

RG-WALL 1600 Next-Generation Firewall Installation and Initialization

Applicable to V5.2-R5.0

Contents

- Preface
- Hardware Installation
- Initialization Setup

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

- Preface
- **Hardware Installation**
- Initialization Setup

Hardware Installation

Preparation

Device installation in specified locations

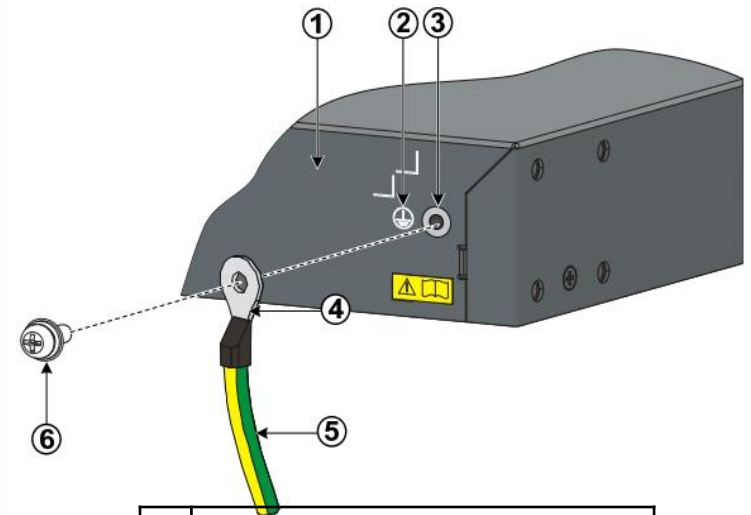
Grounding and cable connection

A ground bar is provided in the installation environment (recommended):

- ① Remove the ground screw from the rear panel of the device.
- ② Put the OT terminal of the ground cable delivered with the device on the ground screw of the chassis.
- ③ Install the ground screw with the OT terminal to the ground hole, fasten it with a screwdriver, and connect the other end of the ground cable to the ground bar of the equipment room.

A ground bar is not provided in the installation environment:

If the device adopts AC power supply, the PE cable of the AC power supply needs to be grounded. Check whether the PE cable of the AC power supply is properly grounded in the power distribution room or on the AC transformer side.



1	Rear panel of the device
2	Grounding label
3	Grounding hole
4	OT terminal of the protective ground cable
5	Protective ground cable
6	Ground screw

Contents

- Preface
- Hardware Installation
- Initialization Setup

| Operating Modes

Device login

Fast configuration

Upgrade

Fast configuration in NAT (routing) mode

Step 1: Select an operating mode. The default is NAT (routing) mode.

System Information	
Software reg number	RGFW513914802639
Hardware reg number	h1hdcvh000051
Host Name	RG-WALL [Change]
Model	RG-WALL 1600-M5100
Uptime	56 day(s) 0 hour(s) 56 min(s)
System Time	Mon May 30Day of Month 09:24:57 2016 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.12.8596.P3.e1-20150914 [Update]
System Configuration	[Backup] [Restore]
Operation Mode	NAT [Change]
Virtual Domain	Disabled [Enable]
Current Administrators	1 [Details]
Current User	admin [Change Password]

NOTE:

The firewall operates either in NAT or transparent mode. The default is NAT mode. If both modes are adopted, VDOM must be implemented.

Interface IP Address

Device login

Fast configuration

Upgrade

Fast configuration in NAT (routing) mode

Step 2: Configure the IP address of the specified interface.

System | **Edit Interface**

— Dashboard

- Status

— Network

- **Interface**
- Zone
- DNS
- DNS Server
- Web Proxy
- Packet Capture
- IP/MAC Binding

+ DHCP Server

Name: internal

Alias:

Link Status: up

Type: Physical Interface

Addressing mode: Manual DHCP PPPoE

IP/Netmask:

Administrative Access: HTTPS PING HTTP SSH SNMP

TELNET

NOTE:

When you configure the IP address of the interface, you can configure its management authority at the same time. For example, if you select **TELNET**, you can use the IP address of the interface to manage the firewall via telnet. If you do not select **TELNET**, management via telnet is disabled.

Default Route



Fast configuration in NAT (routing) mode

Step 3: Configure the default route.

The screenshot shows the 'Edit Static Route' configuration page in the Ruijie web management interface. On the left is a navigation menu with 'System' at the top, followed by 'Router', 'Static', 'Dynamic', and 'Monitor'. Under 'Static', there are sub-items: 'Static Route' (selected), 'Policy Route', and 'Settings'. The main content area is titled 'Edit Static Route' and contains the following fields:

Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
Device	<input type="text" value="wan1"/>
Gateway	<input type="text" value="202.1.1.9"/>
Distance	<input type="text" value="10"/> (1-255)
Priority	<input type="text" value="0"/> (0-4294967295)
Comments	<input type="text"/>

At the bottom right of the form are two buttons: 'OK' and 'Cancel'.

Security Policy

Device login

Fast configuration

Upgrade

Fast configuration in NAT (routing) mode

Step 4: Configure a policy for Internet access.

The screenshot displays the 'Edit Policy' configuration page in the Ruijie Network management interface. On the left, a sidebar menu shows the navigation path: System > Router > Firewall > Policy. The main configuration area is titled 'Edit Policy' and contains the following settings:

- Source Interface/Zone: lan
- Source address: all (Multiple)
- Destination Interface/Zone: wan1
- Destination address: all (Multiple)
- Schedule: always
- Service: ALL (Multiple)
- Action: ACCEPT
- Log Allowed Traffic

The NAT section is expanded, showing three options: 'No NAT', 'Enable NAT' (which is selected and highlighted with a red box), and 'Use Central NAT Table'. There is also an unchecked checkbox for 'Dynamic IP Pool'. Below the NAT options, the 'Session TTL' is set to 0, with a note '(0 or 300-604800)'. At the bottom, there is an unchecked checkbox for 'Enable Identity Based Policy'.

NOTE:

By default, the system has the Internet access policy used to route traffic from the internal interface to the Wan1 interface.

Security Policy

Device login

Fast configuration

Upgrade

Fast configuration in NAT (routing) mode

Step 5: Enable the antivirus feature.

The screenshot shows the 'Edit Policy' configuration page in Ruijie's management interface. The left sidebar shows the navigation menu with 'Firewall' > 'Policy' selected. The main content area is titled 'Edit Policy' and contains the following settings:

- Schedule: always
- Service: ALL (Multiple)
- Action: ACCEPT
- Log Allowed Traffic
- NAT:
 - No NAT
 - Enable NAT (Dynamic IP Pool:)
 - Use Central NAT Table
- Session TTL: 0 (0)
- Enable Identity Based Policy
- UTM
 - Protocol Options: default
 - Enable AntiVirus: default
 - Enable IPS: [Please Select]
 - Enable Web Filter: [Please Select]
 - Enable Email Filter: [Please Select]
 - Enable DLP Sensor: [Please Select]
 - Enable Application Control: [Please Select]

A red box highlights the 'UTM' section, and a note states: **NOTE:** Enable the UTM virus detection feature and enable antivirus. You also need to select protocol options (the protocol option is automatically selected).

Security Policy

Device login

Fast configuration

Upgrade

Fast configuration in NAT (routing) mode

Step 6: Enable trafficcontrol per ip address.

The screenshot displays the configuration interface for a Ruijie device. On the left, a navigation menu is visible with the following items: Policy (highlighted with a red box), Central NAT Table, DoS Policy, Protocol Options, SSL/SSH Inspection, NAT64 Policy, Address, Service, Schedule, Traffic Shaper (with sub-items Shared and Per-IP), Virtual IP, and Load Balance. At the bottom of the menu, 'UTM' is also visible. The main configuration area is titled 'NAT' and includes the following settings:

- No NAT
- Enable NAT
- Dynamic IP Pool
- Use Central NAT Table
- Session TTL: (0 or 300-604800)
- Enable Identity Based Policy
- UTM
 - Protocol Options: default
 - Enable AntiVirus: default
 - Enable IPS: [Please Select]
 - Enable Web Filter: [Please Select]
 - Enable Email Filter: [Please Select]
 - Enable DLP Sensor: [Please Select]
 - Enable Application Control: [Please Select]
 - Enable VoIP: [Please Select]
 - Enable SSL/SSH Inspection: [Please Select]
 - Traffic Shaping: [Please Select]
 - Reverse Direction Traffic Shaping: [Please Select]
 - Per-IP Traffic Shaping: 1M

Operating Modes

Device login

Fast configuration

Upgrade

Fast configuration in transparent mode

Step 1: Select an operating mode. The default is NAT (routing) mode.

The screenshot shows the configuration interface for a Ruijie network device. On the left is a navigation menu with 'System' selected. The main content area is titled 'Mode' and contains a 'Operation Mode' dropdown menu. The dropdown menu is open, showing three options: 'NAT' (selected), 'NAT', and 'Transparent'. Below the dropdown, there are sections for 'Current Administrators' (3 [Details]) and 'Current User' (admin [Change Password]).

NOTE:

The firewall operates either in NAT or transparent mode. The default is NAT mode. If both modes are adopted, VDOM must be implemented.

| Operating Modes

Device login

Fast configuration

Upgrade

Fast configuration in transparent mode

Step 2: Configure the management IP address and the gateway.

The screenshot shows the Ruijie Network configuration interface. On the left is a sidebar menu with 'System' selected. The main content area is titled 'Mode' and contains the following configuration fields:

Operation Mode	Transparent
Management IP/Netmask	192.168.1.253/255.255.255.0
Default Gateway	192.168.1.254

Below the input fields is an 'Apply' button. A red box highlights the Management IP/Netmask and Default Gateway fields.

NOTE:

The firewall operates either in NAT or transparent mode. The default is NAT mode. If both modes are adopted, VDOM must be implemented. If the transparent mode is adopted, the management IP address must be configured.

Operating Modes

Device login

Fast configuration

Upgrade

Fast configuration in transparent mode

Step 3: Configure a policy for Internet access.

The screenshot displays the 'Edit Policy' configuration page in the Ruijie management interface. On the left is a navigation menu with 'System', 'Router', and 'Firewall' sections. Under 'Firewall', 'Policy' is selected, showing sub-items like 'Central NAT Table', 'DoS Policy', 'Protocol Options', 'SSL/SSH Inspection', and 'NAT64 Policy'. Other options include 'Address', 'Service', 'Schedule', 'Traffic Shaper', 'Virtual IP', and 'Load Balance'. The main configuration area includes fields for Source Interface/Zone (wan1), Source address (all), Destination Interface/Zone (wan1), Destination address (all), Schedule (always), Service (ALL), and Action (ACCEPT). A 'Log Allowed Traffic' checkbox is checked. Under the 'NAT' section, the 'No NAT' radio button is selected and highlighted with a red box, while 'Enable NAT' and 'Use Central NAT Table' are unselected. 'Dynamic IP Pool' is also unselected. The 'Session TTL' is set to 0.

Field	Value
Source Interface/Zone	wan1
Source address	all
Destination Interface/Zone	wan1
Destination address	all
Schedule	always
Service	ALL
Action	ACCEPT
Log Allowed Traffic	<input checked="" type="checkbox"/>
NAT	<input checked="" type="radio"/> No NAT
Enable NAT	<input type="radio"/>
Use Central NAT Table	<input type="radio"/>
Dynamic IP Pool	<input type="checkbox"/>
Session TTL	0

NOTE:

Disable NAT in transparent mode. By default, NAT is disabled.

Security Policy

Device login

Fast configuration

Upgrade

Fast configuration in transparent mode

Step 4: Enable the antivirus feature.

The screenshot shows the 'Edit Policy' configuration page in a Ruijie firewall. The left sidebar contains a navigation menu with 'System', 'Router', 'Firewall', and 'Policy' sections. Under 'Policy', 'Policy' is selected, with sub-items like 'Central NAT Table', 'DoS Policy', 'Protocol Options', 'SSL/SSH Inspection', and 'NAT64 Policy'. The main configuration area is titled 'Edit Policy' and contains the following fields:

- Source Interface/Zone: wan1
- Source address: all
- Destination Interface/Zone: wan1
- Destination address: all
- Schedule: always
- Service: ALL
- Action: ACCEPT
- Log Allowed Traffic
- NAT:
 - No NAT
 - Enable NAT Dynamic IP Pool
 - Use Central NAT Table
- Session TTL: 0 (0 or 300-65535)
- Enable Identity Based Policy
- UTM
 - Protocol Options: default
 - Enable AntiVirus: default

A red box highlights the UTM section, and a blue box highlights the 'Protocol Options' dropdown. A teal callout box on the right contains the following text:

NOTE: Enable the UTM virus detection feature and enable antivirus. You also need to select protocol options (the protocol option is automatically selected).

Security Policy

Device login

Fast configuration

Upgrade

Fast configuration in transparent mode

Step 5: Enable **trafficcontrol per ip address**.

The screenshot displays the 'New Policy' configuration page in the Ruijie Networks management interface. The left sidebar shows the navigation menu with 'Firewall' selected. The main content area is divided into sections: Service, Action, NAT, Session TTL, UTM, and Traffic Shaping. The 'Per-IP Traffic Shaping' option is checked and its value is set to '1M', which is highlighted by a red rectangular box. Other UTM options like 'Enable AntiVirus' and 'Protocol Options' are also checked. The 'Traffic Shaping' section includes options for 'Traffic Shaping' and 'Reverse Direction Traffic Shaping', both currently unchecked.

Section	Option	Value
Service	Service	----- SERVICE -----
	Action	ACCEPT
NAT	No NAT	<input checked="" type="radio"/>
	Enable NAT	<input type="radio"/>
	Use Central NAT Table	<input type="radio"/>
Session TTL	Session TTL	0 (0 or 300-604800)
	Enable Identity Based Policy	<input type="checkbox"/>
UTM	UTM	<input checked="" type="checkbox"/>
	Protocol Options	default
	Enable AntiVirus	default
	Enable IPS	[Please Select]
	Enable Web Filter	[Please Select]
	Enable Email Filter	[Please Select]
	Enable DLP Sensor	[Please Select]
	Enable Application Control	[Please Select]
	Enable VoIP	[Please Select]
	Enable SSL/SSH Inspection	[Please Select]
Traffic Shaping	Traffic Shaping	<input type="checkbox"/>
	Reverse Direction Traffic Shaping	<input type="checkbox"/>
Per-IP Traffic Shaping	<input checked="" type="checkbox"/>	1M

Comments (maximum 63 characters)

Changing the Administrator Password

Device login

Fast configuration

Upgrade

Change the administrator account and password, and configure the management host.

System

- Dashboard
 - Status
- Network
- DHCP Server
- Config
- Admin
 - Administrators**
 - Admin Profile
 - Settings
- Certificates
- Maintenance

Edit Administrator

Administrator: **Change Password**

Type: Regular Remote PKI

Comments:

Admin Profile:

Virtual Domain:

Restrict this Admin Login from Trusted Hosts Only

Trusted Host #1:

Trusted Host #2:

Trusted Host #3:

Restrict to Provision Guest Accounts

OK Cancel

Edit Password

Administrator: admin

Old Password:

Edit Password:

Confirm Password:

OK Cancel

NOTE: After device configuration, you are advised to change the administrator account and password. Only the IP addresses of trusted hosts can be used to manage the firewall.

Initialization Setup

Device login

Fast configuration

Upgrade

Version upgrade

To upgrade the system version, do the following:

The screenshot displays the 'Firmware Upgrade/Downgrade' configuration page. The 'Upgrade From' dropdown menu is set to 'Local Hard Disk'. The 'Upgrade File' field contains the file path 'RG-WALL 1600...8596.P3.bin'. Below the file selection, there are 'OK' and 'Cancel' buttons. In the foreground, a file explorer window shows the selected file 'RG-WALL 1600-M5100 V5.2-R5.12.8596.P3.e1-20150914.bin' highlighted. To the right, a table shows a version '150914' with an '[Update]' button next to it.

NOTE: After upgrade, restart the system to make the new version take effect. Each model corresponds to a version, and the same version is not applicable to all models.