RG-WALL 1600 Next-Generation Firewall Routine Maintenance and Troubleshooting

Applicable to V5.2-R5.0

Contents

Preface

Audience

Ruijie business partners and customers who are responsible for configuring and maintaining Ruijie wireless devices.

Revision Record

Release Date	Change Contents	Reviser
2016.06	Initial publication V1.0	TAC Oversea

Note :

For more detail configuration , see configuration guide for each product . you can download configuration guide at http://www.ruijienetworks.com

For more technical enquiry , you can visit Ruijie Service portal at http://case.ruijienetworks.com . You need to sign up before submit a case.

Contents

Routine Maintenance Suggestions

System > Dashboard > Status (homepage)

Maintenance of the CPU, memory, and disks

Log in to the Web management interface and view the usage of the CPU, memory, and disks on the homepage.

CPU usage:

Normally, CPU usage is lower than 80%. If CPU usage remains above 80% for a long time, check the device and analyze the cause.

Memory usage:

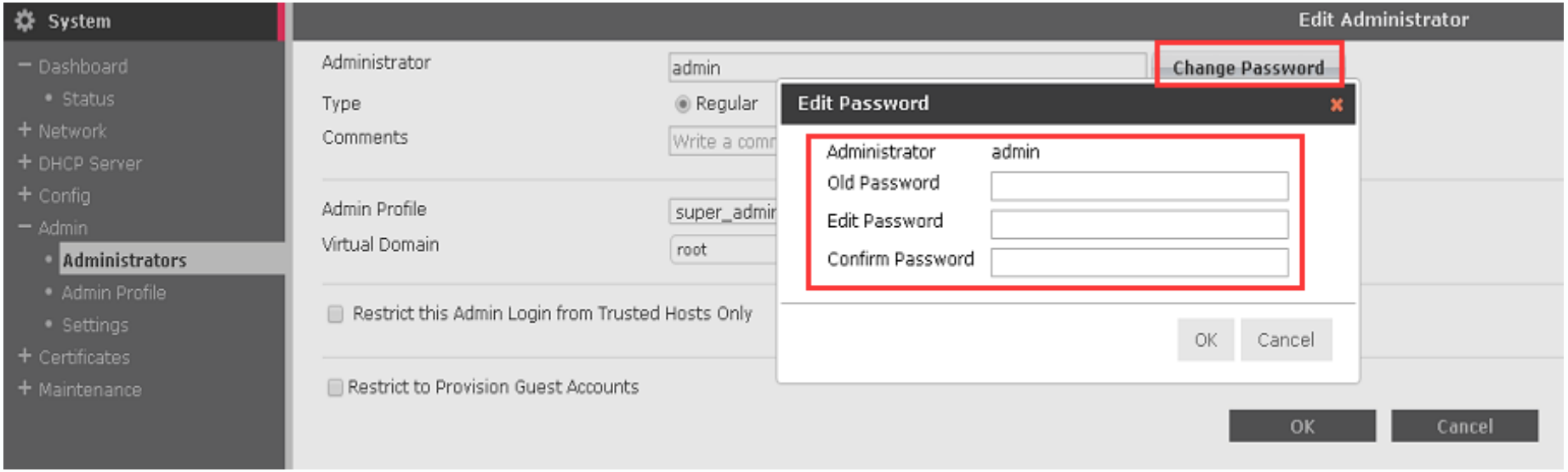
Normally, memory usage is lower than 80%. If memory usage remains above 80% for a long time, check the device and analyze the cause.

Disk usage:

Normally, disk usage is lower than 90%. If the free capacity of disks is too small, check the device and clean up the disks.

Changing the Administrator Password

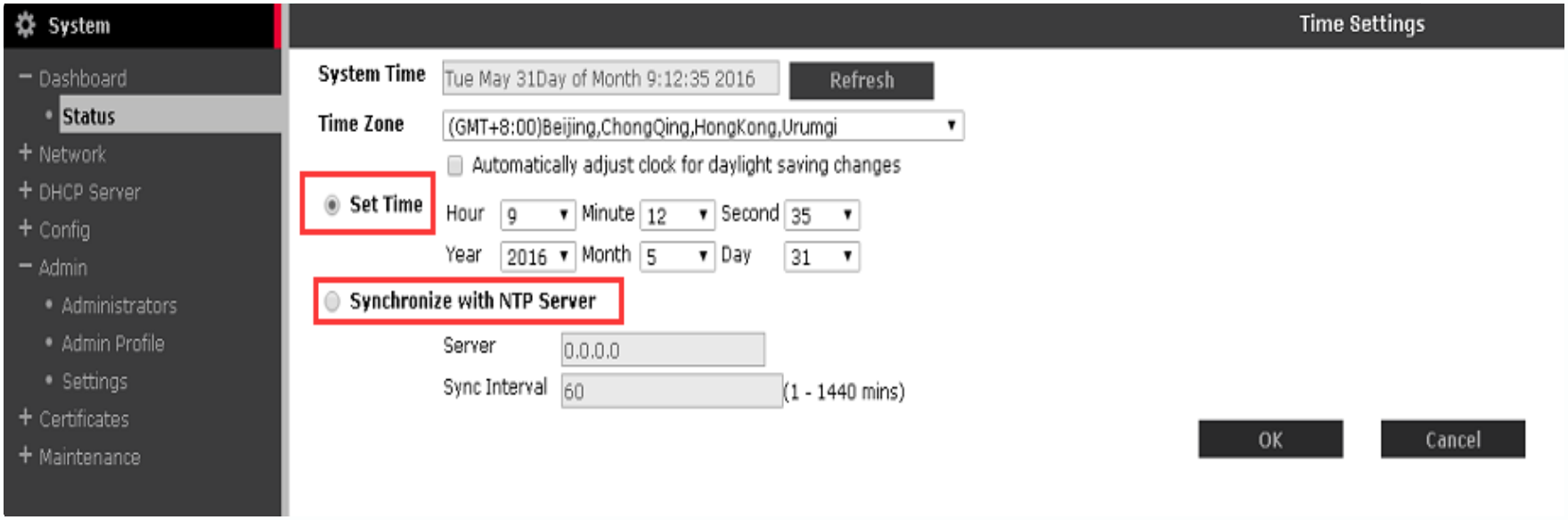
The default administrator account is **admin** and the default password is **firewall**. After the device is put into operation, the default password must be changed to ensure system security and user information confidentiality. It is recommended that the password contain more than six characters, meet complexity requirements, and be changed periodically. Choose **System** > **Admin** > **Administrators**. Select **admin** and click **Edit** to change the administrator password.



Routine Maintenance Suggestions – Setting the System Time

Setting the system time

Open the homepage and view the system time and date, which should be consistent with the local time or the NTP time. To change the system time, choose **System** > **Dashboard** > **Status** > **Set Time**. You can change the system time manually or set it to be synchronized with the time of the NTP server.



Contents

Handling of Common Faults – Failed to Manage the Device

Symptom:

After the IP address of an interface is configured, the IP address cannot be used to manage the device via Web.

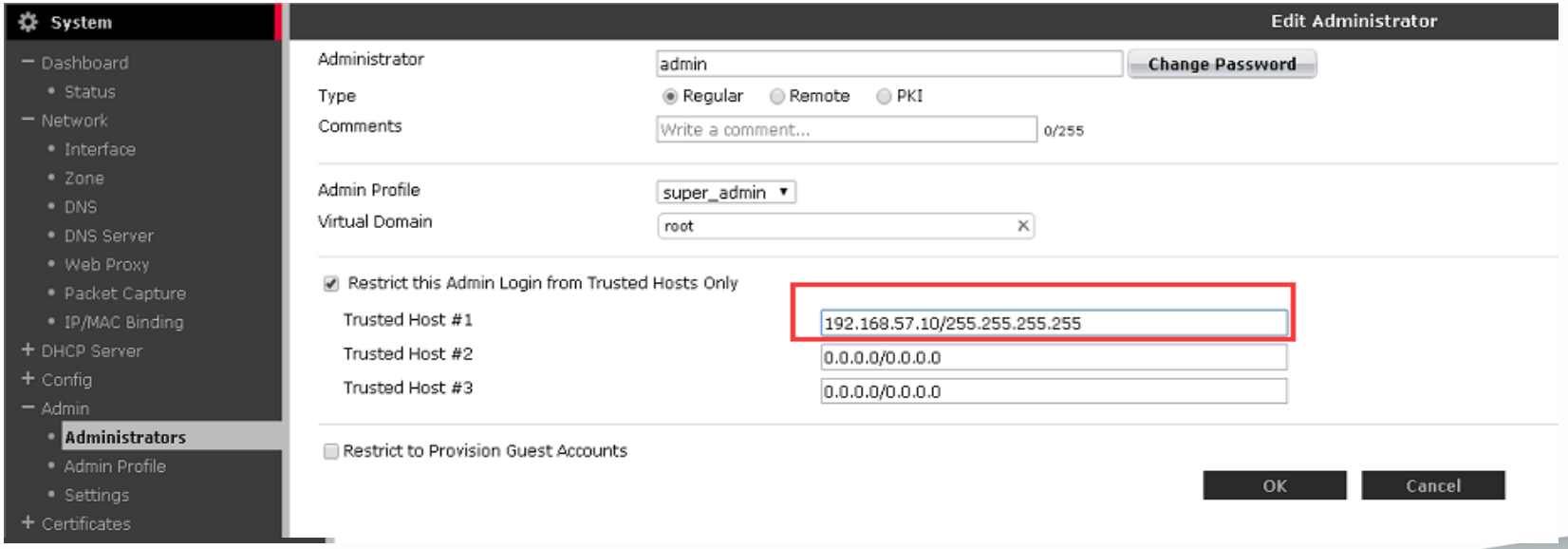
Possible causes:

- The network is unreachable.
- The interface is not enabled with the HTTP/HTTPS management authority.
- The IP address of the management client is not within the trusted management IP address range.

Solution:

- Check the involved physical line, physical interface, IP address, and route.
- Choose **System** > **Network** > **Interface**. On the **Edit Interface** page, select **HTTP** or **HTTPS** for **Manage Access**.
- Choose **System** > **Admin** > **Administrators**. On the **Edit Administrators** page, add the IP address of the management client to the trusted management IP address range.

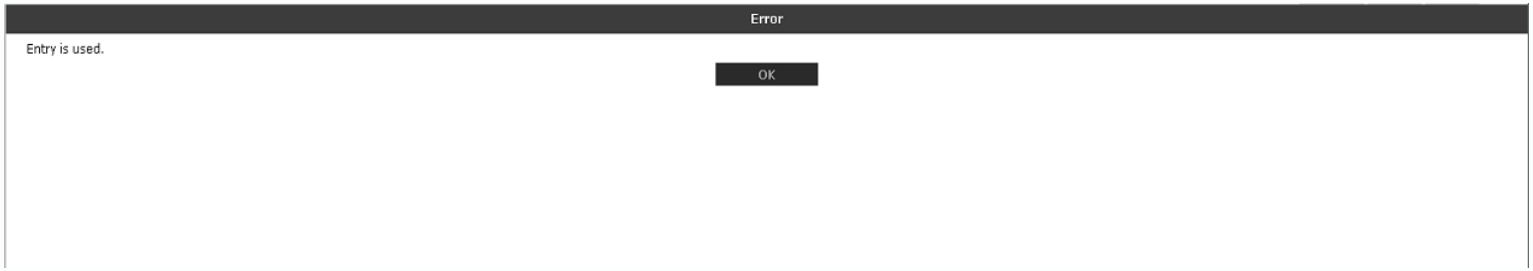
Remarks: If the problem persists, please contact the online customer service http://www.ruijienetworks.com for help.



Handling of Common Faults – Failed to Delete Address Objects and Interfaces

Symptom:

When an address object or interface is deleted, the system prompts " Entry is uesed."



Possible causes:

The address object to be deleted is referenced by a policy.

The interface to be deleted is referenced by a policy, DHCP, or route.

Solution:

Cancel the reference or delete the referencing policy.

Handling of Common Faults – Address Mapping Failed

Symptom:

External users cannot access the internal mapped services normally.

Possible causes:

- The port used to access the services is disabled by the operator.
- The port is blocked by the server system firewall (in this case, internal users cannot access the services either).
- The internal and external interfaces selected for the firewall policy are inconsistent with the actual interfaces.
- Some ports are not mapped.

Solution:

- Modify the external mapped port and contact the operator to enable the port.
- Disable the server system firewall.
- Modify the firewall policy, select the correct interfaces, and map complete ports.

Handling of Common Faults – Application Periodically Interrupted

Symptom:

An Oracle database application is periodically interrupted. The application can start running again after reconnection.

Possible causes:

The firewall imposes a session timeout limit. It will release a session if no data is transmitted within the timeout time.

The default timeout time is 3,600s.

If data is transmitted before the timeout time has elapsed, the ttl timer of the session is reset to the value of the timeout time (such as 3,600s). Some services such as databases require long connections. If no data is transmitted within 3,600s, the connection will be disconnected and the application is interrupted. In this case, you need to manually set up a connection again in order to restart the application.

Solution:

- Modify the firewall policy to increase the value of the ttl session timer. The maximum value is 7 days (604,800s).
- You can also set the value of the global ttl session timer or the ttl session timer for the specified service port. The priorities of different ttl session timers are as follows:

Global ttl session timer < ttl session timer for the specified service port < ttl session timer specified in the firewall policy < ttl session timer for service objects

Low **High**

Contents

Restoration of Factory Defaults

Configuration file backup

Back up the configuration file before you perform important operations or restore to factory defaults. Choose **System** > **Dashboard** > **Status**, click **Backup**, and enter the correct password to export and back up the current system configuration.

Restoration of Factory Defaults

Restoring to factory defaults

The restoration of factory defaults must be performed on the command line interface (CLI). Connect to the device through the console port or via telnet, enter the CLI, run the **execute factoryreset** command, and type **y** after the prompt.

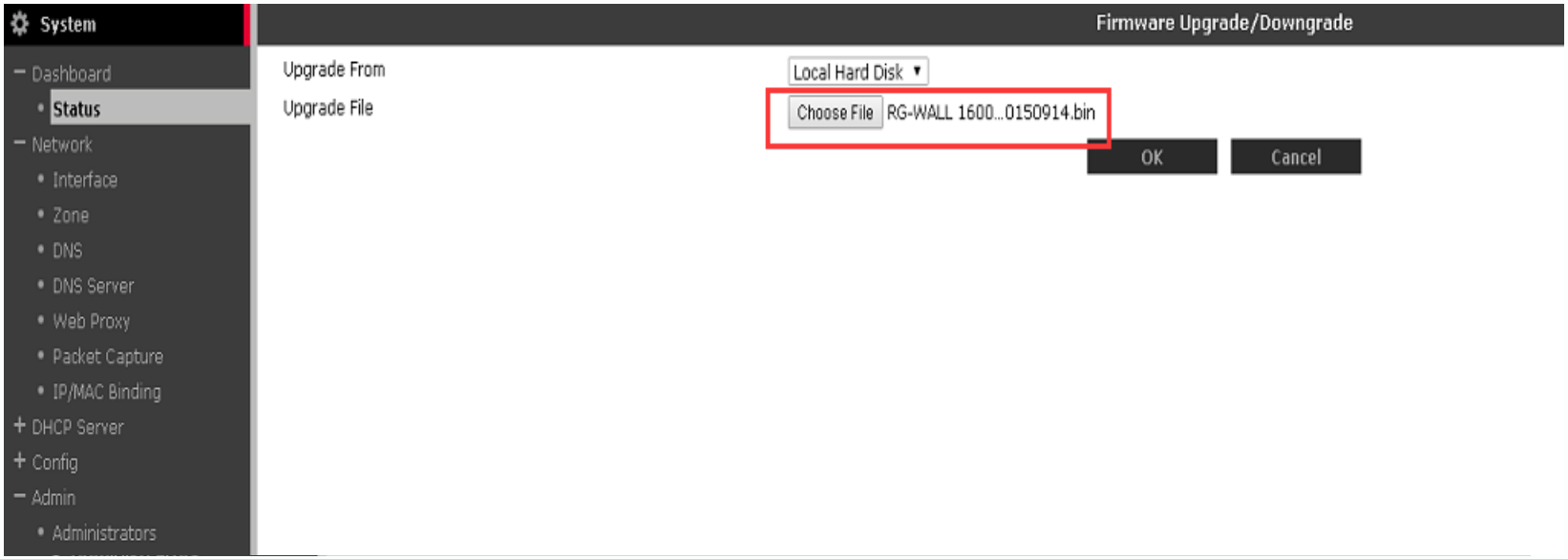
```
RG-WALL login:

RG-WALL login: admin
Password: ********
Welcome !

RG-WALL # execute factoryreset
This operation will reset the system to factory default!
Do you want to continue? (y/n)y


System is resetting to factory default...


The system is going down NOW !!

RG-WALL #
Please stand by while rebooting the system.
Restarting system.
```

Contents

Software Version Upgrade

Upgrading the software version

- Choose **System** > **Dashboard** > **Status**, click **Upgrade**, upload the local version file, and click **OK**.
- Because the device needs to be restarted after upgrade, perform the upgrade when network disconnection is allowed. The upgrade lasts about 5 minutes.



Contents

System resource usage

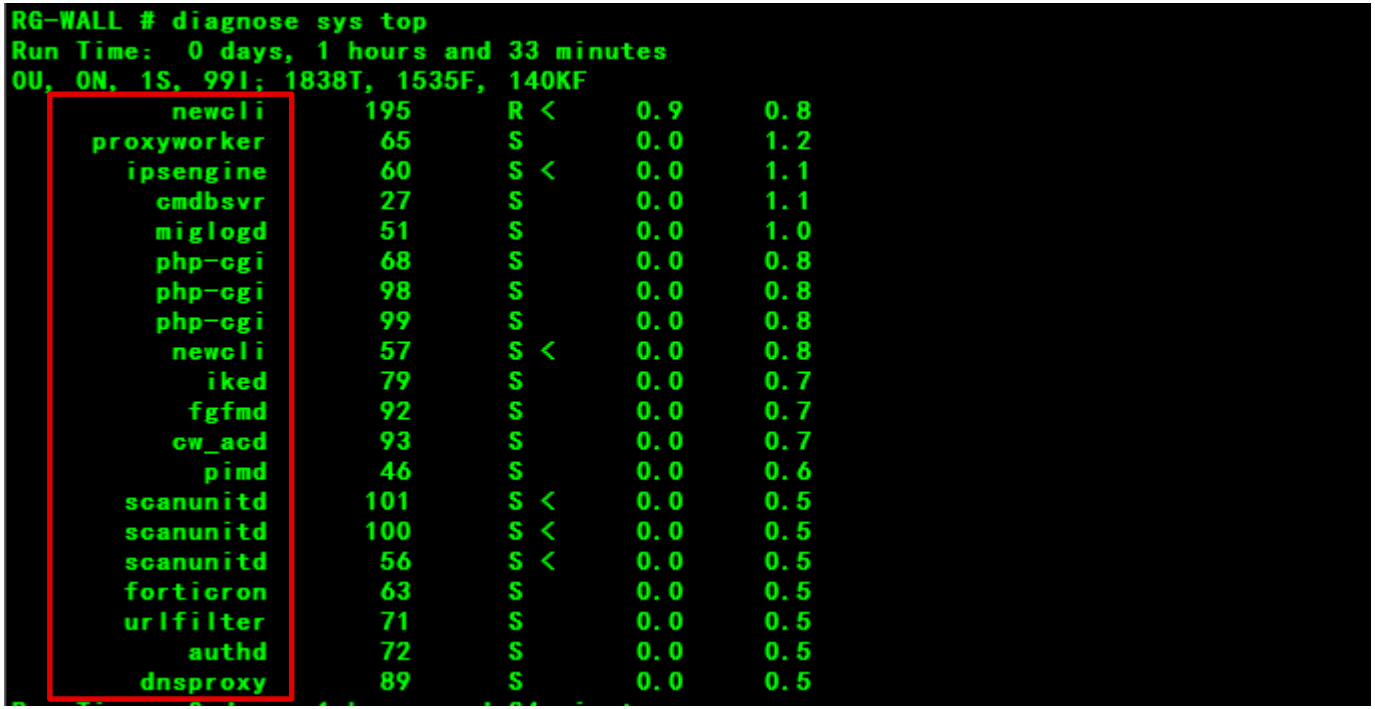
Run the **get system performance status** command on the CLI to view the details about the CPU usage, memory usage, sessions, and runtime.

```
RG-WALL # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle
CPU0 states: 0% user 0% system 0% nice 100% idle
Memory states: 16% used
Average network usage: 10 kbps in 1 minute, 108 kbps in 10 minutes, 73 kbps in 30 minutes
Average sessions: 1 sessions in 1 minute, 20 sessions in 10 minutes, 79 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 0 days, 1 hours, 21 minutes
```

Enter this command.

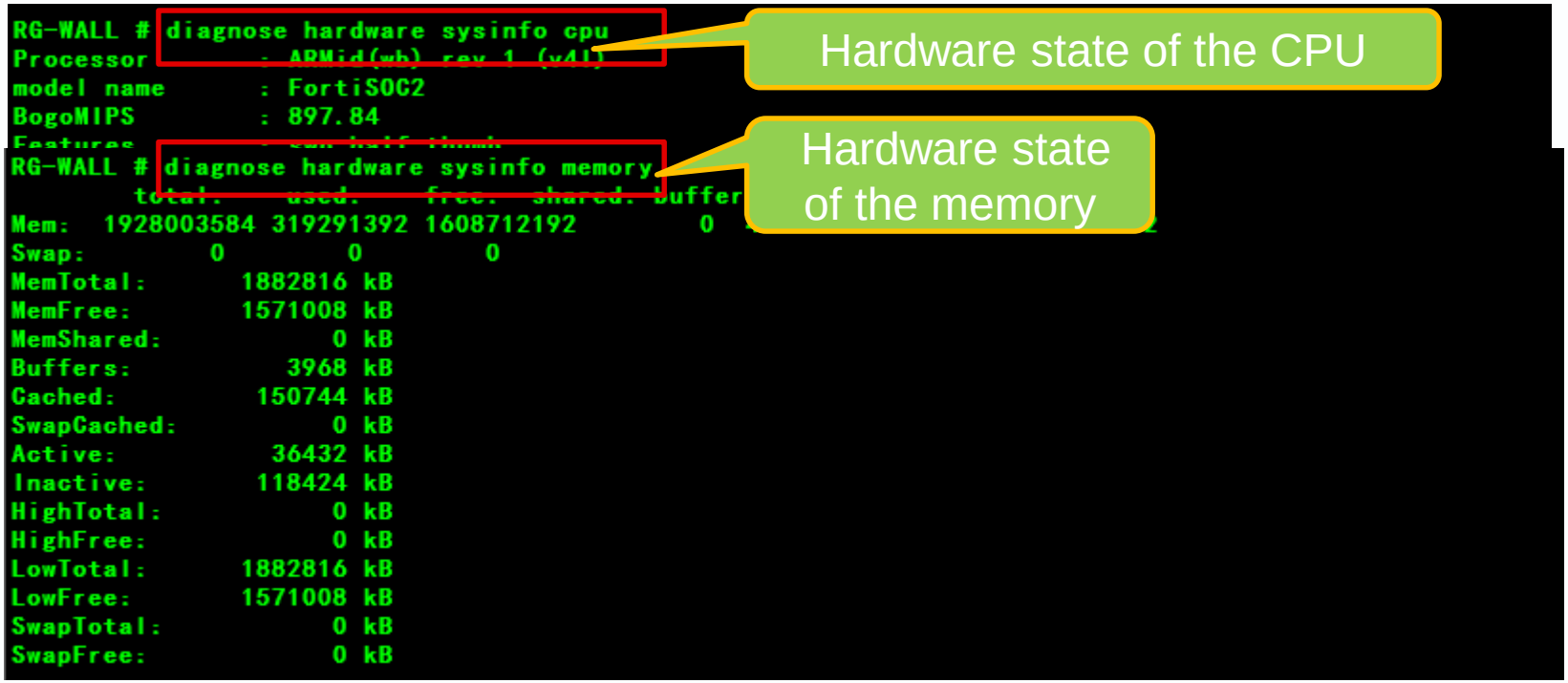
Process resource usage

Run the **diagnose sys top** command on the CLI to view the details about the CPU usage and memory usage of system processes.



Hardware status

Run the **diagnose hardware deviceinfo** command on the CLI to view the hardware states of the CPU, memory, and network interface card (NIC).



Detection of network communication failures——ARP table

Run the **get sys arp** command on the CLI to view the ARP table and the interface mapping relationship.

View the ARP table:

```
RG-WALL # get system arp
Address           Age(min)    Hardware Addr       Interface
192.168.1.99      0           28:d2:44:66:b2:f7 internal
192.168.57.1      0           00:00:5e:00:01:39 wan2
```

Clear the ARP cache:

```
RG-WALL # execute clear system arp table

RG-WALL #
```

Fault Diagnosis

Detection of network communication failures——Tracking data

When a data communication failure occurs, you can locate the cause by checking the session table and data flow forwarding information and using a packet capture tool to capture and analyze packets.

Which method to use depends on the characteristics of the data involved.

- Command used to check the session table: **RG-WALL # diagnose system session**

  Run this command to list all ongoing sessions. You can filter the sessions based on specified criteria, and view information such as the session setup time and timeout time, as well as the corresponding policy ID.

- Command used to check the data flow forwarding information: **RG-WALL # diaggnose debug flow**

  Run this command to track packet processing. You can view how a packet is processed by each function module and how it is forwarded or discarded.

- Command used to capture packets: **RG-WALL # diag sniffer packet**

  Run this command to view the detailed content of a packet and the fields of the packet header. You can filter the TCP flag and the packet header at Layer 2, Layer 3, and Layer 4. You can open the exported file by using Wireshark or other tools.