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.

The screenshot shows the SSH configuration page. The 'SSH' tab is active. The 'SSH Port' field is highlighted with a red box and contains the value '22'. The 'Allowed Consecutive Login Failures' field contains '3', and the 'Lockout Period (min)' field contains '1'. There are 'Save' and 'Restore Defaults' buttons at the bottom.

5.4 Why Is the Threat Intelligence Function Enabled, but the Status Is Unauthorized?

Possible Causes

The threat intelligence (TI) license is not activated.

Troubleshooting Procedure

- (1) Log in to the firewall web page.
- (2) Choose **System > System Config > Authorization Management**. On the page that is displayed, check whether the TI license is activated and within the validity period.

If the TI function is not authorized or authorization expires, the detection based on the 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.

5.5 Session Logs of the Z-S Series Firewall Are Not Displayed

The possible causes are as follows:

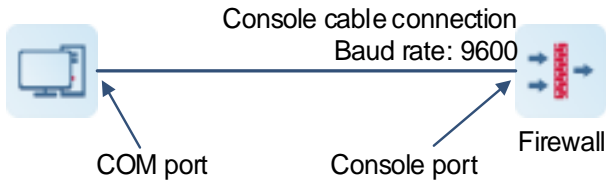
- (1) No hard disk is installed.


Solution: Purchase and install a hard disk. For details about hard disk installation, see *RG-WALL 1600-Z3200-S Cloud Management Firewall Hardware Installation and Reference Guide*.

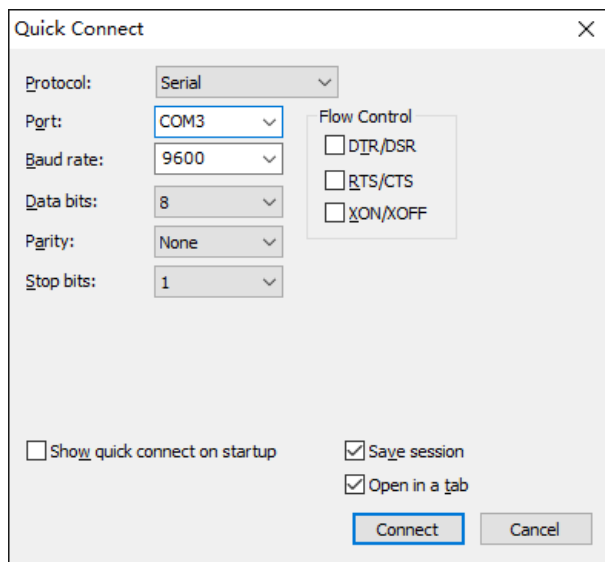
- (2) The session log function is not enabled for the firewall.

Solution: The session log function is enabled by default. If session logs are not displayed with a hard disk installed, you need to enable the session log function on the CLI. The procedure is as follows:

- a Log in to the firewall through the console port:



- 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, configure connection parameters according to the following figure and click **Connect**.



Note

Select the COM port as required. If a PC has only one COM port, it is displayed as COM1 by default.

- c Press **Enter** and enter the username and password (for example, the default values **admin/firewall**) as prompted.

```
Sent SIGKILL to all process
Switching rootfs

Welcome to NTOS
Z3200-S login: admin
Password:
Please wait a moment while the system is initializing..
.....
```

- d After successful login, run the following command to check whether the session log function is enabled on the firewall.

```
Z3200-S> show congfig running system collect
collect
  enable true
  max-records 3072
  record-interval 200
  memory-storage-threshold 90
  statistics-enabled false
  flow-log-enabled true //false indicates that the session log function is
not enabled. In this case, run the flow-log-enabled true command to enable it.
  log-language Chinese
..
Z3200-S>
```