RG-WALL 1600 Series Next-Generation Firewall Troubleshooting Guide V1.1

Revision History

Revision	Date Revised	Description
1.0	20180620	First Release
1.1	20180718	Added FAQ in Web Filter

Contents

1 Product Function Related

Function \ Model	S3100	S3600	M5100	M6600	X9300
Reset Button	Y	Y	N	N	N
Console Port	N	N	Y	Y	Y
Bypass Port	N	N	N	N	N
MGMT Port(RJ45)	N	N	Y	Y	Y
Hard Disk	N	Y	Y	N	Y
Redundant Power Supplies	N	N	FRPS-100	FRPS-100	Y

2 Device Management Related

2.1 Device Login

Q: How to login firewall by using default IP address?

A: User can manage firewall device through https web management (192.168.1.200/24). Here are the ports can be managed on firewall with default setting:

- RG-WALL 1600-X9300 : MGMT1
- RG-WALL 1600-X8500 : MGMT1
- RG-WALL 1600-X6600 : MGMT1
- RG-WALL 1600-M5100 : MGMT
- RG-WALL 1600-S3600 : internal (1-14)
- RG-WALL 1600-S3100 : internal (1-7)

Step1: Set a static IP address for your PC with same subnet as firewall (e.g. 192.168.1.1/24)

Step2: Connect your PC to firewall's MGMT or internal port.

Step3: Open https://192.168.1.200 with your browser and enter default username & password(admin/firewall)

2.2 Password Recovery

Q: How to recover device's password without losing running configuration?

A:

Step1: Mark down the software serial number on lateral or back plane.

Step2: Use username(admin) and password(RGFWXXXXXXXXXXX) which showed as above captured to login firewall via **console cable in 15s** after the device is powered off and restarted.

Step3: Modify admin password on CLI UI.

- RG-WALL # config system admin
- RG-WALL (admin) # edit admin
- RG-WALL (admin) # set pass 123455@!@#
- RG-WALL (admin) # end

2.3 License Activation

Temporary License

NGFW 1600 Firewall provides temporary license one month for each firewall device once. Below are the procedures to activate temporary license.

- Collect device's **Software reg number.** Claim for temporary license to mail **service_rj@ruijienetworks.com**
- Once we approve your request, signature database will be renewed when the internet is reachable.

Official License

- Collect related information according to samples in the following table and mail to rgngfw3@ruijie.com.cn

	Software SN (16 digits)	Model	Authorization Code (12 digits)	Project Name	Customer Name
Sample	DB99KKK124667235	Sample*	Sample*	Sample	Sample*

- Ensure that the firewall is connected to the Internet and configured with the correct DNS address.

Troubleshooting

- Ensure destination ports of signature database listed below are permitted (default source port is random).

Anti-Virus, IPS: UDP 9443, TCP 8890/443

Web Filter, Spam: UDP 53, 8888, 8889

- Ensure "**management-vdom**" can access Internet for signature database update if VDOM feature is enabled.
- Collect following diagnostic information to Ruijie Support Team

RG-WALL #print cliovrd enabl4e ---restart CLI session after this command

RG-WALL #execute ping google.com

RG-WALL #diagnose debug enable

RG-WALL #diagnose debug application update -1

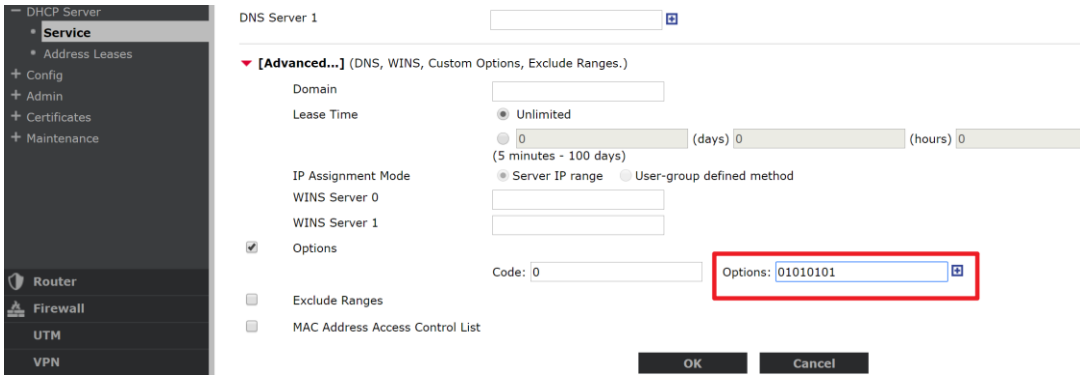
RG-WALL #exec update-now

3 Firewall Function Related

3.1 DHCP Option Setting

In NGFW firewall, we need to use **Hex to set DHCP option**. Require transforming IP address to Hex number and zero in the front of the HEX string cannot ignore.

e.g. 1.1.1.1->'01010101'. But cannot enter "1010101"



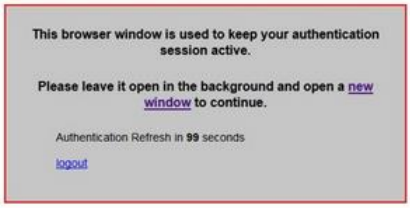
3.2 IPSEC/SSL VPN Agent

Ruijie NGFW Firewall doesn't have official IPSEC/SSL VPN agent for Windows or mobile phone. User can use build-in IPSEC client on Apple device and PPTP or L2TP VPN for windows and Android platform.

3.3 User Authentication

Q: How to set a keepalive page for authenticated user?

A: As there is not logout page for authentication function, so the user can't logout the account when they want. And user can configure the keepalive page for holding the authenticated session.



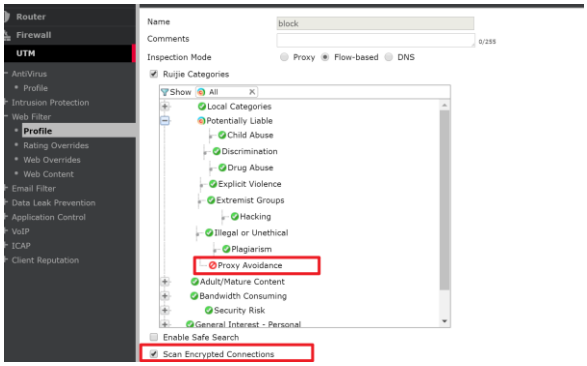
- RG-WALL#config user setting
- RG-WALL#set auto-keepalive enable

3.4 Web Filter

Q: How to block the online proxy on firewall?

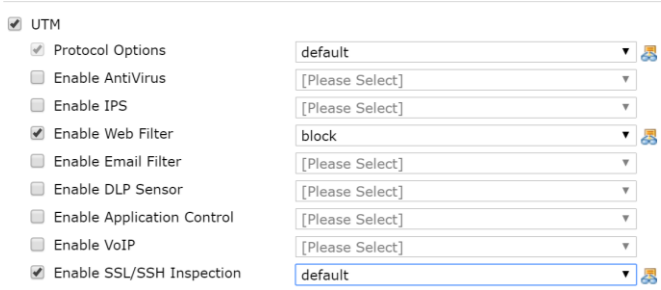
A:

Step1: Select "flow based" web filter and block the Proxy Avoidance on Ruijie categories.



Step2: Enable scan encrypted connections

Step3: Apply web filter and ssl/ssh inspection.



After that, all HTTPS website will be converted into firewall certification.

Q: Web filter feature cannot be used and it shows Ruijie Guard server failed to response.

A: This problem is related to signature license and internet connection between firewall and Ruijie Guard cloud server.

Troubleshooting

1. Verity firewall signature license status, if web filter signature is expired, Ruijie Guard service will be not available. For more details about license activation, please refer *License Activation* chapter.
2. Ensure the destination port for web filter update is not blocked by ISP or uplink device, or you can exec below setting to change port for server communication.

RG-WALL #print cliovrd enabl4e ---restart CLI session after this command

RG-WALL # config system Ruijieguard

RG-WALL (Ruijieguard) # set port

53 Port 53 for server communication.

8888 Port 8888 for server communication. //default setting

3. If above troubleshooting steps cannot solve your problem, please collect following debug information for Ruijie Support.

   RG-WALL #print cliovrd enabl4e ---restart CLI session after this command

   RG-WALL #diagnose debug enable

   RG-WALL #diagnose deb rating

3.5 Anti-Virus

Q: Some viruses cannot be scanned even the anti-virus feature is enabled.

A: All Ruijie NGFW firewall units have the normal antivirus signature database but some models have additional databases you can select for use. Which you choose depends on your network and security needs.

Normal	Includes viruses currently spreading as determined by the RuijieGuard Global Security Research Team. These viruses are the greatest threat. The Normal database is the default selection and it is available on every NGFW unit.
Extended	Includes the normal database in addition to recent viruses that are no-longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared.
Extreme	Includes the extended database in addition to a large collection of 'zoo' viruses. These are viruses that have not spread in a long time and are largely dormant today. Some zoo viruses may rely on operating systems and hardware that are no longer widely used.

```
config antivirus setting
  set default-db [normal|extended|extreme]
end
```

Q: NGFW UTM features are not working while memory reaches to 80%.

A: Conserve mode is activated when the remaining free memory is nearly exhausted (up to 80%). While conserve mode is active, the UTM does not accept new sessions and bypass all session by default.

Conserve Mode Setting:

```
config system global
        set av-failopen {idledrop | off | one-shot | pass}
end
```

- idledrop – Drop idle connections.
- off – Off.
- one-shot – try to create new session
- pass – bypass new session(default)

3.6 IPSEC VPN

Q: IPSEC VPN tunnel cannot bring up

A:

- Ensure that the pre-shared keys match exactly
- Ensure that both ends use the same P1 and P2 proposal settings
- Ensure that you have allowed inbound and outbound traffic for all necessary network services, especially if services such as DNS or DHCP are having problems.
- Check that a static route has been configured properly to allow routing of VPN traffic.

- Ensure that your unit is in NAT/Route mode, rather than Transparent.
- Check your NAT settings, enabling NAT traversal in the Phase 1 configuration while disabling NAT in the security policy. You might need to pin the PAT/NAT session table, or use some of kind of NAT-T keepalive to avoid the expiration of your PAT/NAT translation.
- Ensure that both ends of the VPN tunnel are using Main mode, unless multiple dial-up tunnels are being used.
- If you have multiple dial-up IPsec VPNs, ensure that the Peer ID is configured properly
- and that clients have specified the correct Local ID.
- If you are using Perfect Forward Secrecy (PFS), ensure that it is used on both peers. You can use the diagnose vpn tunnel list command to troubleshoot this.
- Ensure that the Quick Mode selectors are correctly configured. If part of the setup currently uses firewall addresses or address groups, try changing it to either specify the IP addresses or use an expanded address range.
- If XAUTH is enabled, ensure that the settings are the same for both ends, and that the firewall unit is set to Enable as Server.
- Check IPsec VPN Maximum Transmission Unit (MTU) size. A 1500 byte MTU is going to exceed the overhead of the ESP-header, including the additional ip_header,etc. You can use the diagnose vpn tunnel list command to troubleshoot this.
- If your unit is behind a NAT device, such as a router, configure port forwarding for UDP ports 500 and 4500.
- Remove any Phase 1 or Phase 2 configurations that are not in use. If a duplicate instance of the VPN tunnel appears on the IPsec Monitor, reboot your unit to try and clear the entry.

If you are still unable to connect to the VPN tunnel, run the following diagnostic command in the CLI and send to Ruijie support.

Troubleshooting

RG-WALL#diagnose debug enable

RG-WALL#diagnose debug application ike -1

3.7 PPTP/L2TP VPN

The following steps can be used to understand why a PPTP/L2TP VPN user is experiencing disconnections from NGFW firewall, and to enable the appropriate debug depending on the type of PPTP/L2TP VPN User. Collect below information and send to Ruijie support.

1. A PPTP/l2TP VPN user connects to the NGFW firewall with local authentication.

RG-WALL#diag deb enable

RG-WALL#diag deb reset

RG-WALL#diag deb console timestamp en

RG-WALL#diag deb app ppp -1

2. If the PPTP VPN User uses authentication with LDAP then enable the following debug with step.

diag test auth ldap (ldapservername in GUI) (username to test) (pwd user)

diag test auth ldap LDAP_Server user password

3. If the PPTP VPN User uses Radius then also collect the following debug.

diag test authserver radius <server_name> <chap | pap | mschap | mschap2> <username> <password>

4. Collect a sniffer trace on the port of the PPTP/L2TP connection.

diag sniffer packet <port of pptp/l2tp connection> 'local_ip_addr of pc' 6

4 Firewall Maintenance Related

4.1 CPU & Memory Utilization

When the CPU or Memory running in high utilization, take below actions and collect necessary information for Ruijie Support.

CPU:

1.Abnormal Data like virus is dropped while passing through.

diagnose sniffer packet any none 4 100

2.Check the Top 5 processes

diagnose sys top 5 99 -----press Q to quit

Memory:

1.Check the Top 5 processes

diagnose sys top 5 99 -----press Q to quit

2.Check the cache if enabled the logging function

diagnose hardware sysinfo memory

4.2 Traffic Flow Diagnose

'Debug Flow' is usually used to debug the behavior of the traffic in a NGFW device and to check how the traffic is flowing. The use of proper filtering can help by narrowing down to only the desired traffic and thus ease the debugging process.

Troubleshooting

RG-WALL#diagnose debug disable

RG-WALL#diagnose debug flow trace stop

RG-WALL#diagnose debug flow filter clear

RG-WALL#diagnose debug reset

RG-WALL#diagnose debug flow filter addr x.x.x.x

RG-WALL#diagnose debug flow show console enable

RG-WALL#diagnose debug flow show function-name enable

RG-WALL#diagnose debug console timestamp enable

RG-WALL#diagnose debug flow trace start 999

RG-WALL#diagnose debug enable

Common Problems:

msg="iprope_in_check() check failed, drop“ ---- mismatch policy

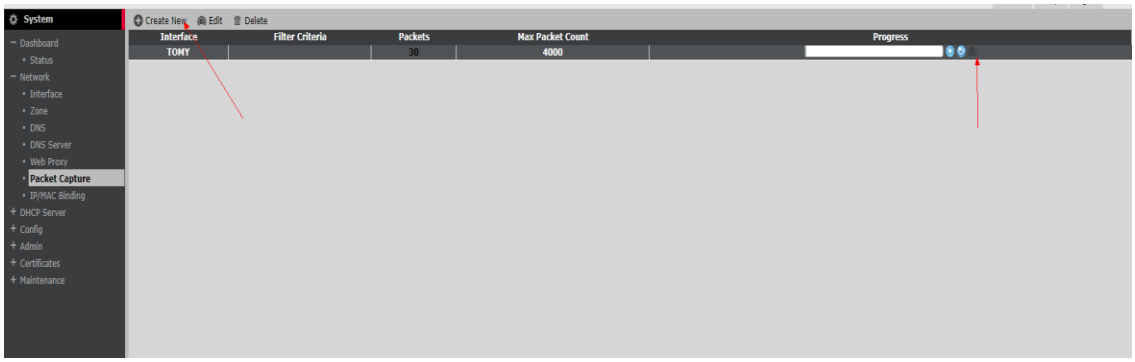
msg="Denied by forward policy check“ ---- policy deny

msg="reverse path check fail, drop“ ---- RPF check failed

4.3 Packets Capture

To use packet capture through the GUI, your firewall model must have internal storage and disk logging must be enabled. If your device doesn’t support disk logging, please execute packet capture under CLI.

GUI Capture



CLI Capture

diagnose sniffer packet <interface> <'filter'> <verbose> <count>

4.4 Log & Report

Q: Why cannot see any logs on model M6600?

A: Logging is not enabled by default for this model. Because firewall M6600 doesn't have storage disk, logs will be saved in memory and drag down the performance if enabled. Here are steps to enable the logging on memory and not be recommended.

1) Tick the logging traffic option on firewall setting.

2) Exec below command on firewall:

RG-WALL # Config log memory setting

RG-WALL (setting) # Set status enable

RG-WALL (setting) #end

RG-WALL #

4.5 Common Commands

1. Configure an interface address.

RG-WALL # config system interface

RG-WALL (interface) # edit lan

RG-WALL (lan) # set ip 192.168.100.99/24

RG-WALL (lan) # end

2. Configure a static route.

RG-WALL (static) # edit 1

RG-WALL (1) # set device wan1

RG-WALL (1) # set dst 10.0.0.0 255.0.0.0

RG-WALL (1) # set gateway 192.168.57.1

RG-WALL (1) # end

3. Configure a default route.

RG-WALL (1) # set gateway 192.168.57.1

RG-WALL (1) # set device wan1

RG-WALL (1) # end

4. Configure a firewall address.

RG-WALL # config firewall address

RG-WALL (address) # edit clientnet

new entry 'clientnet' added

RG-WALL (clientnet) # set subnet 192.168.1.0 255.255.255.0

RG-WALL (clientnet) # end

5. Configure an IP pool.

RG-WALL (ippool) # edit nat-pool

new entry 'nat-pool' added

RG-WALL (nat-pool) # set startip 100.100.100.1

RG-WALL (nat-pool) # set endip 100.100.100.100

RG-WALL (nat-pool) # end

6. Configure a virtual IP address.

RG-WALL # config firewall vip

RG-WALL (vip) # edit webserver

new entry 'webserver' added

RG-WALL (webserver) # set extip 202.0.0.167

RG-WALL (webserver) # set extintf wan1

RG-WALL (webserver) # set mappedip 192.168.0.168

RG-WALL (webserver) # end

7. Configure the Internet access policy.

RG-WALL # config firewall policy

RG-WALL (policy) # edit 1

RG-WALL (1)#set srcintf internal //Indicates the source interface.

RG-WALL (1)#set dstintf wan1 ///Indicates the destination interface.

RG-WALL (1)#set srcaddr all //Indicates the source address.

RG-WALL (1)#set dstaddr all //Indicates the destination address.

RG-WALL (1)#set action accept //Indicates the action.

RG-WALL (1)#set schedule always //Indicates the schedule.

RG-WALL (1)#set service ALL //Indicates the service.

RG-WALL (1)#set logtraffic disable //Enables or disables logs.

RG-WALL (1)#set nat enable //Enables NAT.

8. Configure the mapping policy.

RG-WALL # config firewall policy

RG-WALL (policy) #edit 2

RG-WALL (2)#set srcintf wan1 //Indicates the source interface.

RG-WALL (2)#set dstintf internal //Indicates the destination interface.

RG-WALL (2)#set srcaddr all //Indicates the source address.

RG-WALL (2)#set dstaddr ngfw1 //Indicates the destination address used for virtual IP address mapping, which is added beforehand.

RG-WALL (2)#set action accept //Indicates the action.

RG-WALL (2)#set schedule always //Indicates the schedule.

RG-WALL (2)#set service ALL //Indicates the service.

RG-WALL (2)#set logtraffic disable //Enables or disables logs.

9. Change the internal switching interface to the routing interface.

Ensure that routing, DHCP, and firewall policies of the internal interface are deleted.

RG-WALL # config system global
RG-WALL (global) # set internal-switch-mode interface
RG-WALL (global) #end

10. View the host name and management port.

RG-WALL # show system global

11. View the system status and available resources.

RG-WALL # get system performance status

12. View the application traffic statistics.

RG-WALL # get system performance firewall statistics

13. View the ARP table.

RG-WALL # get system arp

14. View ARP details.

RG-WALL # diagnose ip arp list

15. Clear the ARP cache.

RG-WALL # execute clear system arp table

16. View the current session table.

RG-WALL # diagnose sys session stat or RG-WALL # diagnose sys session full-stat

17. View the session list.

RG-WALL # diagnose sys session list

18. View the physical interface status.

RG-WALL # get system interface physical

19. View settings of the default route.

RG-WALL # show router static

20. View the static route in the routing table.

RG-WALL # get router info routing-table static

21. View OSPF configuration.

RG-WALL # show router ospf

22. View the global routing table.

RG-WALL # get router info routing-table all

23. View HA status.

RG-WALL # get system ha status

24. Check synchronization of active and standby routers.

RG-WALL # diagnose sys ha showcsum