RG-WALL 1600 Next-Generation Firewall Installation and Initialization

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

- 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):

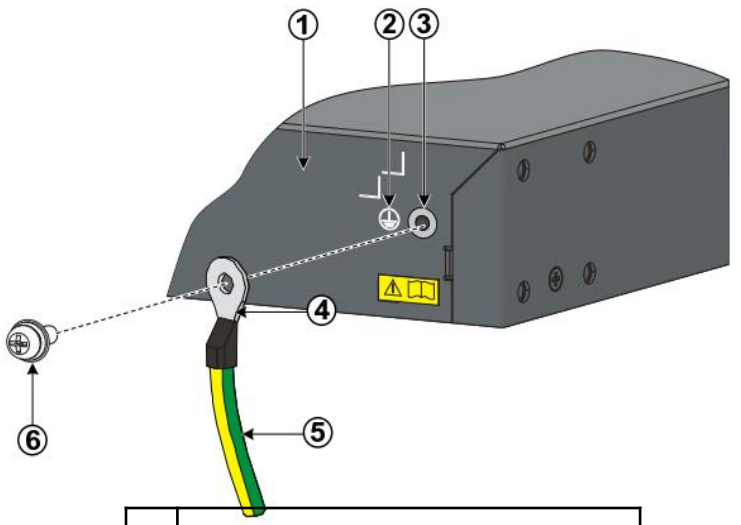
① Remove the ground screw from the rear panel of the device.

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

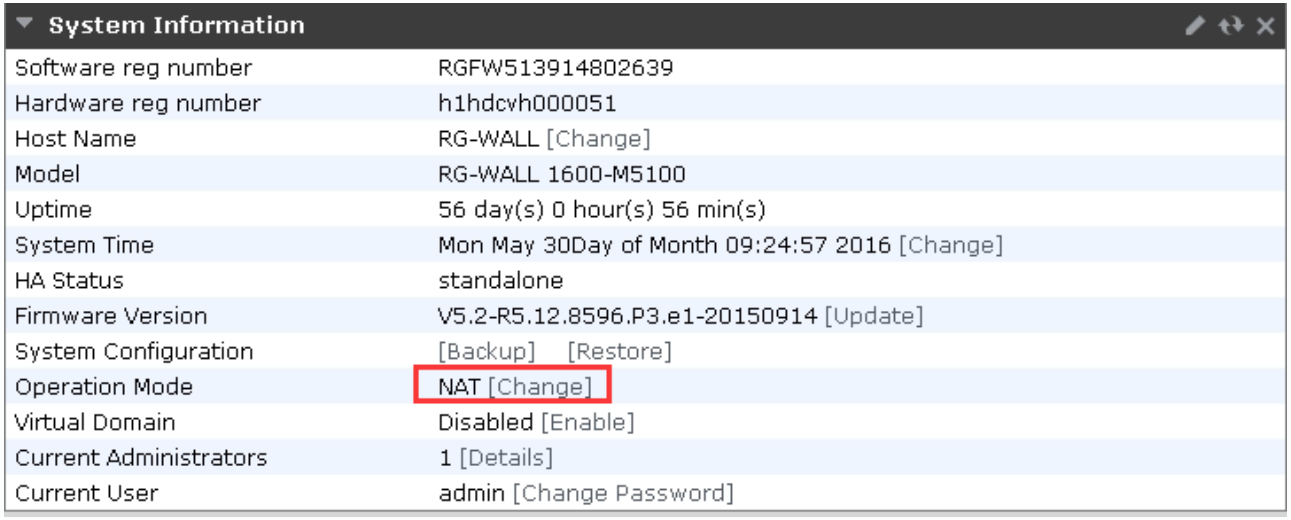
Contents

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]

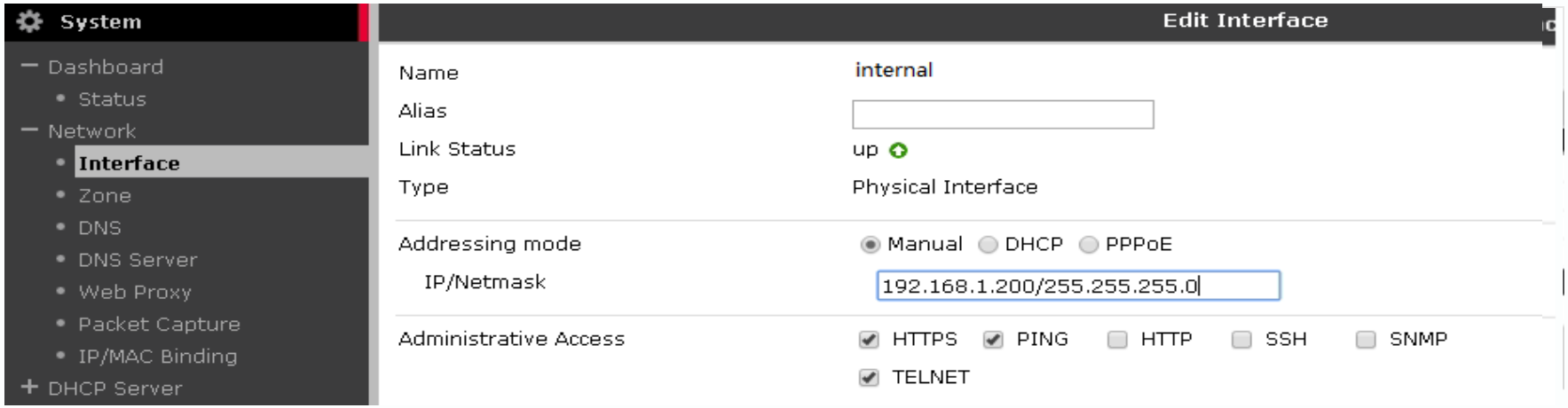
NOTE:
The firewall operates either in NAT or transparent mode. The default is NAT mode. If both modes are adopted, VDOM must be implemented.

Interface IP Address

Device login | Fast configuration | Upgrade

Fast configuration in NAT (routing) mode

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



NOTE:

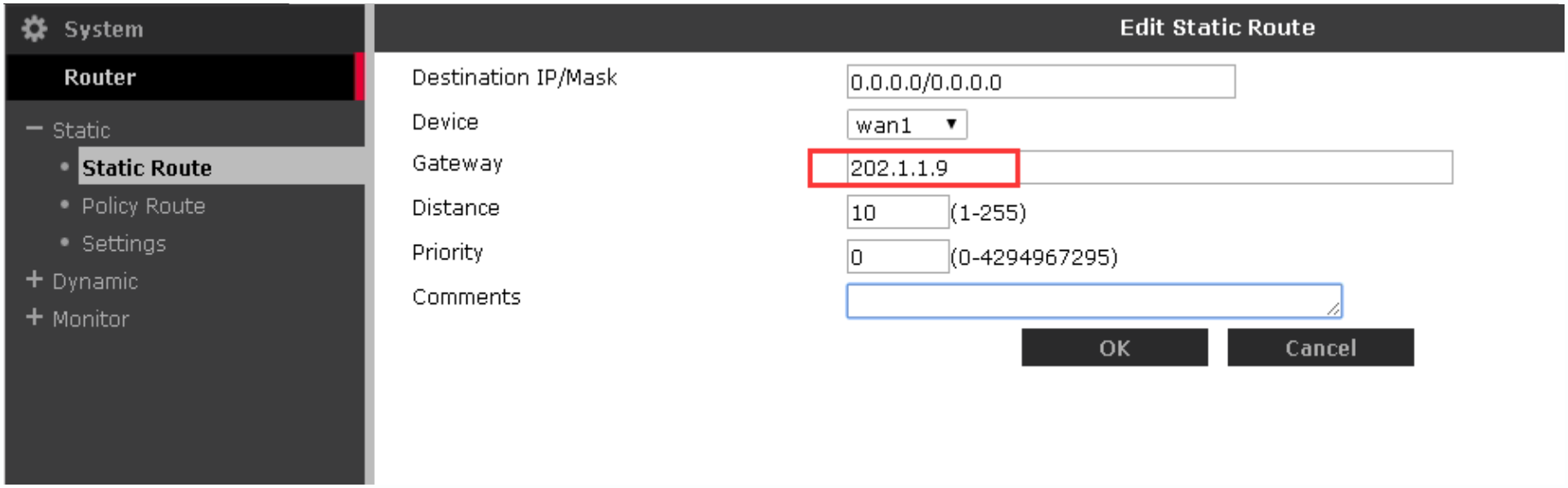
When you configure the IP address of the interface, you can configure its management authority at the same time. For example, if you select **TELNET**, you can use the IP address of the interface to manage the firewall via telnet. If you do not select **TELNET**, management via telnet is disabled.

Default Route

Device login | Fast configuration | Upgrade

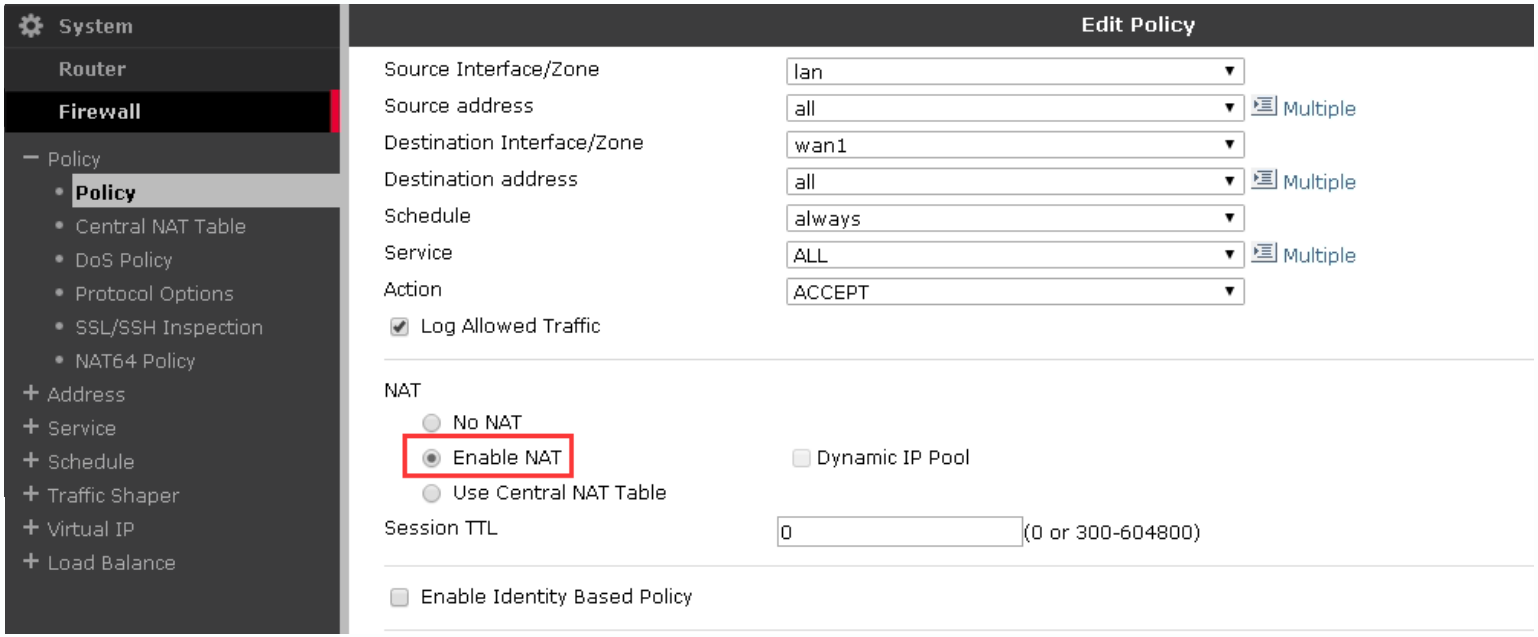
Fast configuration in NAT (routing) mode

Step 3: Configure the default route.



Fast configuration in NAT (routing) mode

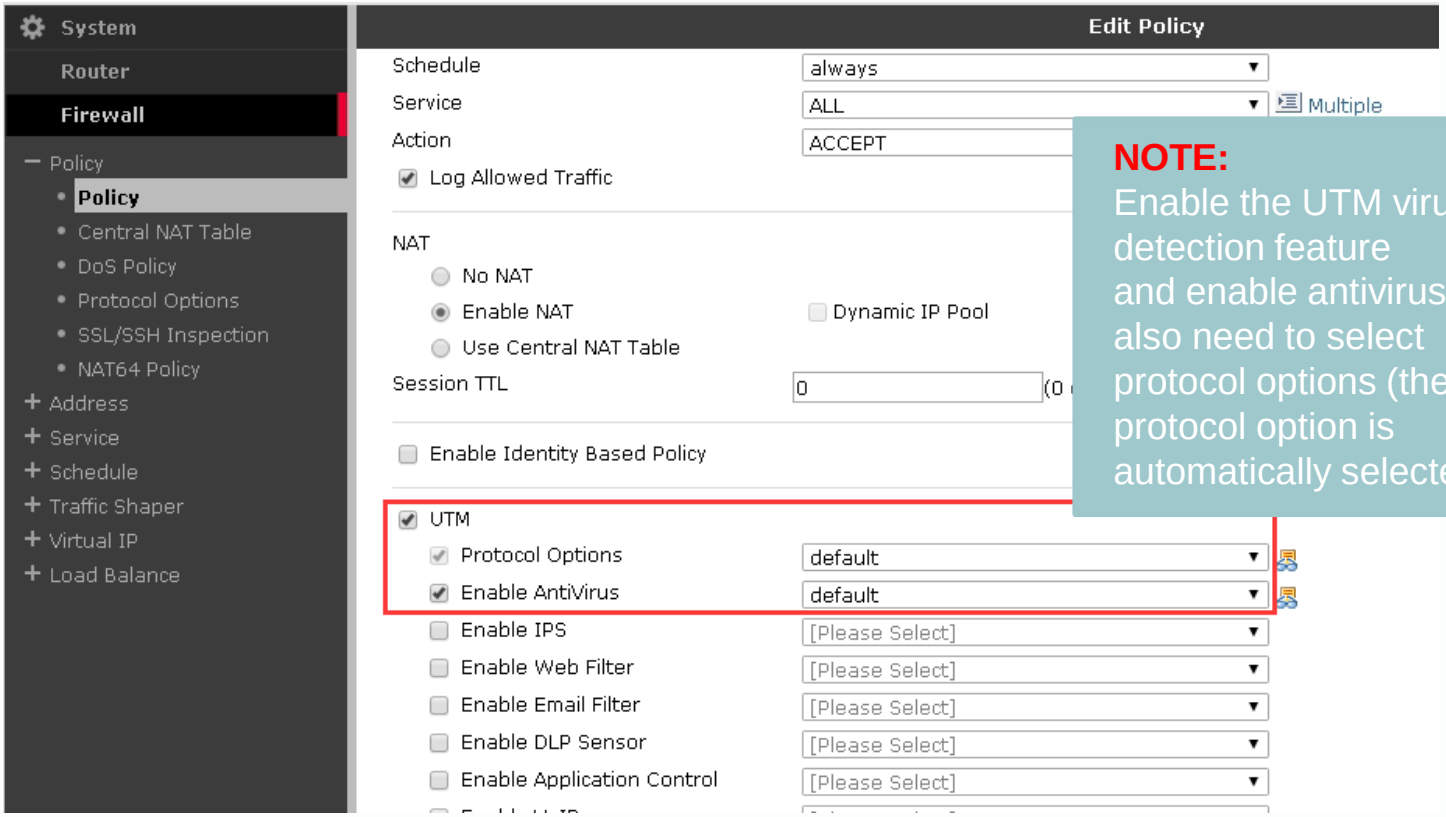
Step 4: Configure a policy for Internet access.



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

Fast configuration in NAT (routing) mode

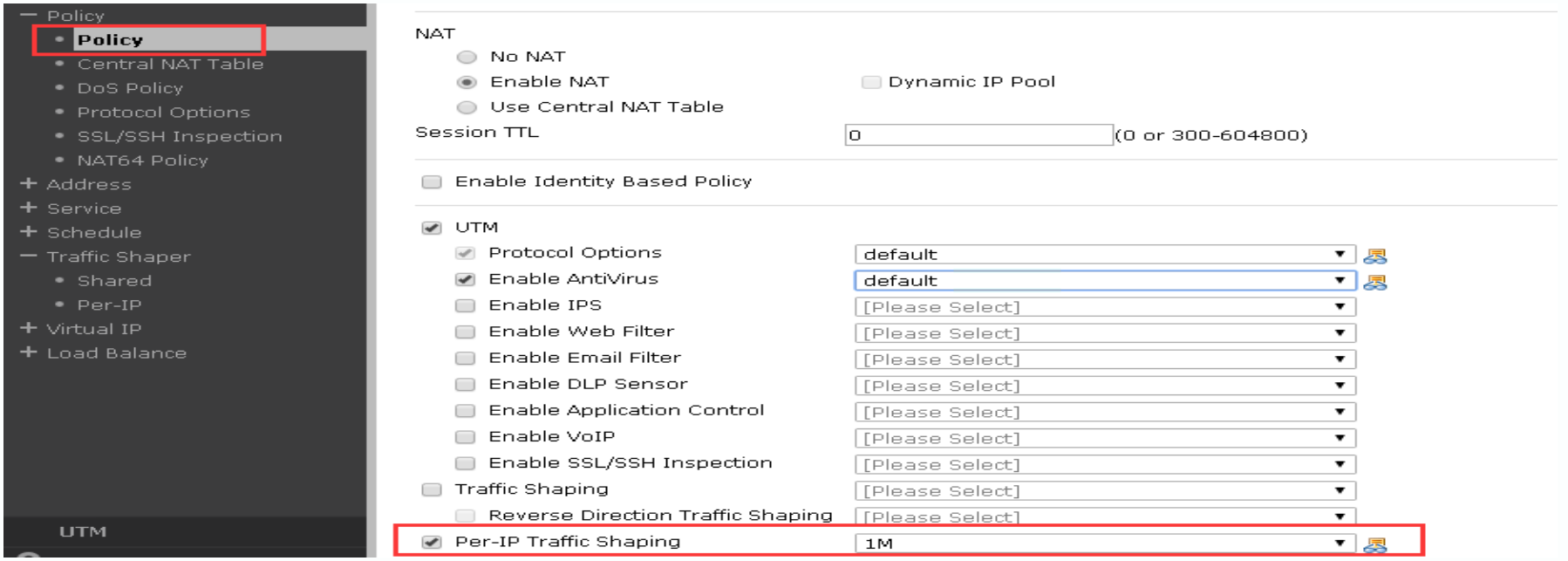
Step 5: Enable the antivirus feature.



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

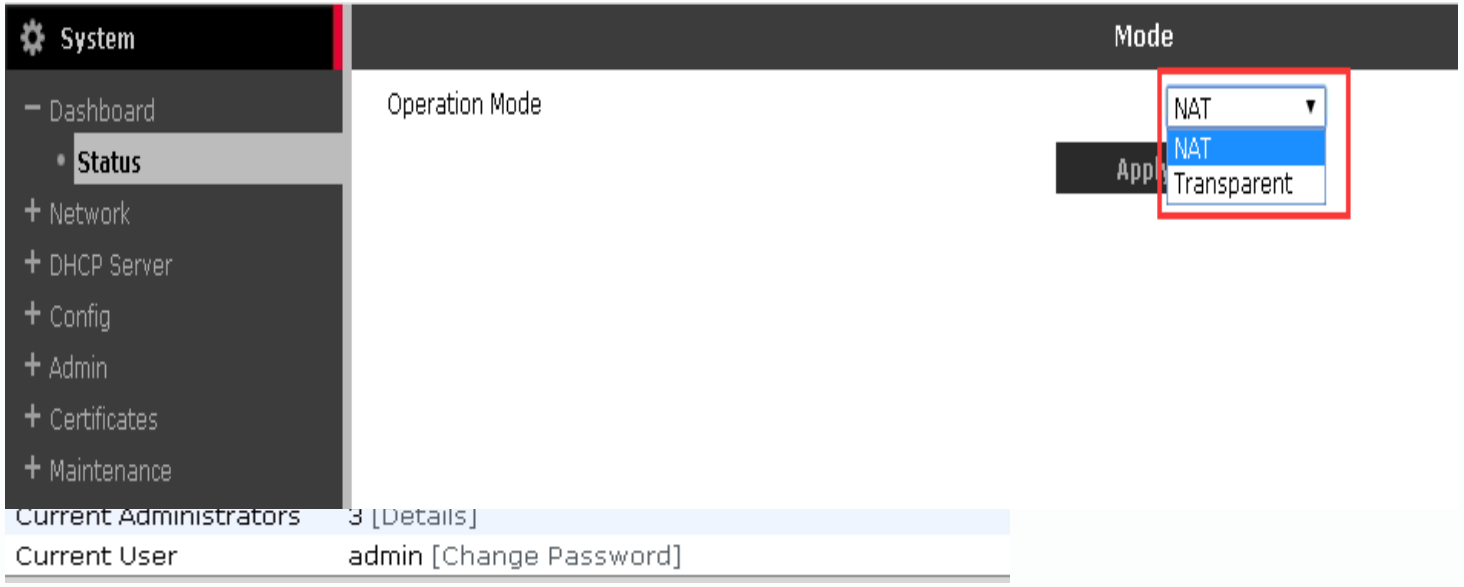
Fast configuration in NAT (routing) mode

Step 6: Enable **trafficcontrol per ip address**.



Fast configuration in transparent mode

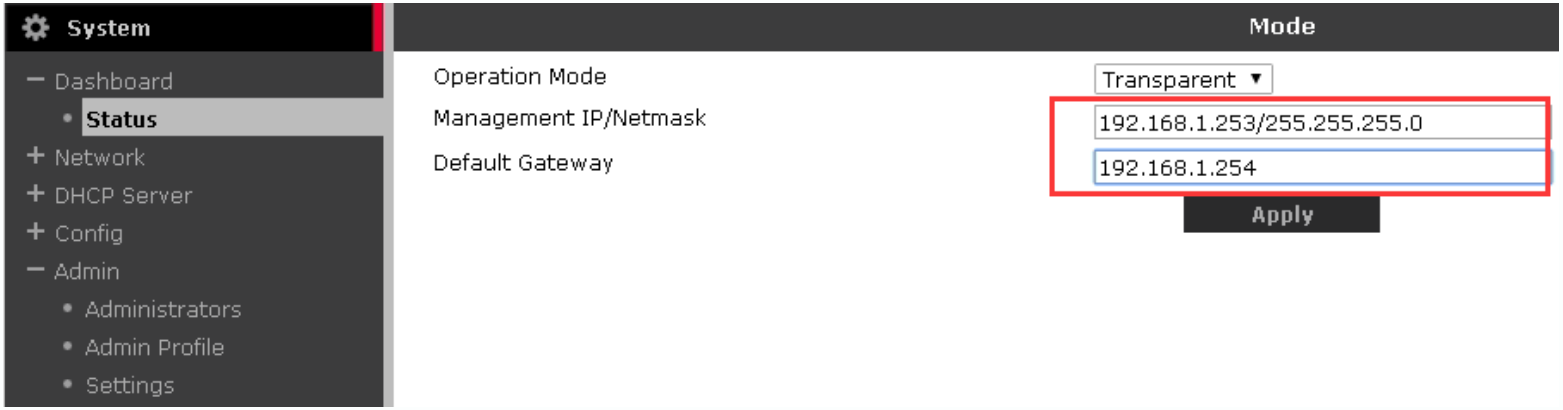
Step 1: Select an operating mode. The default is NAT (routing) mode.



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

Fast configuration in transparent mode

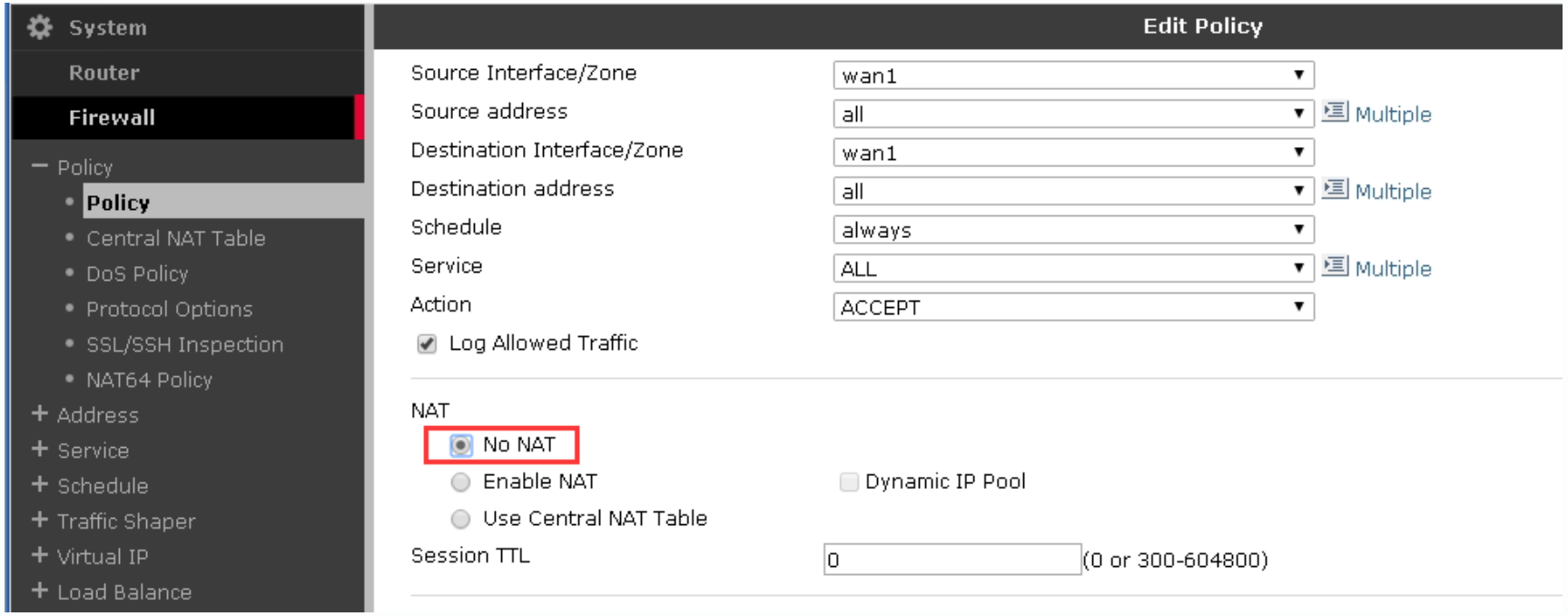
Step 2: Configure the management IP address and the gateway.



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.

Fast configuration in transparent mode

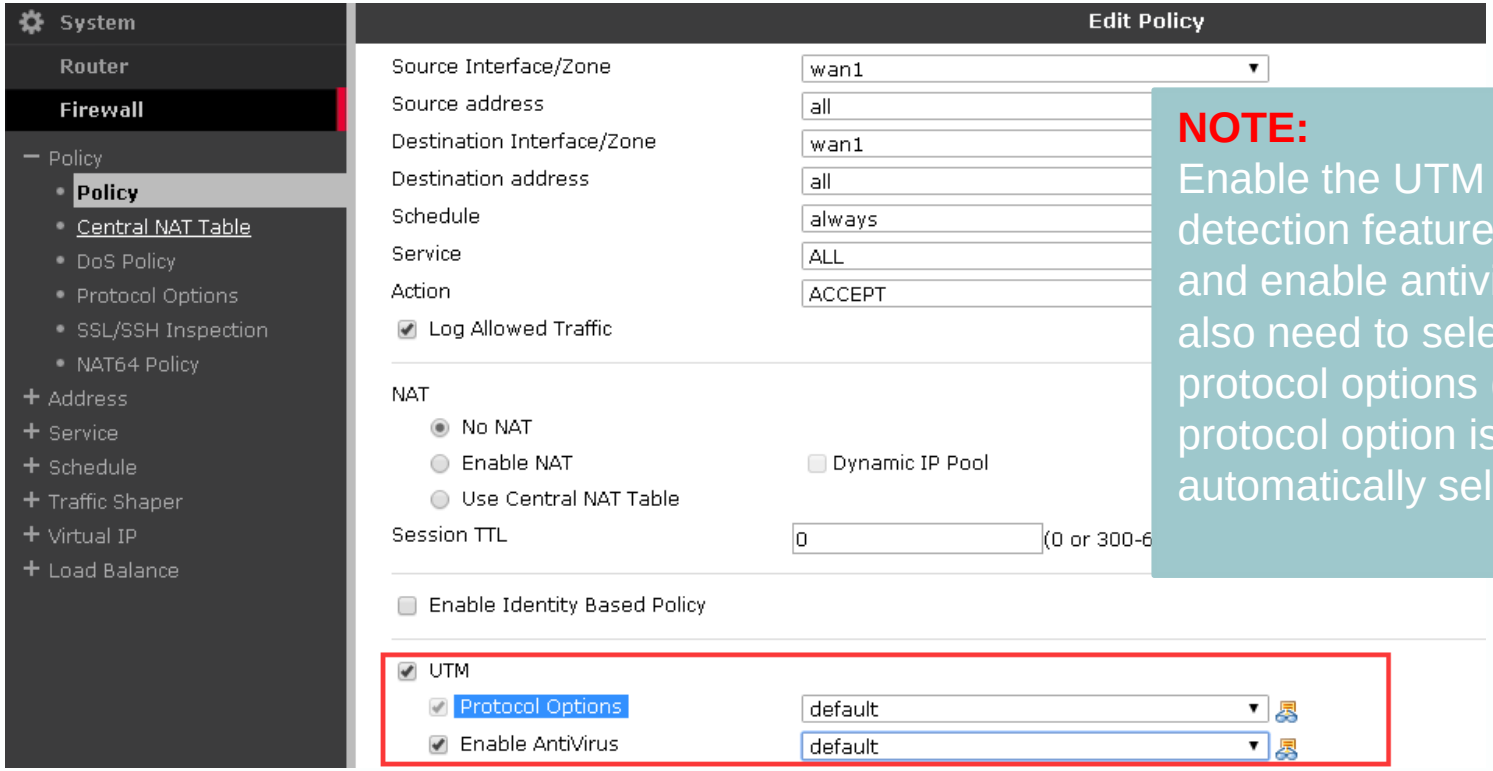
Step 3: Configure a policy for Internet access.



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

Fast configuration in transparent mode

Step 4: Enable the antivirus feature.



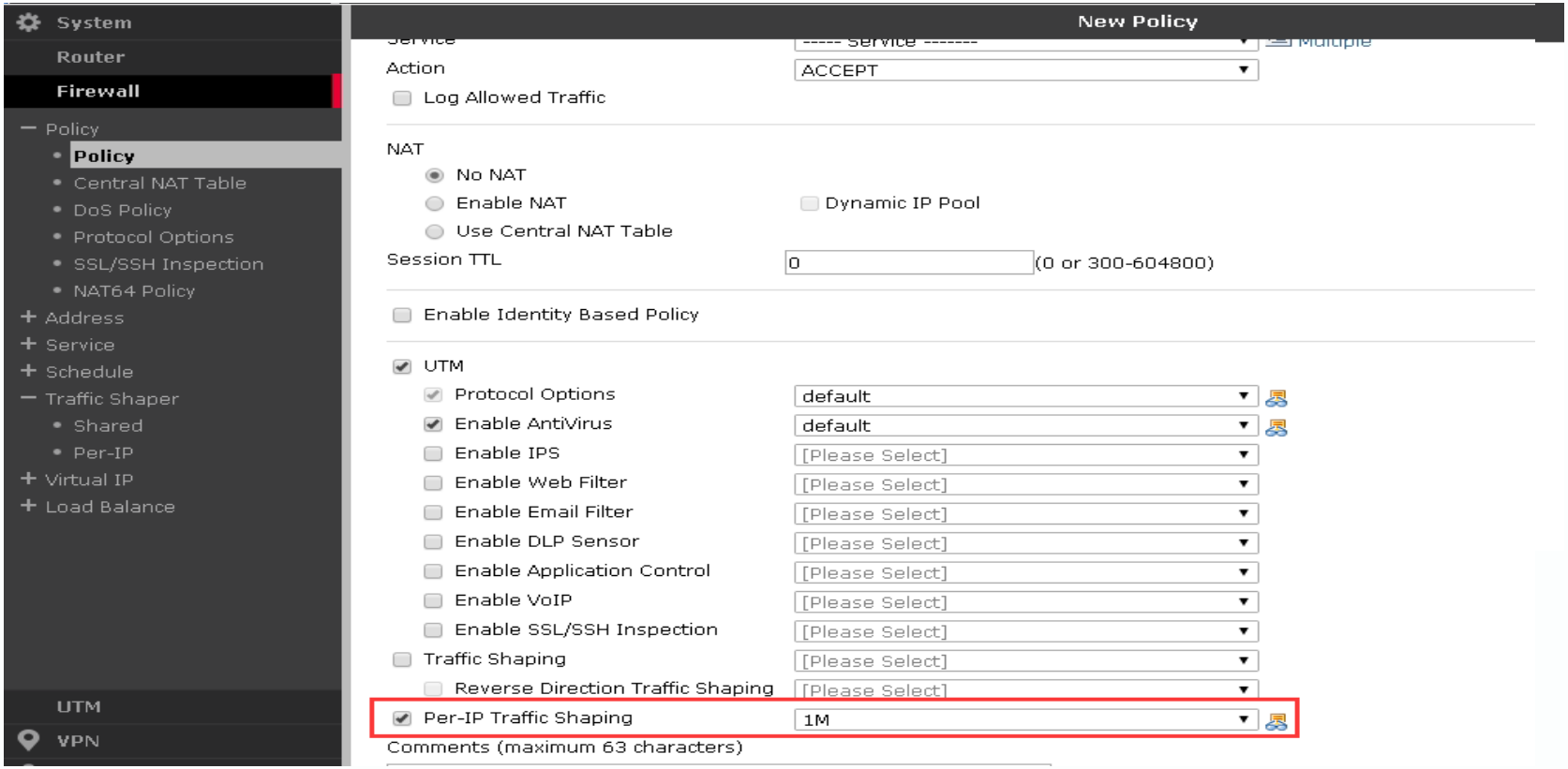
NOTE:
Enable the UTM virus detection feature and enable antivirus. You also need to select protocol options (the protocol option is automatically selected).

Security Policy

Device login | **Fast configuration** | Upgrade

Fast configuration in transparent mode

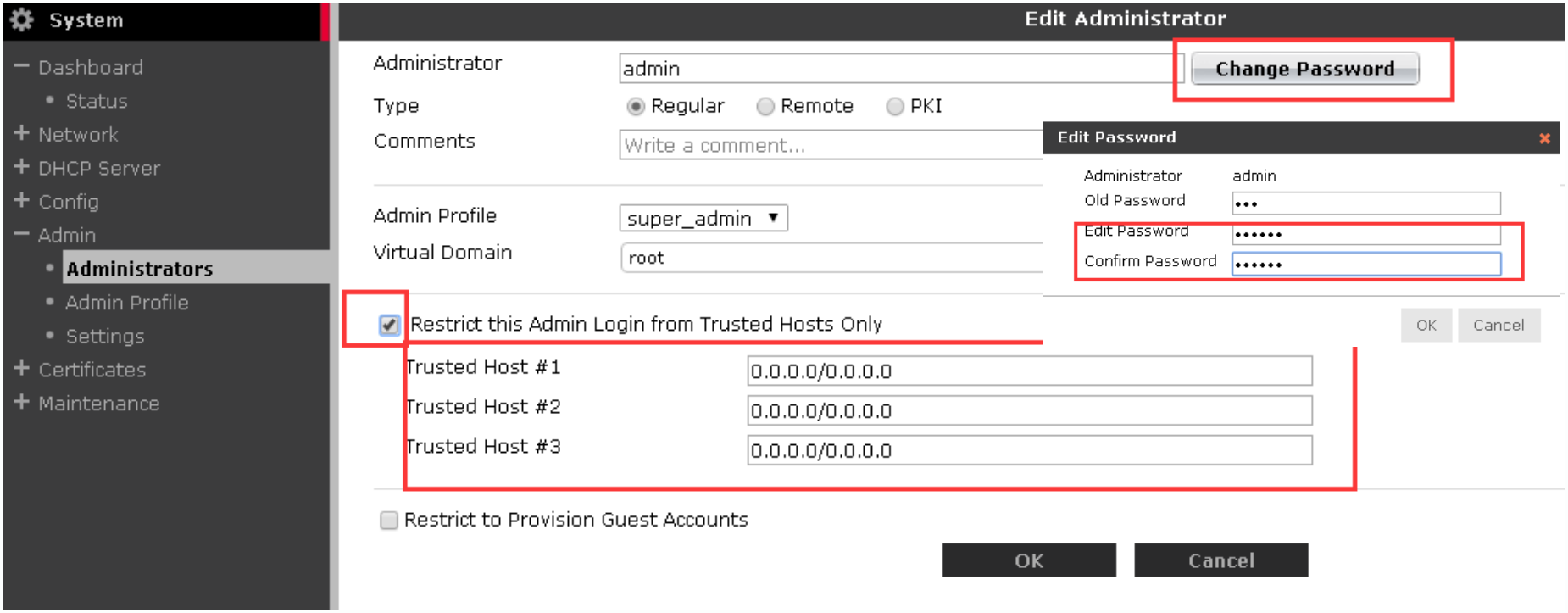
Step 5: Enable **trafficcontrol per ip address**.



Changing the Administrator Password

Device login | **Fast configuration** | Upgrade

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



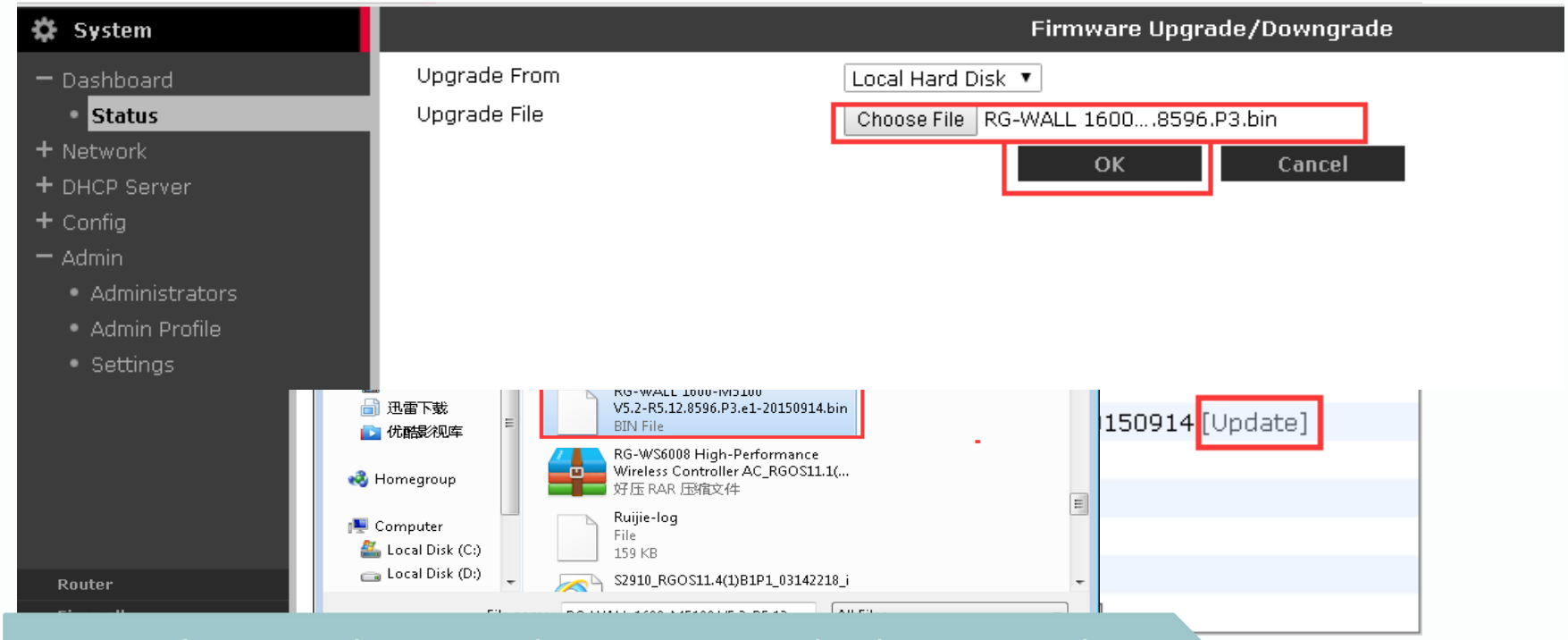
NOTE: After device configuration, you are advised to change the administrator account and password. Only the IP addresses of trusted hosts can be used to manage the firewall.

Initialization Setup

Device login | Fast configuration | Upgrade

Version upgrade

To upgrade the system version, do the following:



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.