# WS-431E 4G Router

# User Manual


Figure 1 WS-431E 4G Router

## 1. OVERVIEW

- Support 4G/3G/2G Internet access in various modes, which can be used in the fields of Internet of Networked Medical Treatment, Intelligent Agriculture, Smart City, Smart Robots, Security Monitoring Networking, Intelligent Bus Wifi etc.
- 1x WAN RJ45 port (configurable for LAN), 10/100 Mbps, supports automatic MDI/MDIX, 1.5KV electromagnetic isolation protection.
- 2 x LAN RJ45 port, 10/100 Mbps, supports automatic MDI/MDIX,1.5KV electromagnetic isolation protection.
- Support 1 WLAN(802.11b/g/n)
- Support Web Server
- Support LED to show work status
- Support Reload button to restore default settings by hardware way
- Support VPN client(PPTP/L2TP)
- Support one SIM card socket
- Support DDNS and port forwarding
- Support QoS and firewall

## CONTENTS

# 2. PRODUCT OVERVIEW

## 2.1. INTRODUCTION

The WS-431E 4G Router is a new Qualcomm solution Wi-Fi enhanced industrial router with excellent anti-interference capability and stable connection performance, supports WIFI hotspot, WIFI client, and WIFI relay modes, and is integrated with 4G LTE, Wi-Fi, Ethernet ports (2LAN and 1WAN/LAN) and VPN technologies.

The WS-431E can provide advanced Internet connectivity and high-speed data access for the devices, allowing users to quickly build their own application network, and also helping enterprise customers achieve efficient large-scale network deployment and management. It is suitable for various IoT and M2M solutions such as service robots, inspection robots, unmanned vehicle networking, massage chair networking, AGV car, and other industrial application scenarios.

## 2.2. SPECIFICATIONS

| CELLULAR NETWORK PARAMETERS | |
|---|---|
| Frequency band | TDD-LTE: B38/40/41<br>FDD-LTE: B1/3/7/8/20/28A<br>WCDMA: B1/8<br>GSM/EDGE:B3/8 |
| **WIFI** | |
| Standard | IEEE 802.11b/g/n，2.4GHz |
| Data speed | 300Mbps |
| MIMO | 2×2 |
| Transmission distance | 500 meters with an open field, the actual transmission distance depends on the environment of the site |
| **INTERFACES** | |
| WAN/LAN | 1× WAN RJ45 port (can be configured as LAN), 10/100 Mbps, supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection |
| LAN | 2× LAN RJ45 port, 10/100 Mbps, supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection |
| SIM card slot | Supports standard Nano (3 V/1.8 V) |
| Antenna | SMA-K standard antenna connector, comes with 1x 4G antennas, 2x WiFi antennas by default |
| TBD | Debug interface |
| Reload button | Supports factory restore |
| Grounding screw | Grounding protection |

| INDICATORS | |
|---|---|
| PWR | Power indicator, lights up after powered on |
| WIFI | Lights up when WiFi is enabled |
| 2/3/4G network indicator | 2G led lights up after being connected to 2G network<br>3G led lights up after being connected to 3G network<br>Both leds light up after being connected to 4G network |
| SIG | 2× signal strength indicator: lights up one indicates that the signal is average; lights up two indicates that the signal is strong |
| **POWER SUPPLY** | |
| Power adapter | DC 12V/1A |
| Input voltage | DC 9-36V |
| Power consumption | Average 260mA/12V |
| **PHYSICAL CHARACTERISTICS** | |
| Operating temperature | -20℃~+70℃ |
| Storage temperature | -40℃～+125℃（non-condensing) |
| Relative humidity | 5%~95%（non-condensing） |
| Case material | Metal case, IP30 protection level |
| Dimensions (L × W × H) | 104.0×102.0×28.0mm |
| Installation | DIN rail mounting, wall mounting, tabletop |
| EMC | level 3 |

## 2.3. INTERFACE DESCRIPTION

The interface description as follows：

Figure 2 Interface description

The SIM card does not support hot swap. Therefore, install or replace the SIM card with the power off.

## 2.4. HARDWARE SIZE

The hardware dimensions as follows:


Figure 3 Interface description

- Sheet metal shell, fixed holes on both sides, compatible with rail mounting parts
- Length, width and height are 102*104*28mm (excluding power terminal, antenna and antenna base)
- Installation method: 35mm guide rail installation, hanging ear installation.

# 3. QUICK START

4G router provides a wireless remote fast networking solution for user devices, and parameters are set through the built-in web page to meet the application scenario.This chapter is a quick introduction to WS-431E router products. It is recommended that users read this chapter and follow the instructions to have a basic understanding of 4G router products. Refer to subsequent sections for specific functional details and descriptions.

### 3.1.1. HARDWARE ENVIRONMENT

Product test data flow topology:


**Figure 4 Get started testing data flow diagrams**

- Hardware: 1 PC, 1 set of router (including antenna, power adapter), 1 network cable (self-provided), 4G SIM card (self-provided)
- Wiring: The computer is connected to the LAN port of the WS-431E through the network cable, and the WiFi antenna and the full-frequency antenna are connected to the corresponding antenna interface in turn
- Networking: Insert the SIM card in the power off state (the front of the card slot corresponds to the positive direction of the "sim "screen printing)
- Power supply: The working voltage of the WS-431E is DC5-36V. You are advised to use the DC 12V/1A power adapter provided by the factory
- After power-on, observe the indicators: the PWR is on, the LAN is blinking, the 4G indicator (3G+2G) is on, and the indicator is all on, indicating that the signal is good


Figure 5 4G indicator (3G+2G)

### 3.1.2. NETWORK CONNECTION

Internet test: Power on the WS-431E, wait for about 2 minutes, the 2/3G indicator starts to light, indicating that the 4G network of the router is successful, then you can directly surf the Internet. Let's go to the Settings to check the network status through the default parameters of WS-431E.

Default parameters of WS-431E as follows:

| SSID | WS-431E-XXXX |
|---|---|
| IP Address | 192.168.1.1 |
| User name | admin |
| Password | admin |
| WLAN Password | www.waveshare.com |

Take default parameters as example: User can connect PC to SSID WS-431E-XXXX. Then open browser and enter 192.168.1.1, log in with User name and Password(both are admin), user can enter WebServer.

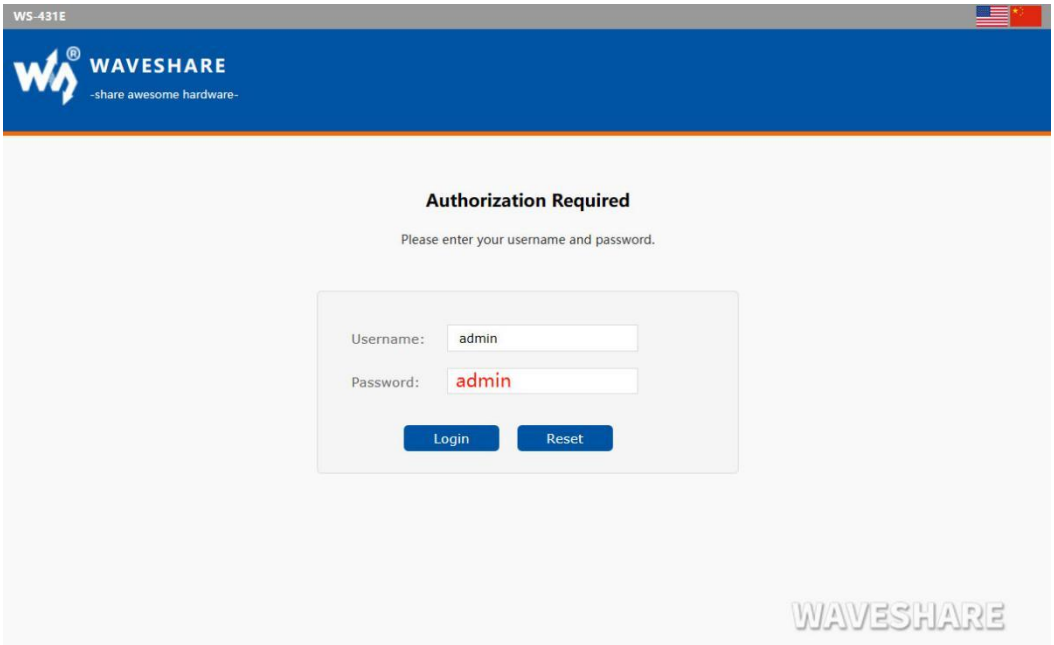



Figure 6 Web Server login web

Enter admin for the user name and password. On the left menu bar, select Network => Network Diagnosis => ping. If the domain name can be pinged, the network connection is normal. You can also directly open the browser and enter the URL of the website you want to land.

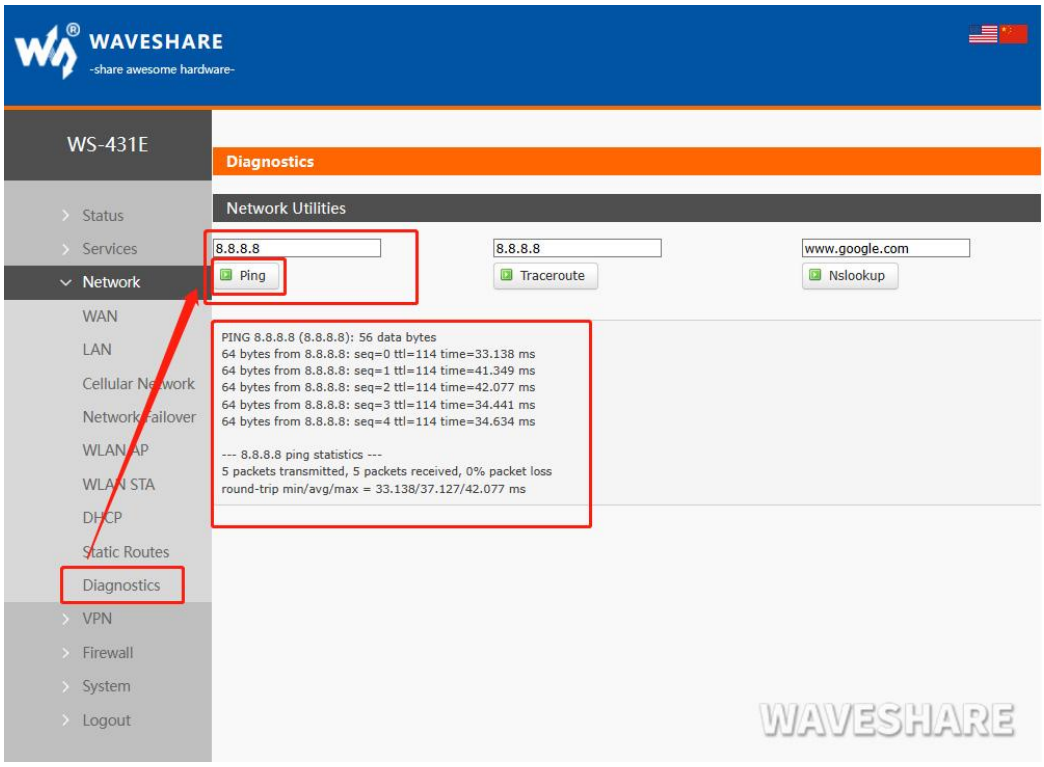



Figure 7 Network diagnosis page

# 4. PRODUCT FUNCTIONS

This chapter introduces the functions of WS-431E, as the following diagram shown, you can get an overall knowledge of it.


Figure 8 Product functions

## 4.1. INSTALL PROCEDURE

(1) Connect the 4G antenna and Wi-Fi antenna to the router. (Shorter one is 3G/4G antenna and Longer one is Wi-Fi antenna.)

(2) Plug the SIM card in socket.

(3) Power on the module by power adaptor and check the LED status.

(4) Connect PC or mobile to the WS-431E router via LAN interface or Wi-Fi interface. Wi-Fi password is “www.waveshare.com”.

(5) Log in Web Server of router. (Default IP address of router is 192.168.1.1, either the username and password is “admin” .)

(6) Configure APN parameters according to SIM card. Some SIM card APN can be recognized automatically.

(7) Configure other parameters according to user applications.

## 4.2. APN

### 4.2.1. APN CONFIGURATION BY WEB SERVER

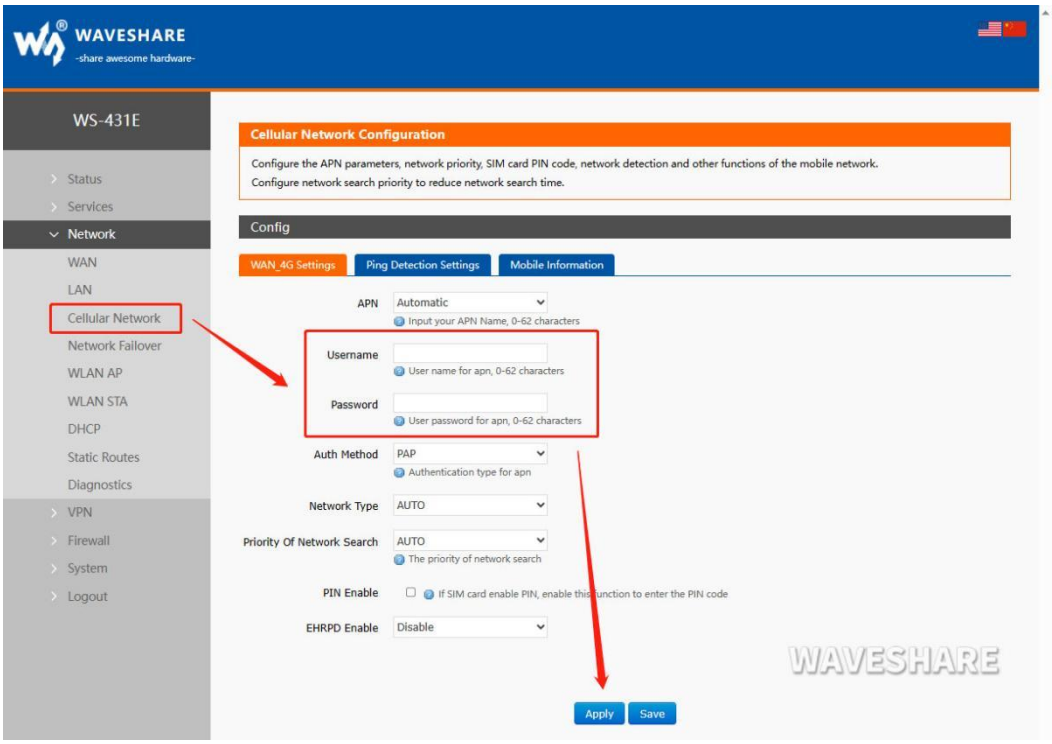



Figure 9 APN configuration

## 4.2.2. CREATE A VPN CLIENT

User can set VPN client configuration by Web Server as follow:

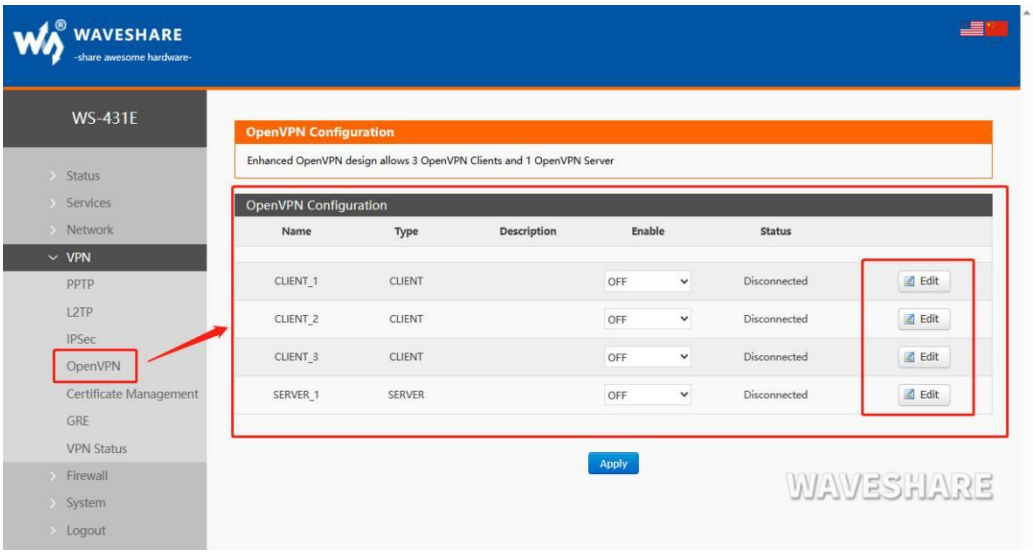



Figure 10 VPN Client

# 4.3. NETWORKING MODE

## 4.3.1. WAN+LAN+4G

In this networking mode, user can access internet through WAN interface and 4G interface. WAN interface has higher priority than 4G interface to ensure communication and save 4G flows. When WAN interface occurs problems, router can change to 4G interface to connect internet. In this mode, user can also connect to router through WIFI.

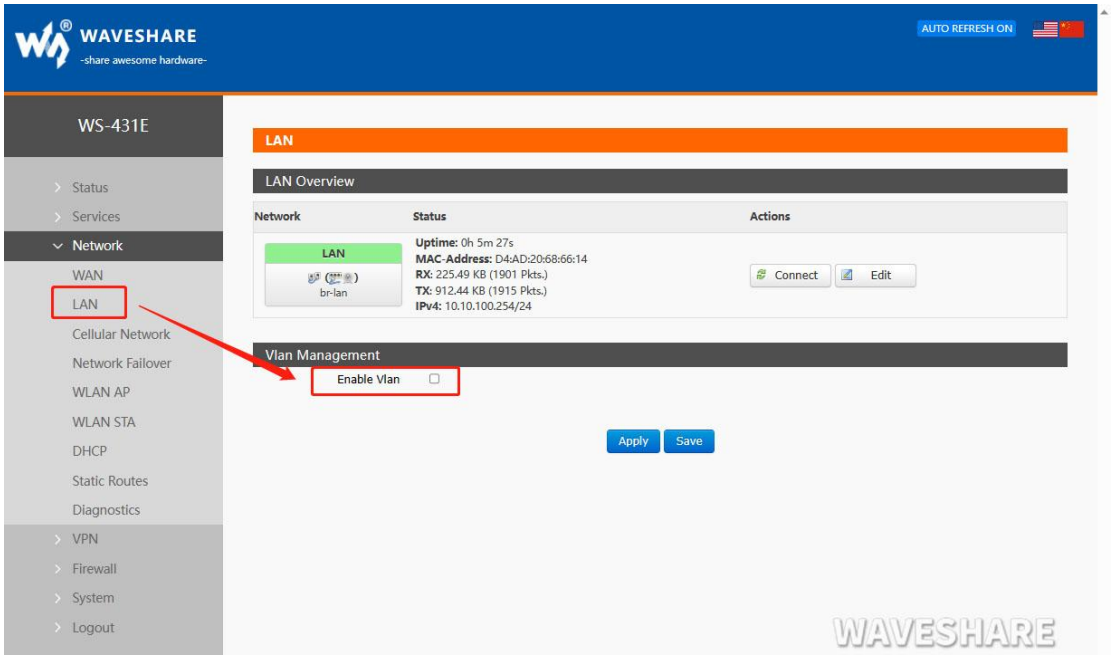
To achieve this mode, user don't need to change the router's parameters. Just connect the cable to router and insert SIM card, then power the router.

Application diagram as follow:


Figure 11 WAN+LAN+4G networking

### 4.3.2. LAN+LAN+4G

In this networking mode, three devices can connect to router through LAN and access the Internet by 4G network. User can achieve this by Web Server as follow:



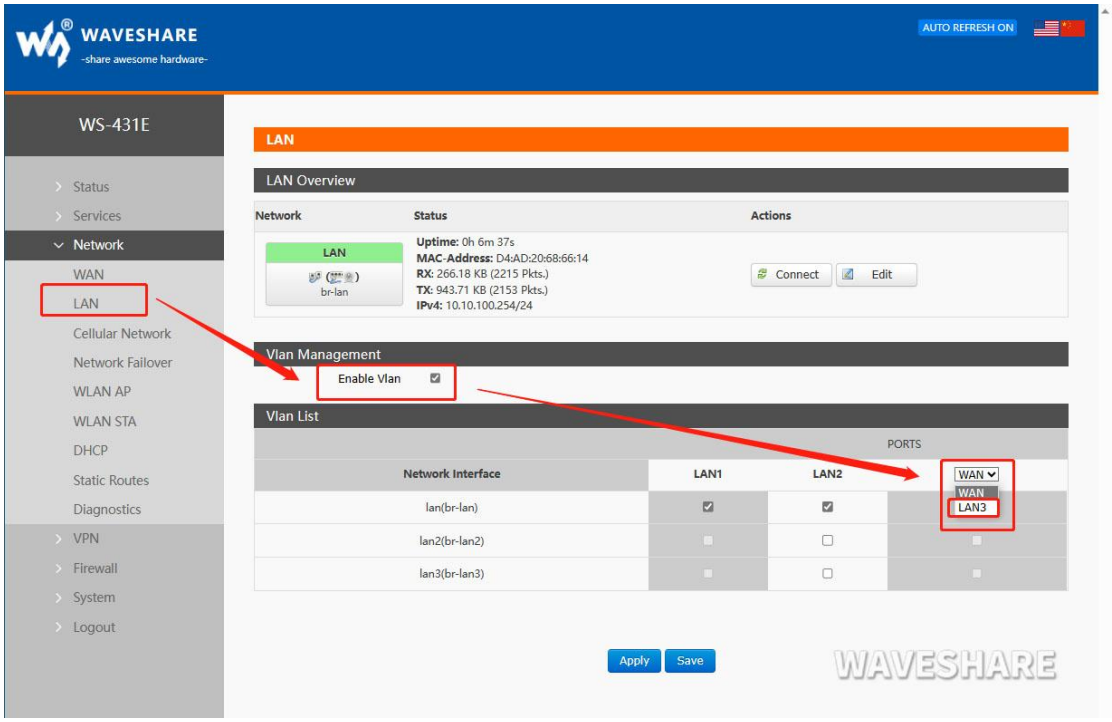




**Figure 12 Switch WAN/LAN interface**

Application diagram as follow:


Figure 13 LAN+LAN+4G networking

## 4.4. COMMON FUNCTIONS

### 4.4.1. 4G INTERFACE

WS-431E 4G Router supports one 4G interface to access internet. Functional diagram as follow:

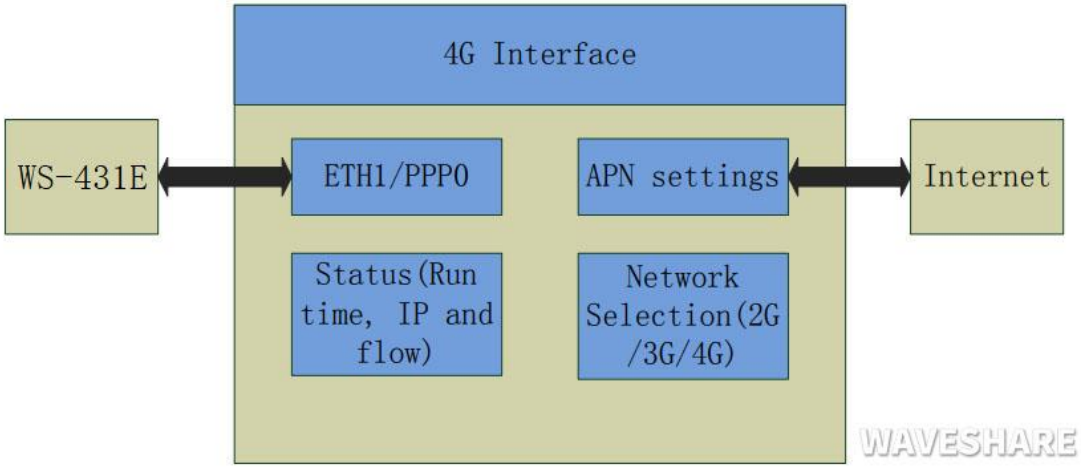



Figure 14 4G interface

User can configure 4G interface by Web Server as follow:

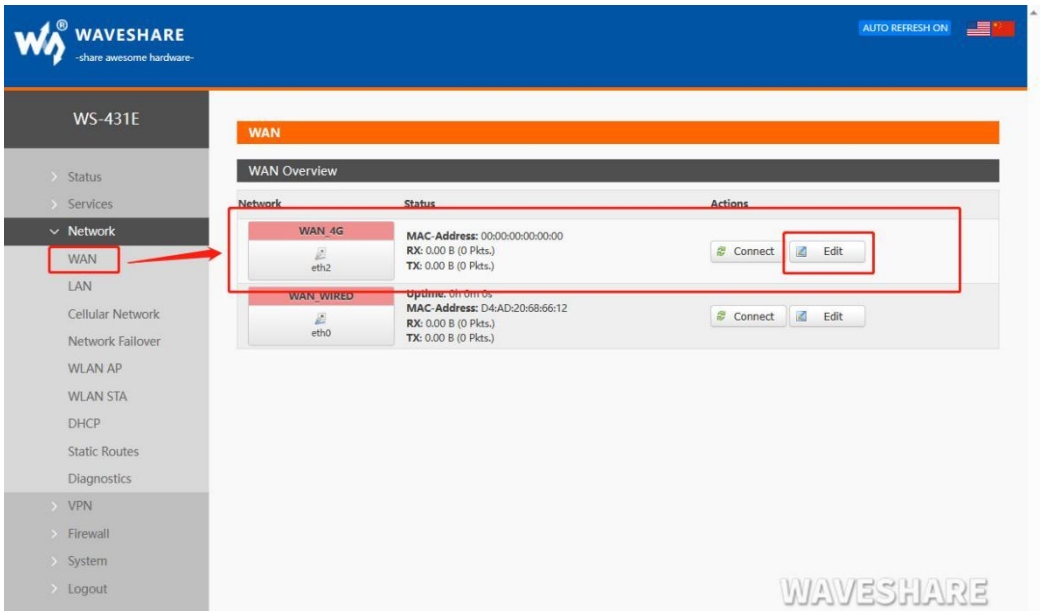



Figure 15 4G interface

## 4.4.2. LAN INTERFACE

WS-431E supports two LAN interface (one is WAN/LAN interface).

Default settings: One LAN interface (WAN/LAN used as WAN interface; IP address: 192.168.1.1; Subnet mask: 255.255.255.0; Open DHCP function).

User can configure LAN interface by Web Server as follow:

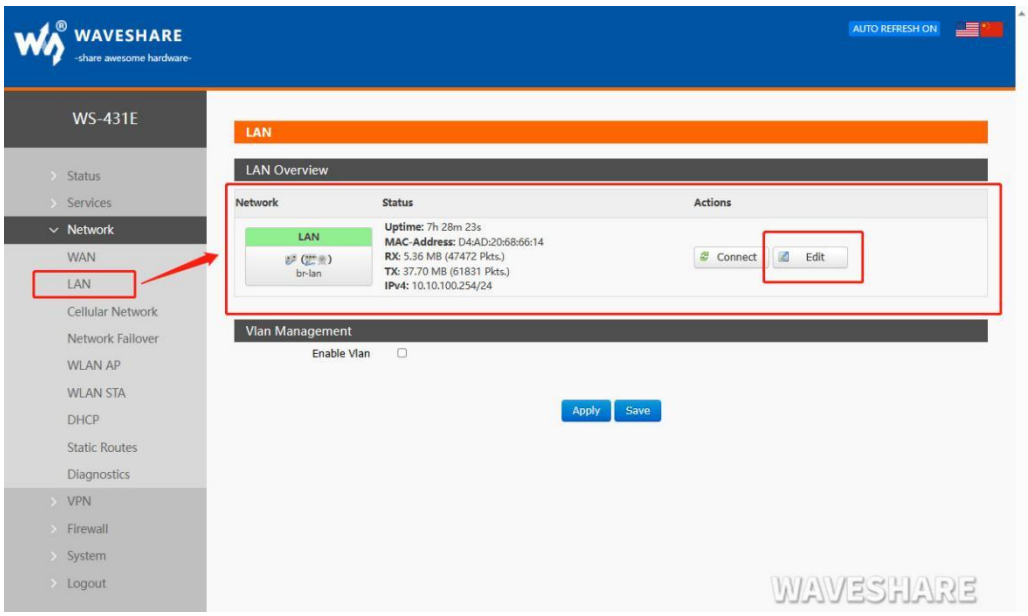



Figure 16 LAN interface

DHCP default range of distribution is from 192.168.1.100 to 192.168.1.250 and default address lease time is 12 hours. Address range and lease time can be changed.

you can find 'DHCP Server'as follow:

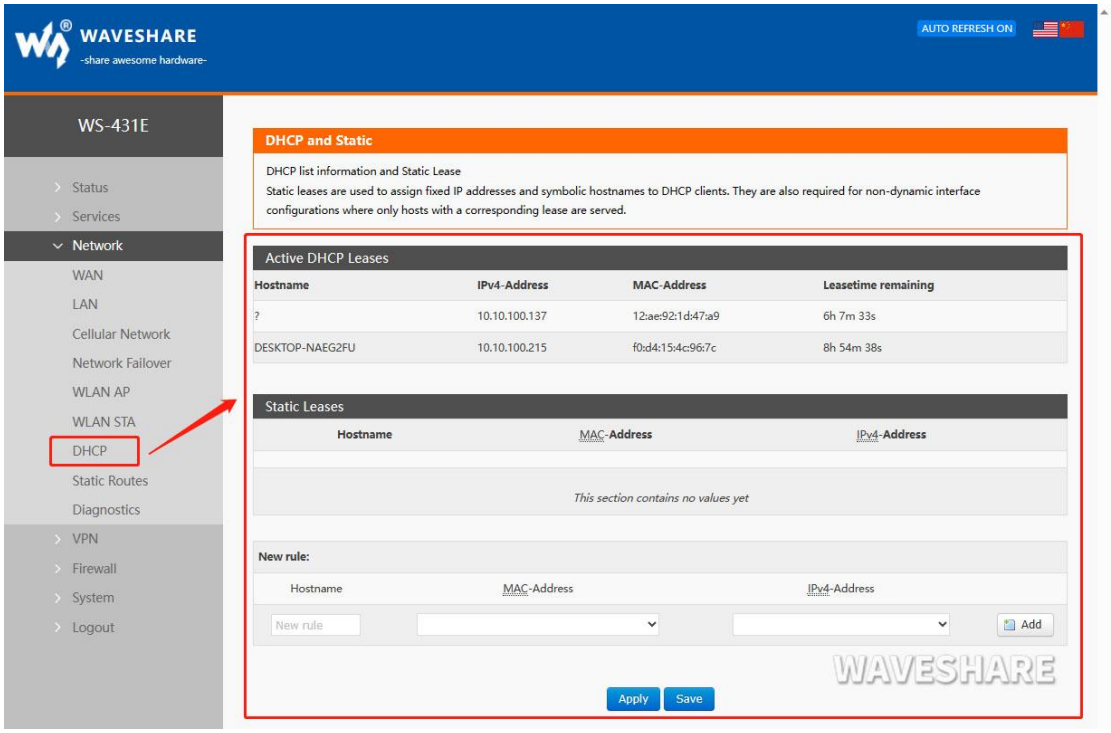



Figure 17 DHCP function

## 4.4.3. WAN INTERFACE

WS-431E supports one WAN interface and WAN interface can switch between WAN/LAN interface. WAN interface supports DHCP and Static IP, and default setting is DHCP. User can configure WAN interface by Web Server as follow:

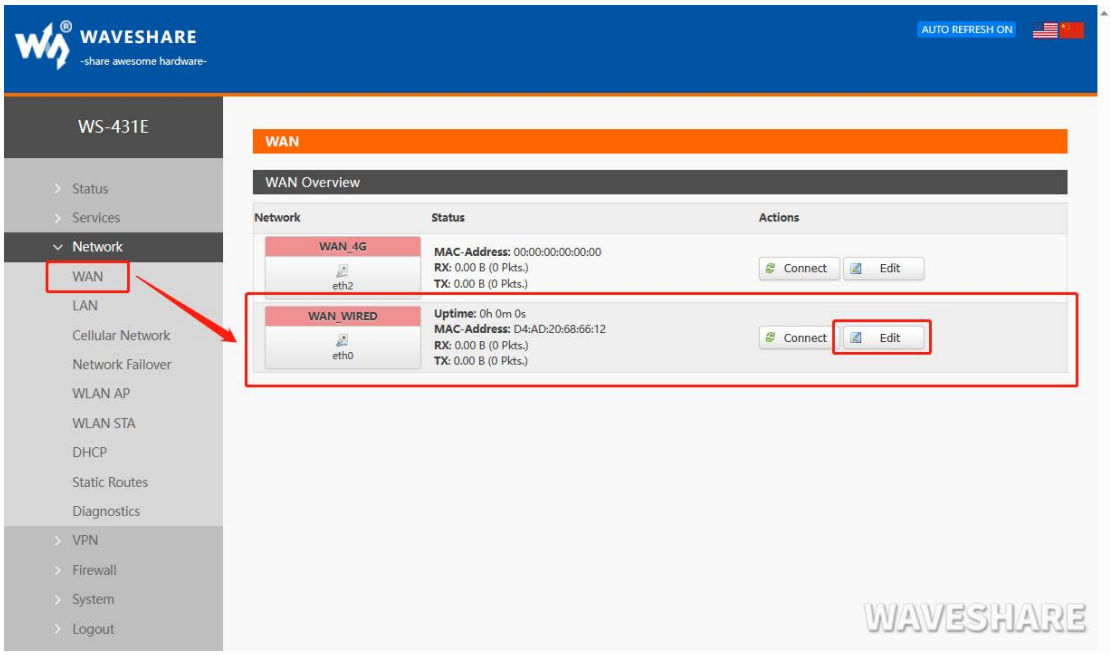


Figure 18 WAN interface

### 4.4.4. WLAN INTERFACE

Default parameters as follows:

| SSID | WS-431E-XXXX(XXXX 是 MAC) |
|---|---|
| Password | www.waveshare.com |
| Channel | auto |
| HT Mode | auto |
| Encryption | mixed-psd |

Figure 19 WLAN default parameters

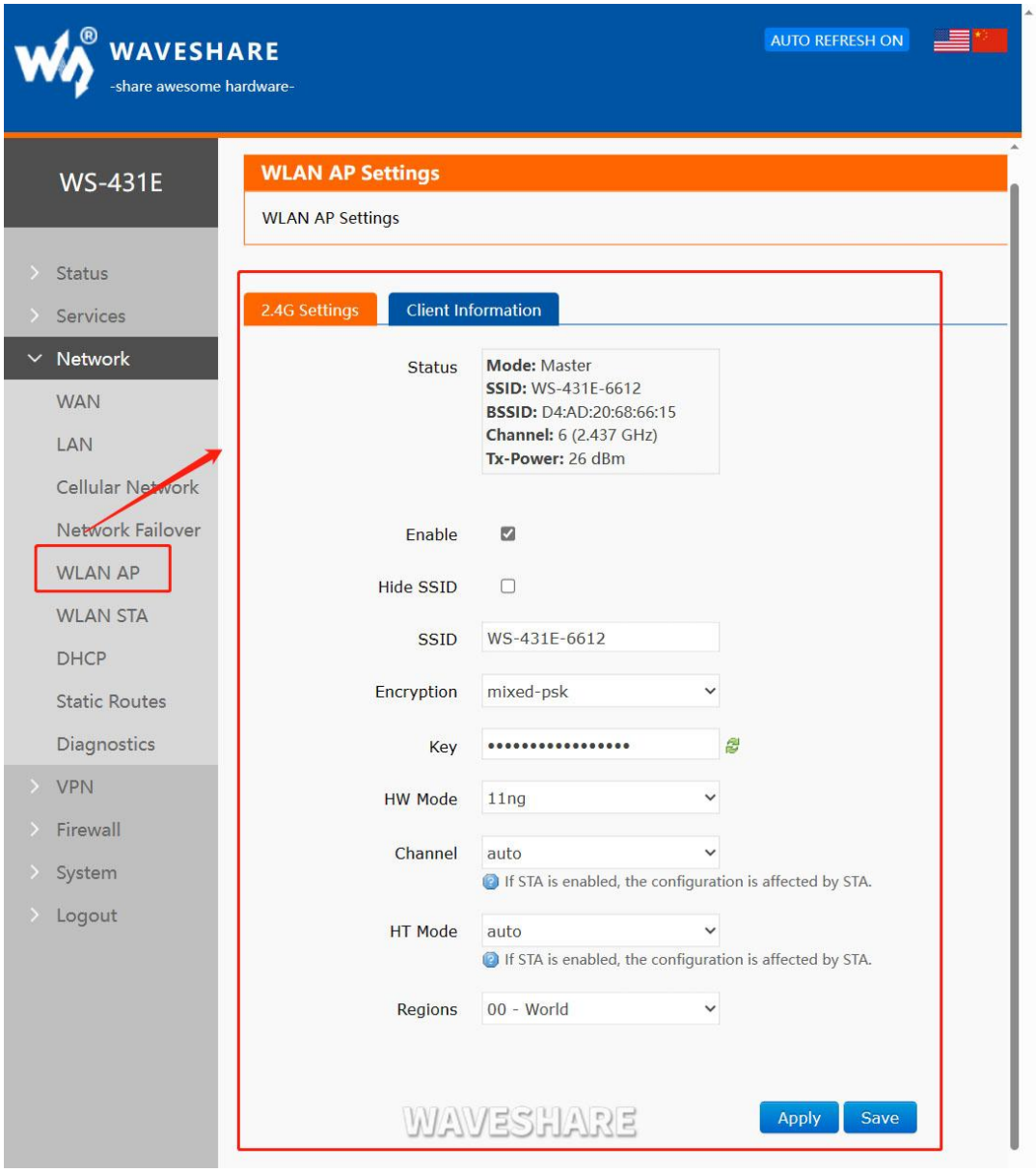



Figure 20 WLAN interface

Entering WLAN interface configuration web, user can change follow parameters. User can configure SSID on Web Server as follow:

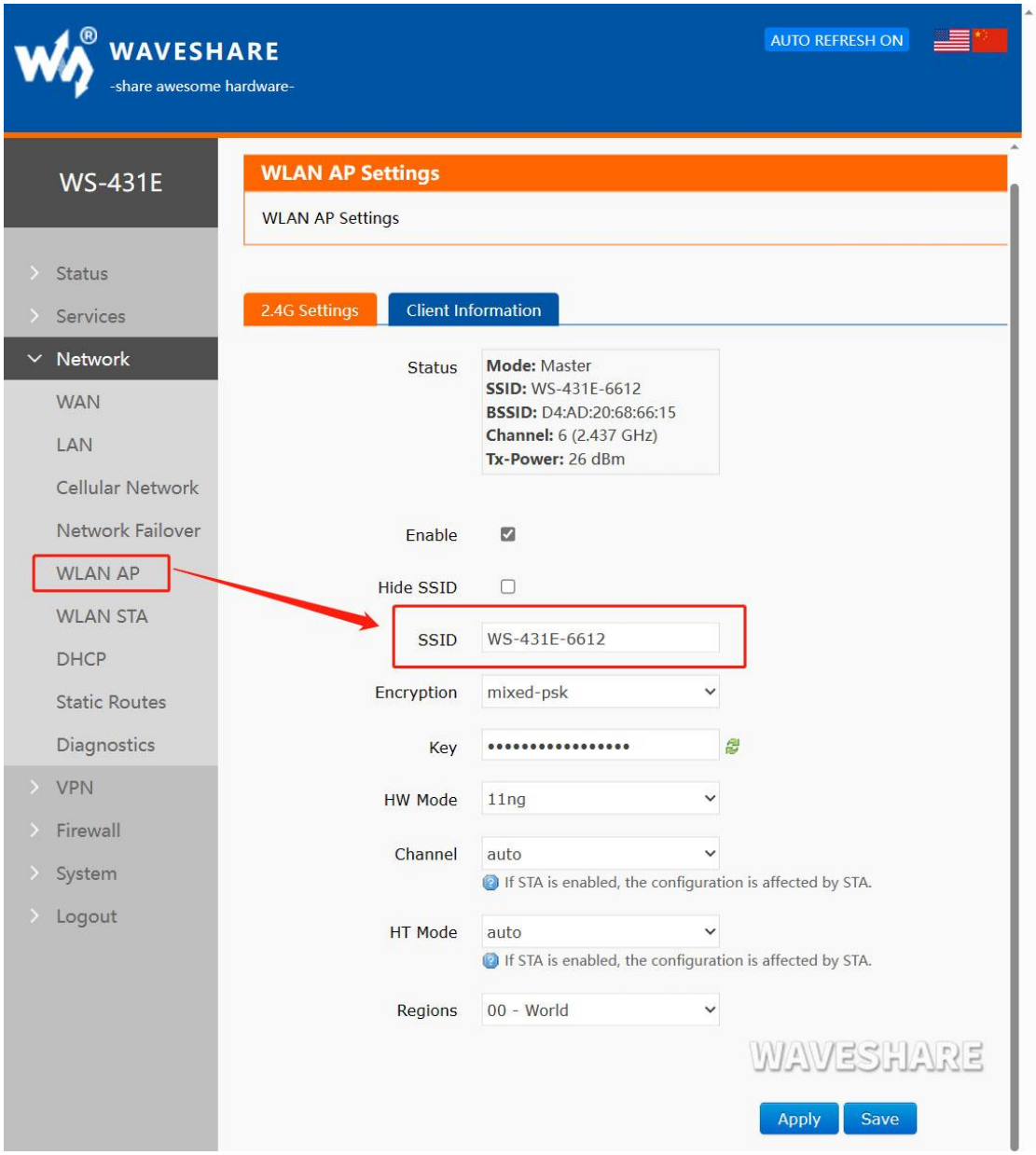



**Figure 21 WLAN interfaceConfigure SSID**

User can configure password on Web Server as follow:

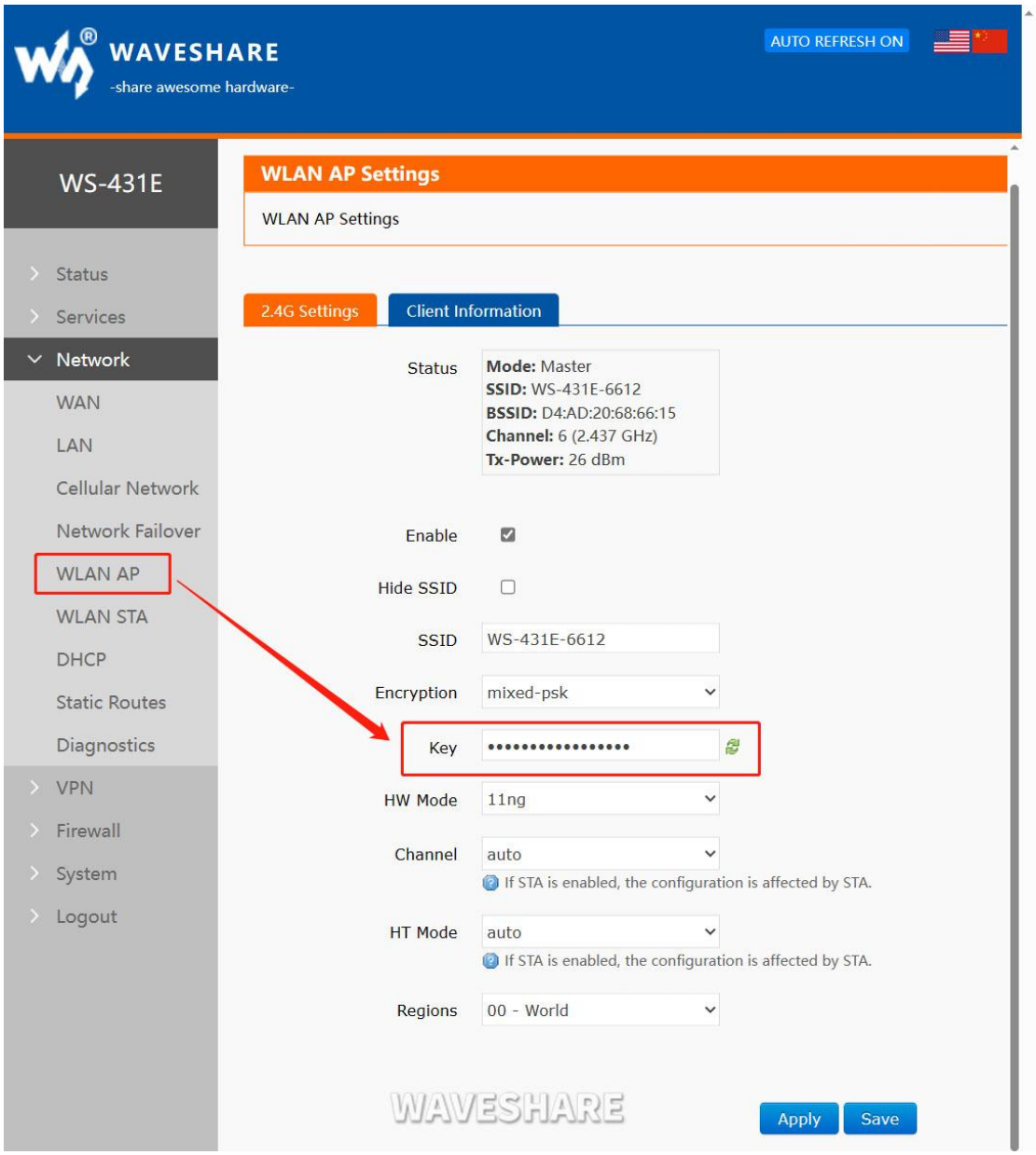



**Figure 22 Configure password**

Other settings on Web Server as follow:

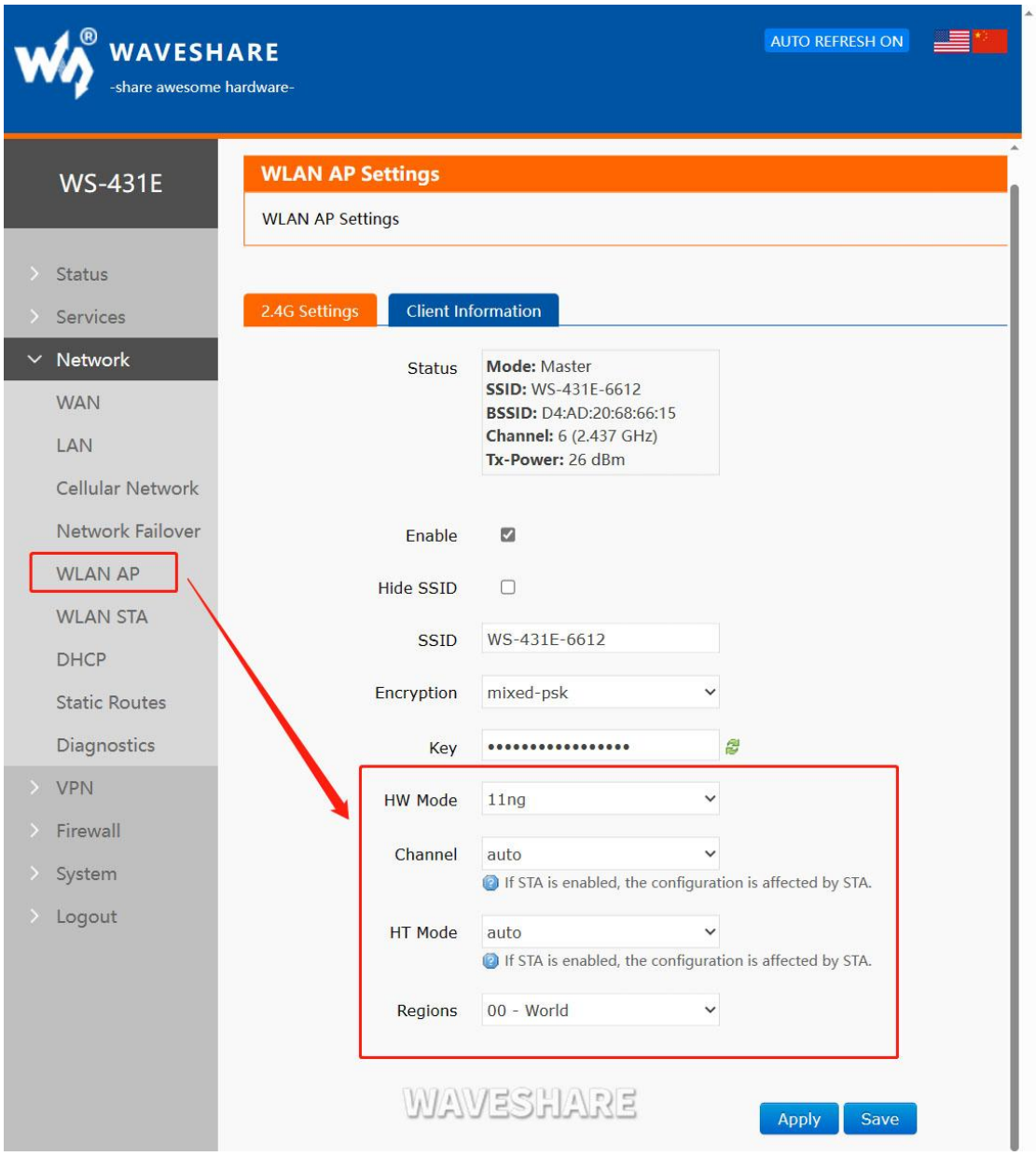



Figure 23 Other settings

You can view the list of wifi clients on the wireless screen：

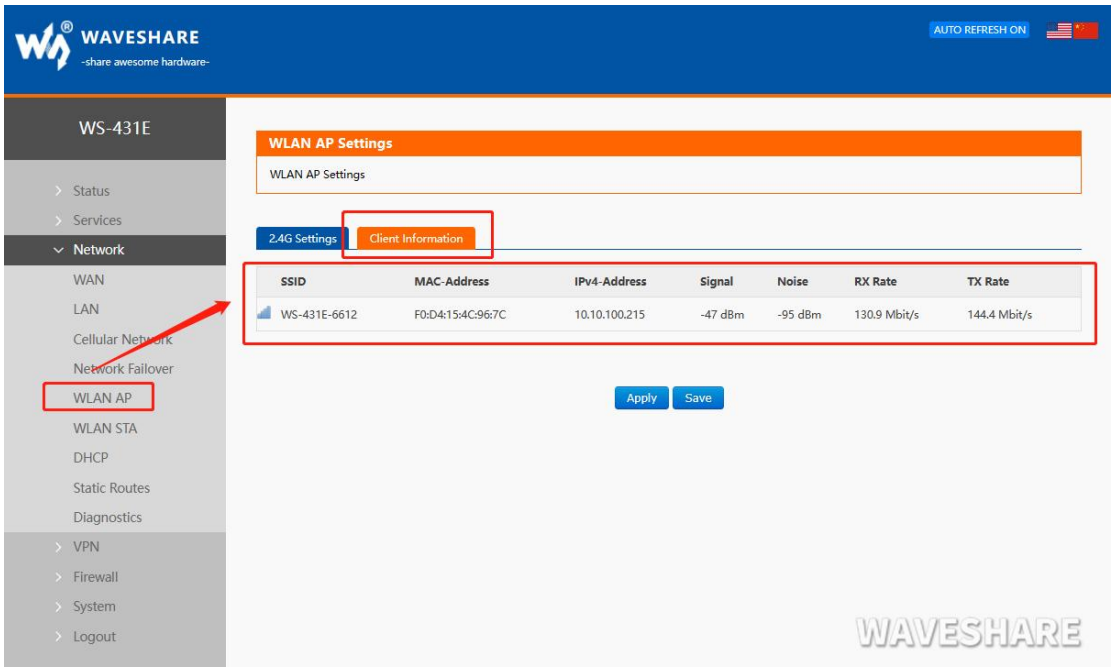



Figure 24 WiFi client list page

## 4.4.5. NETWORK DIAGNOSIS

User can use network diagnosis function by Web Server as follow:

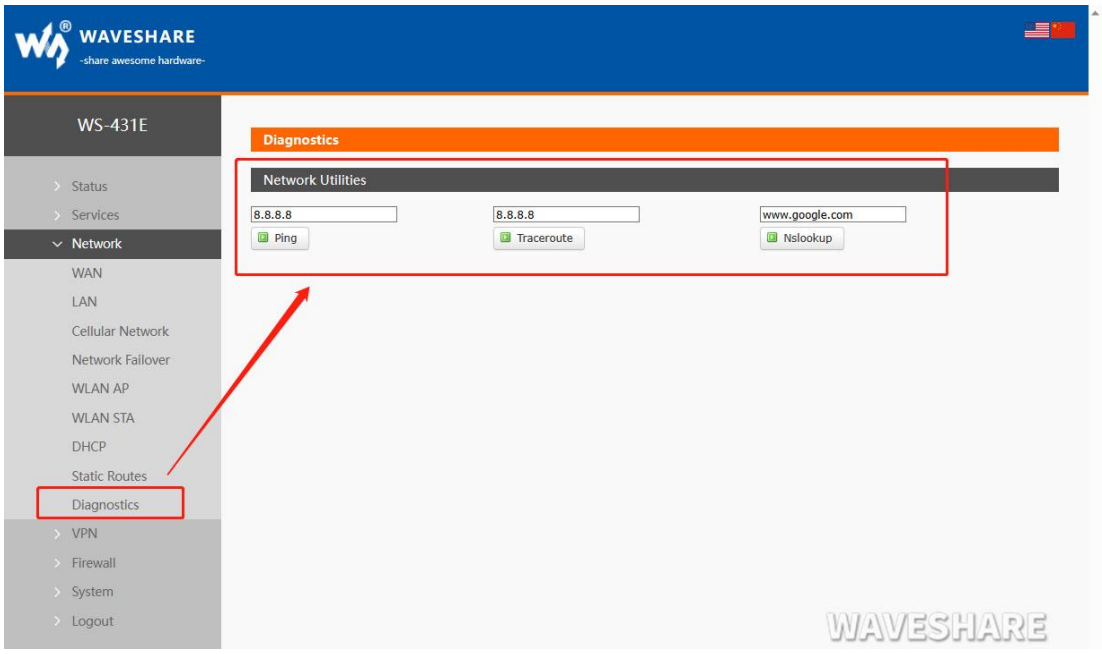



Figure 25 Network diagnosis

- Ping: User can do PING test to a specific address in WS-431E.
- Traceroute: Can acquire routing path to visit a specific address.

- Nslookup: Can analyse DNS into IP address

### 4.4.6. MODULE NAME AND TIME ZONE

WS-431E default module name is WS-431E and default Time Zone is New York time zone.

User can configure module name and Time Zone by Web Server as follow:

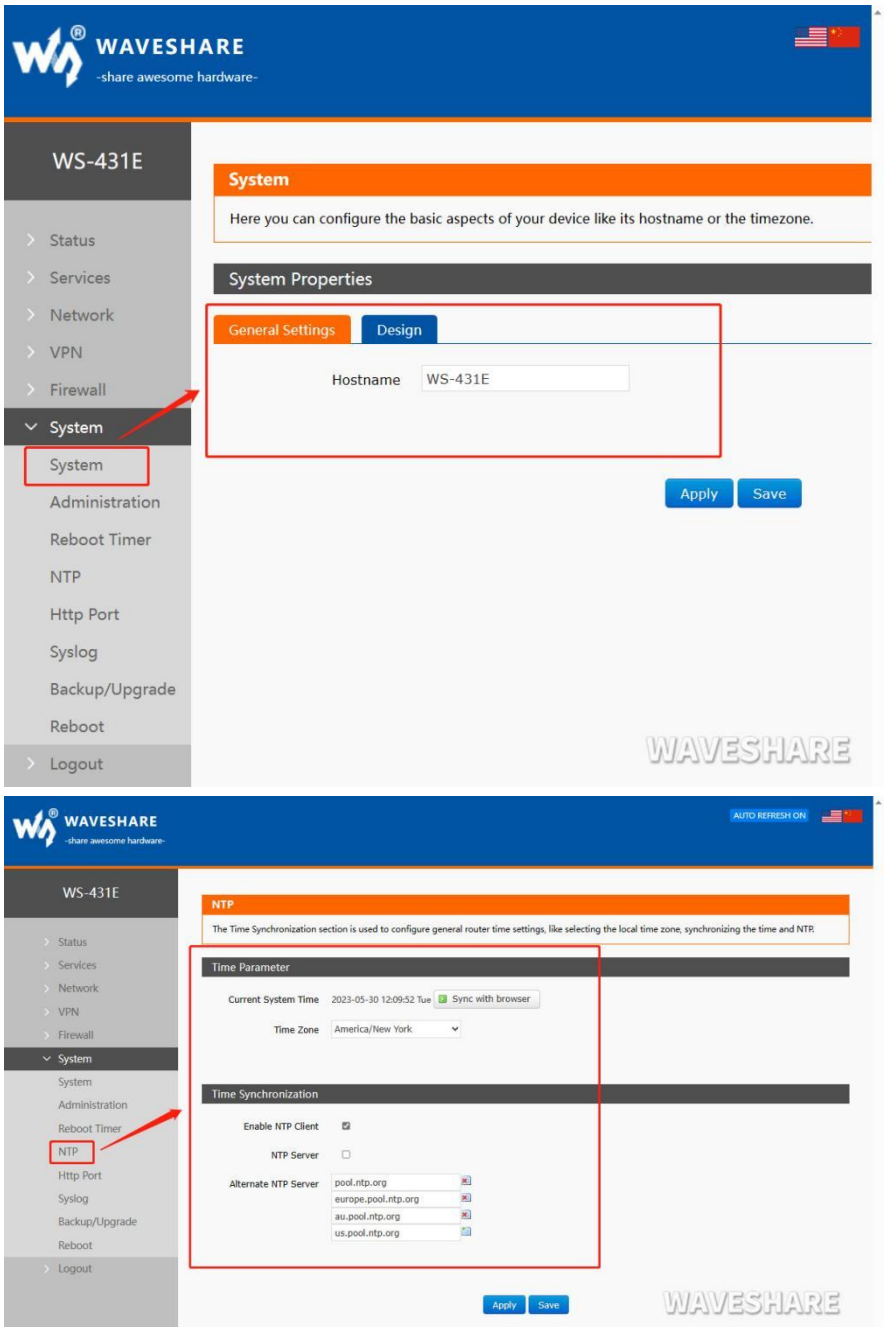



**Figure 26 Module name and Time Zone**

### 4.4.7. STATIC ROUTE

The static route has the following parameters. By default, a maximum of 20 static routes can be added.

| Name | Description | Default parameter |
|---|---|---|
| port | Lan, wan_4G, wan_wired, vpn interfaces | Lan |
| Object (destination address) | The address or address range of the object to be accessed | empty |
| Subnet mask | The subnet mask of the object network to be accessed | empty |
| Gateway (Next hop) | The address to forward to | empty |
| Metric | Number of packet hops | empty |

Figure 27 Static route parameter table

Static route describes the routing rules of Ethernet packets.Test example: Test environment, two flat routers A and B, as shown below.

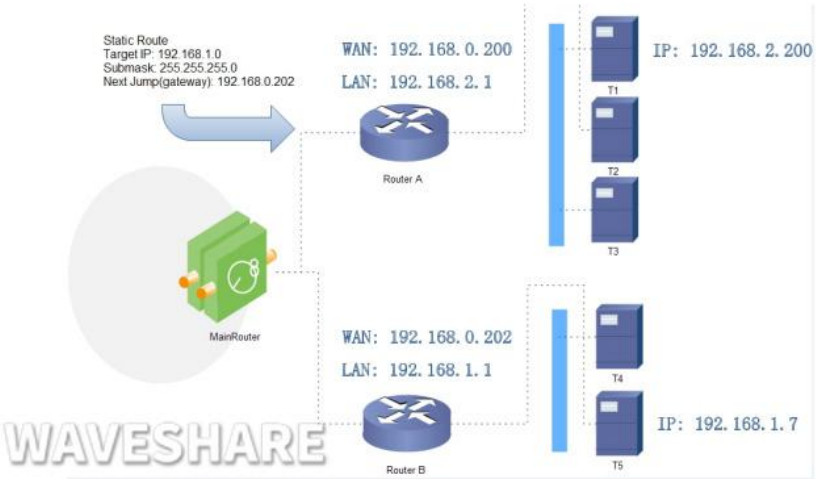



Figure 28 Static routing table example diagram

The WAN ports of routers A and B are connected to the network at 192.168.0.0. The LAN port of router A is on the 192.168.2.0 subnet, and the LAN of router B is on the 192.168.1.0 subnet.Now, if we want to make A route on router A so that when we access the 192.168.1.x address, it is automatically forwarded to the router

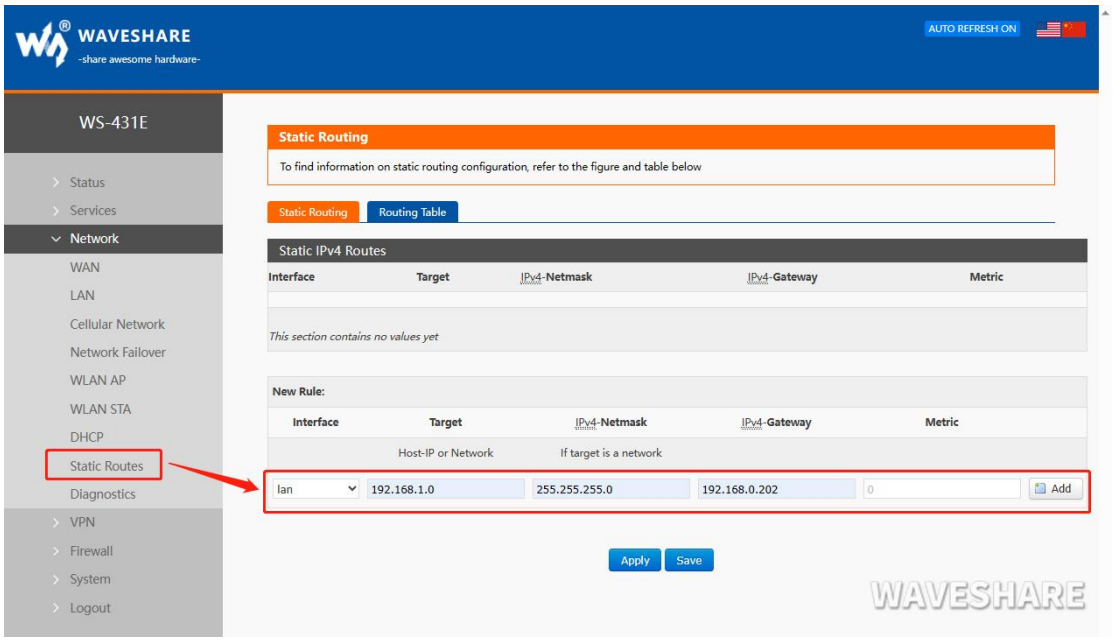



Figure 29 Add routing table page

## 4.5. BASIC FUNCTIONS

### 4.5.1. WEB SERVER PASSWORD

Default password is root, this password is used to enter Web Server.

User can change password by Web Server as follow:

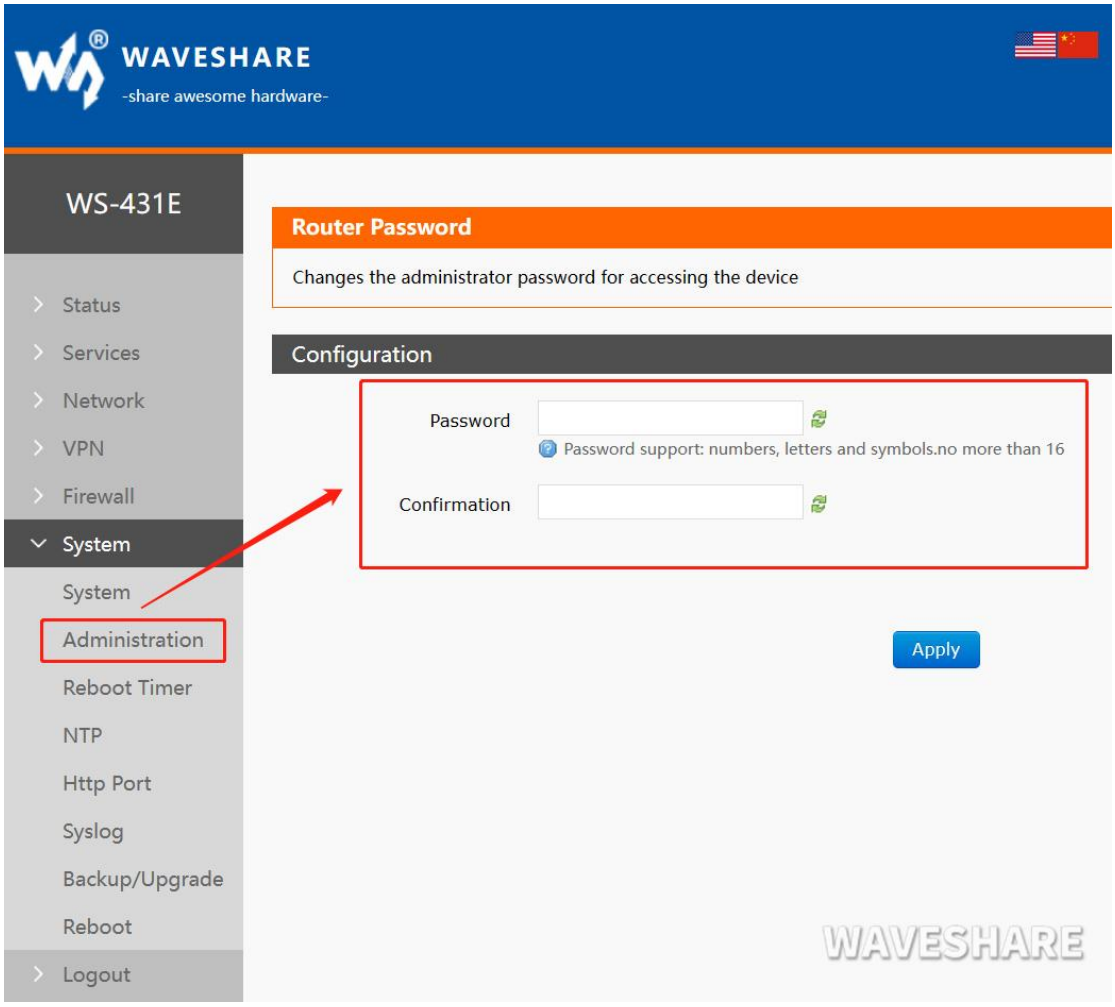



Figure 30 Web Server password

### 4.5.2. RESTORE

Hardware restore: Press Reload button over 5 seconds and release, WS-431E will restore default settings and reset.

User can restore default settings by Web Server as follow:

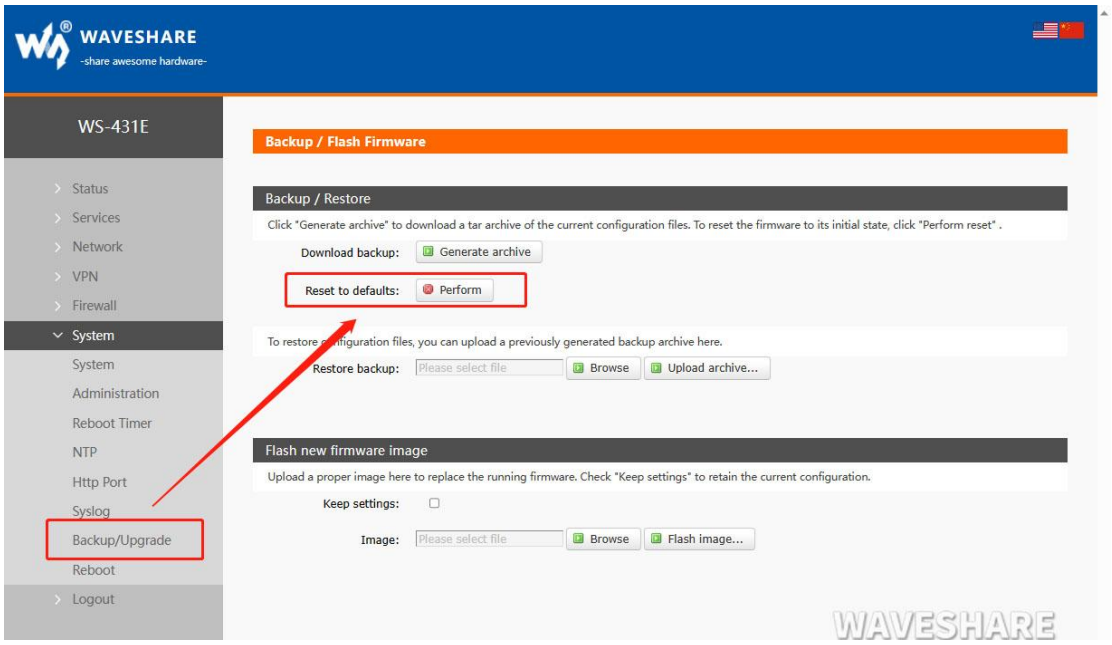



Figure 31 Restore default settings

## 4.5.3. UPGRADE FIRMWARE VERSION

Upgrade by Web Server as follow:

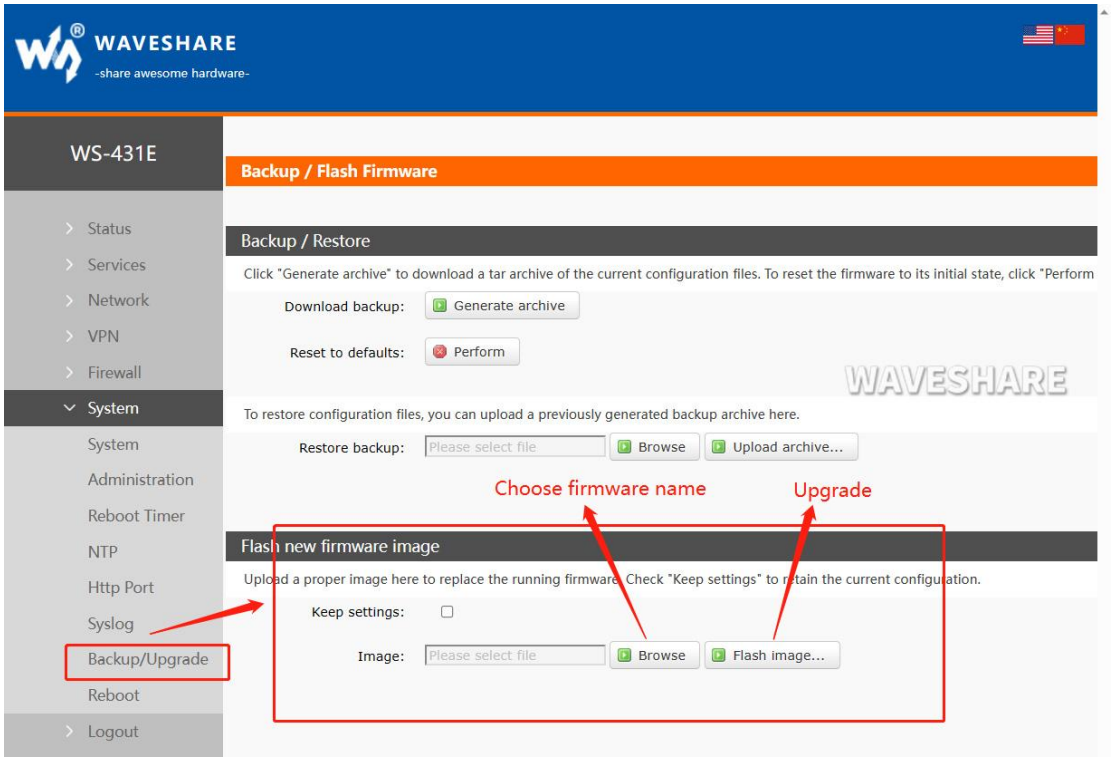



Figure 32 Upgrade firmware version

The whole upgrade process will last about 1 minute, user can enter Web Server after about 1 minute. User can choose saving settings.User should keep powering up and LAN/WIFI connection during the whole upgrade process.

### 4.5.4. RESET

Reset time is about 40~60 seconds.Reset by Web Server as follow:

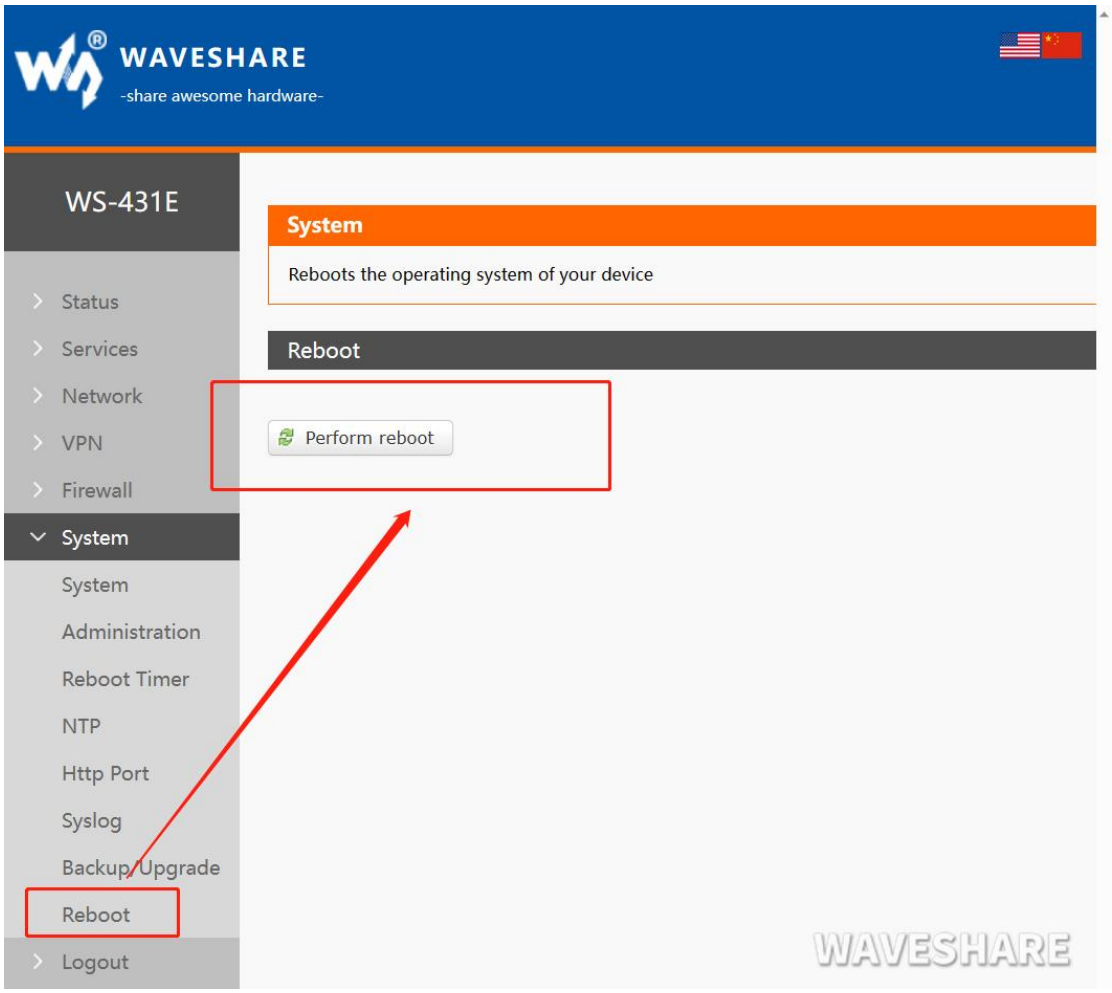



Figure 33 Reset module

## 4.6. FIREWALL FUNCTION

### 4.6.1. BASIC SETTINGS

The default value is two firewall rules.

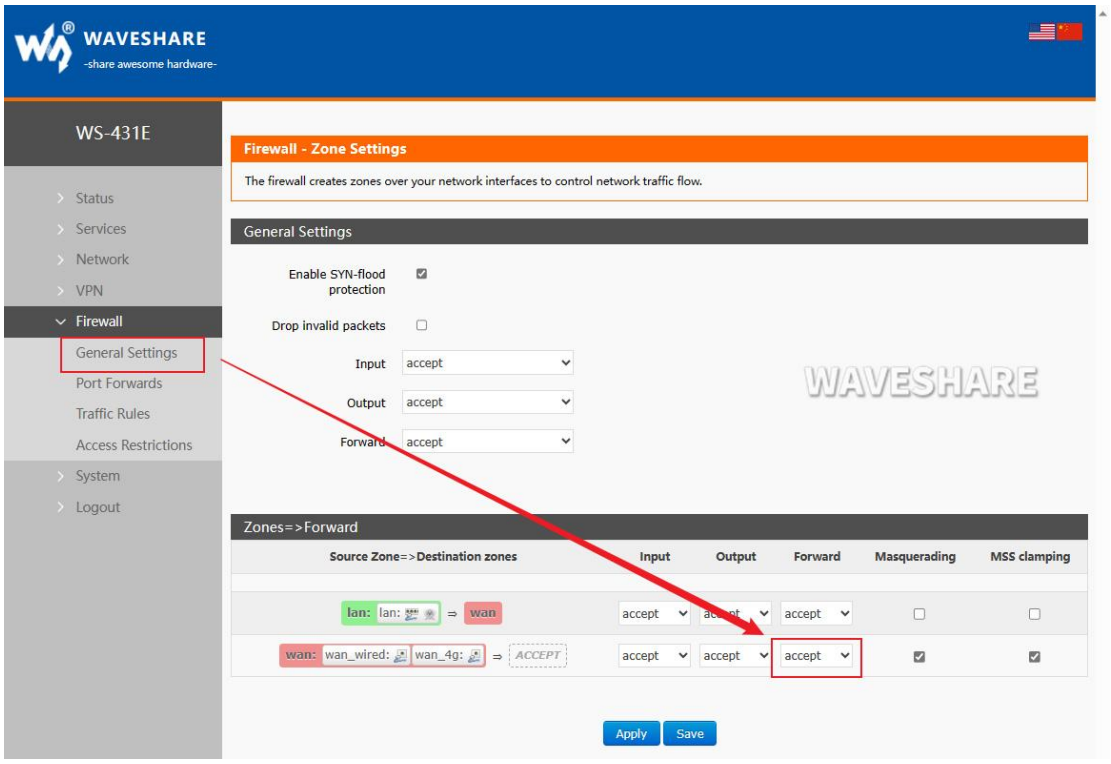



Figure 34 Firewall setting interface

<Introduction>

- Input: a packet accessing the router IP.
- Output: the packet to be sent by the router IP;
- Forwarding: data forwarding between interfaces, without going through the route itself;
- Masquerading: it is only meaningful for WAN port and 4G port, and the camouflage of IP address when accessing external network;
- MSS clamping: limits the size of message MSS, which is generally 1460.

<A, Rule 1>

- Input and forwarding from LAN port to wired WAN port are accepted;
- If there is a data packet from the LAN port and needs to access the WAN port, allowing the data packet to be forwarded from the LAN port to the WAN port is considered forwarding.
- You can also open the router's webpage on the LAN port, which is considered "input".
- The router itself connects to the external network, such as synchronizing time, which is considered "output".

<B, Rule 2>

- Wired WAN port and 4G port accept "inbound", "outbound" and "forwarding";
- If there is an "input" packet, logging in to the router's webpage from the WAN port is allowed;
- If there is an "output" packet, the router accessing the external network through WAN port or 4G port is allowed;
- If there is a "forward" packet, a packet from WAN port being forwarded to 4G port is allowed.

For example: In a certain application scenario, the LAN port needs to access the router's settings, and the router is also capable of connecting to the internet. However, devices connected to the LAN port are not allowed to access the internet. In this case, the LAN to WAN forwarding rule can be set to "deny" or "discard" (discard meaning no feedback information) to achieve this requirement.In a certain application scenario, the LAN port needs to access the router's settings, and the router is also capable of connecting to the internet. However, devices connected to the LAN port are not allowed to access the internet. In this case, the LAN to WAN forwarding rule can be set to "deny" or "discard" (discard meaning no feedback information) to achieve this requirement.

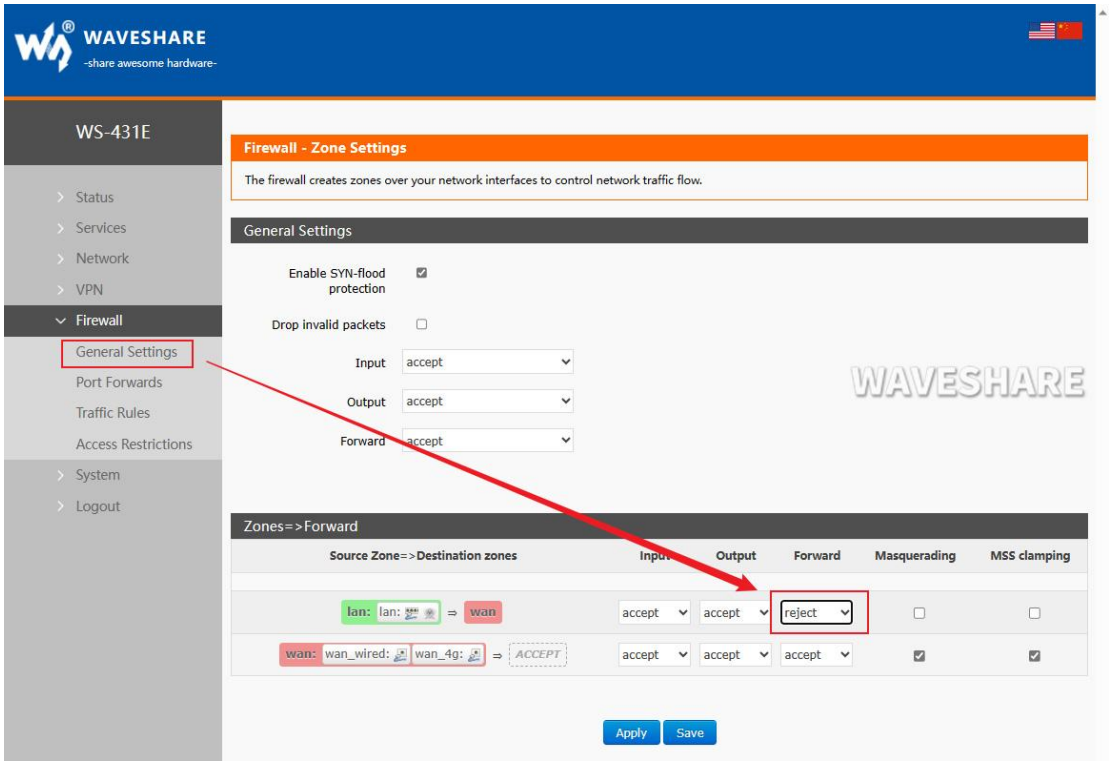



Figure 35 Firewall Settings page 2

### 4.6.2. NAT FUNCTION

1. IP address masquerading

IP address masquerading refers to the practice of modifying the source IP address of outgoing data packets to a specific interface's IP address on the router. When the "Masquerading" option is selected, the system will change the source IP address of outgoing data packets to the IP address of the WAN port on the router.

Note: IP dynamic masquerading and MSS clamping must be turned on on WAN port, and IP dynamic masquerading and MSS clamping are prohibited on LAN port.

IP address masquerading settings are located in the "Firewall-Zone Settings" interface.

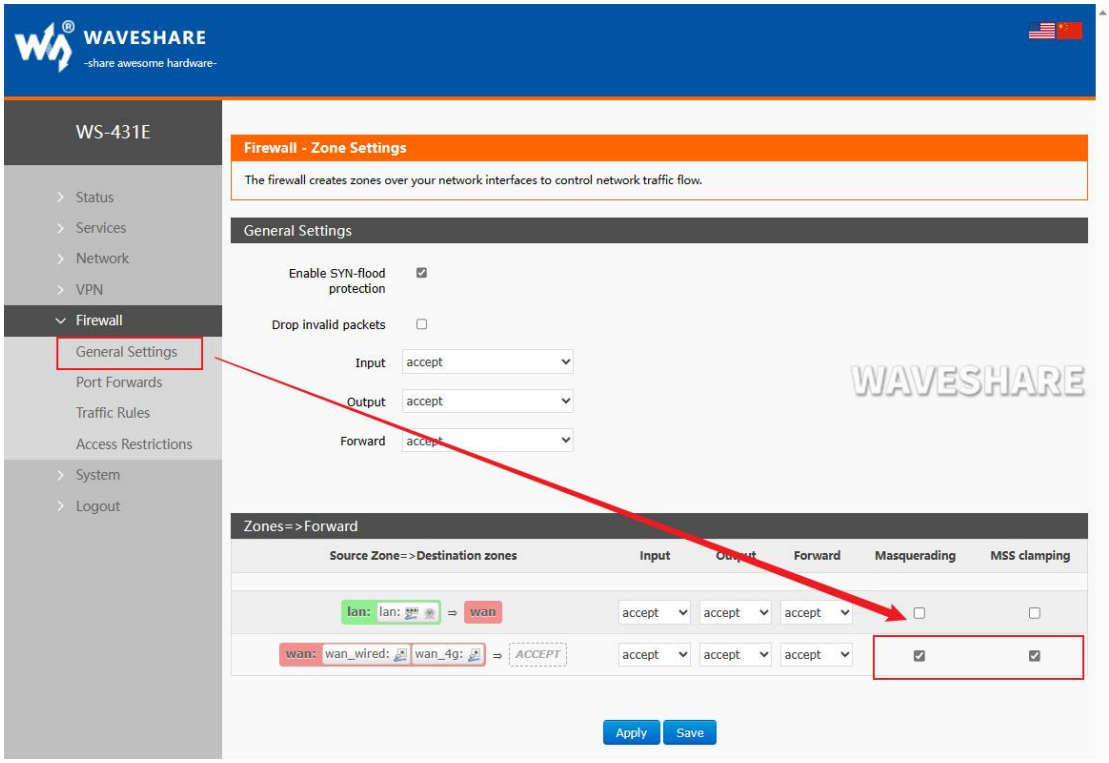



Figure 36 IP address camouflage Settings

2.SNAT

Source NAT is a special form of packet masquerading, which changes the source address of packets leaving the router and fixes the source IP address of packets leaving the router as a specific IP to send out. When using it, you should disable the IP dynamic masquerading of the WAN port.

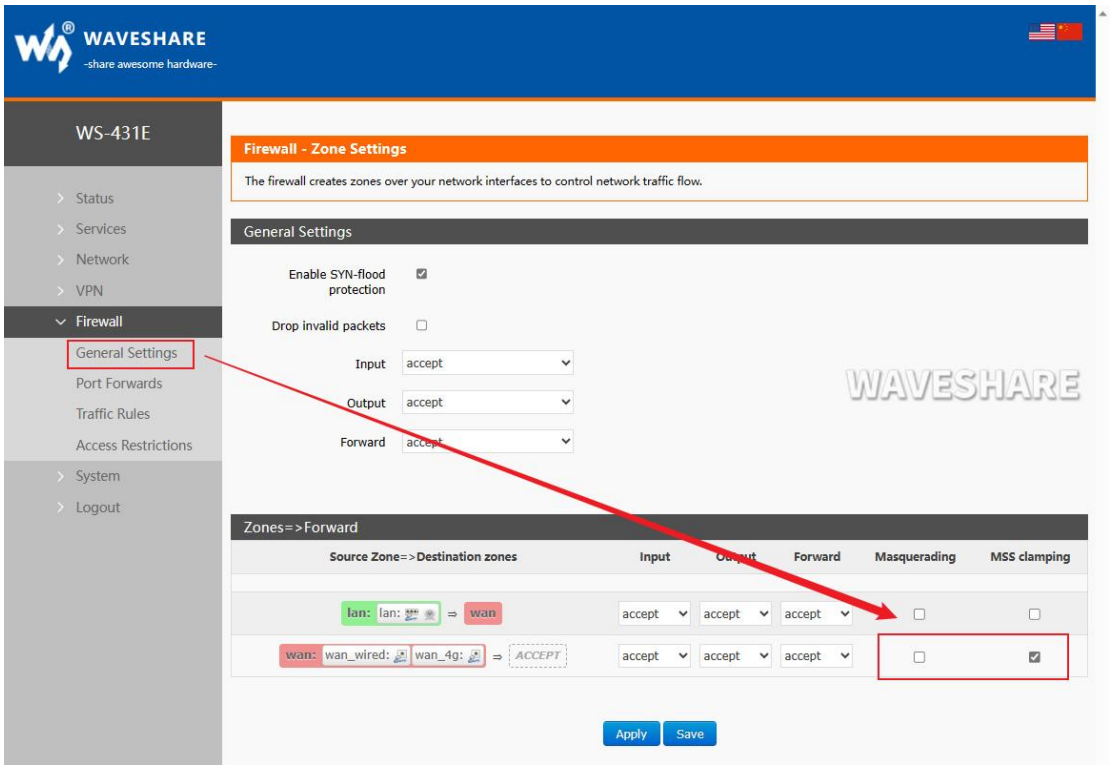



Figure 37 SNAT setting 1

Then set the Source NAT, and change the source IP address of the packet leaving the router to a fixed IP, which is located under "firewall-Traffic rules". Fix the source IP address to 192.168.9.1, and its setting interface is as follows.

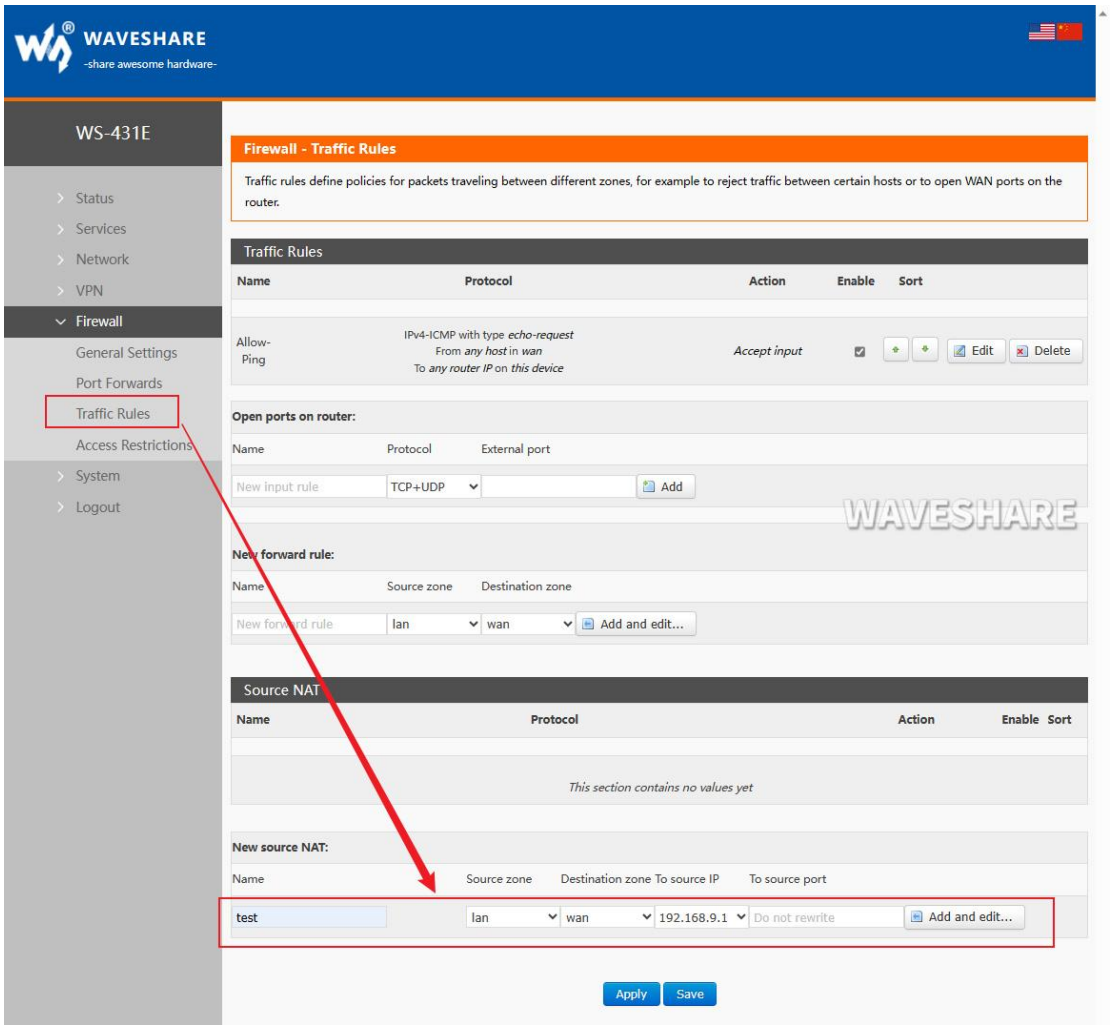



**Figure 38 SNAT setting 2**

Click “Add” and “Edit”.

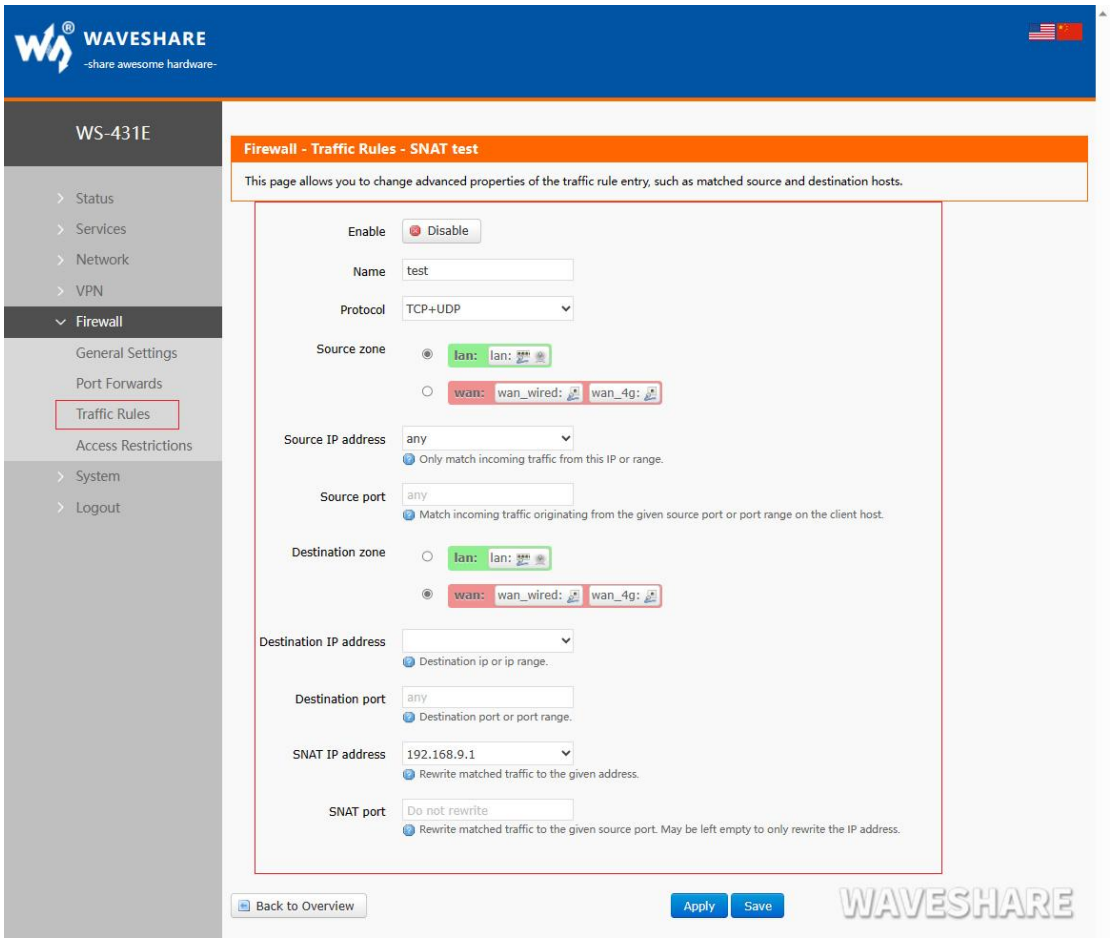



Figure 39 SNAT setting 3

If the source IP, source port and destination IP and destination port are not filled in, all IP and ports will be defaulted. Save after setting.

| Name | Description | Default parameter |
|---|---|---|
| Name | The name of this firewall rule | - |
| Protocol | Configurable: TCP+UDP/TCP/UDP/ICMP | TCP+UDP |
| Source IP address | Need to match the source IP of input traffic.<br>Empty means matching all source IPS. | empty |
| Source port | Need to match the source port of input traffic.<br>Empty means all source ports are matched. | empty |
| Desteation IP | Need to match the destination IP of input traffic.<br>Empty means that all target IPS are matched. | empty |
| Target port | Destination port that needs to match | empty |

| | | |
|---|---|---|
| | input traffic, empty means matching the destination port. | |
| SNAT IP address | Modify the source address of matching traffic to this address. | Customized IP when adding |
| SNAT port | Modify the source port of matching traffic to this port, empty means using the source port. | empty |

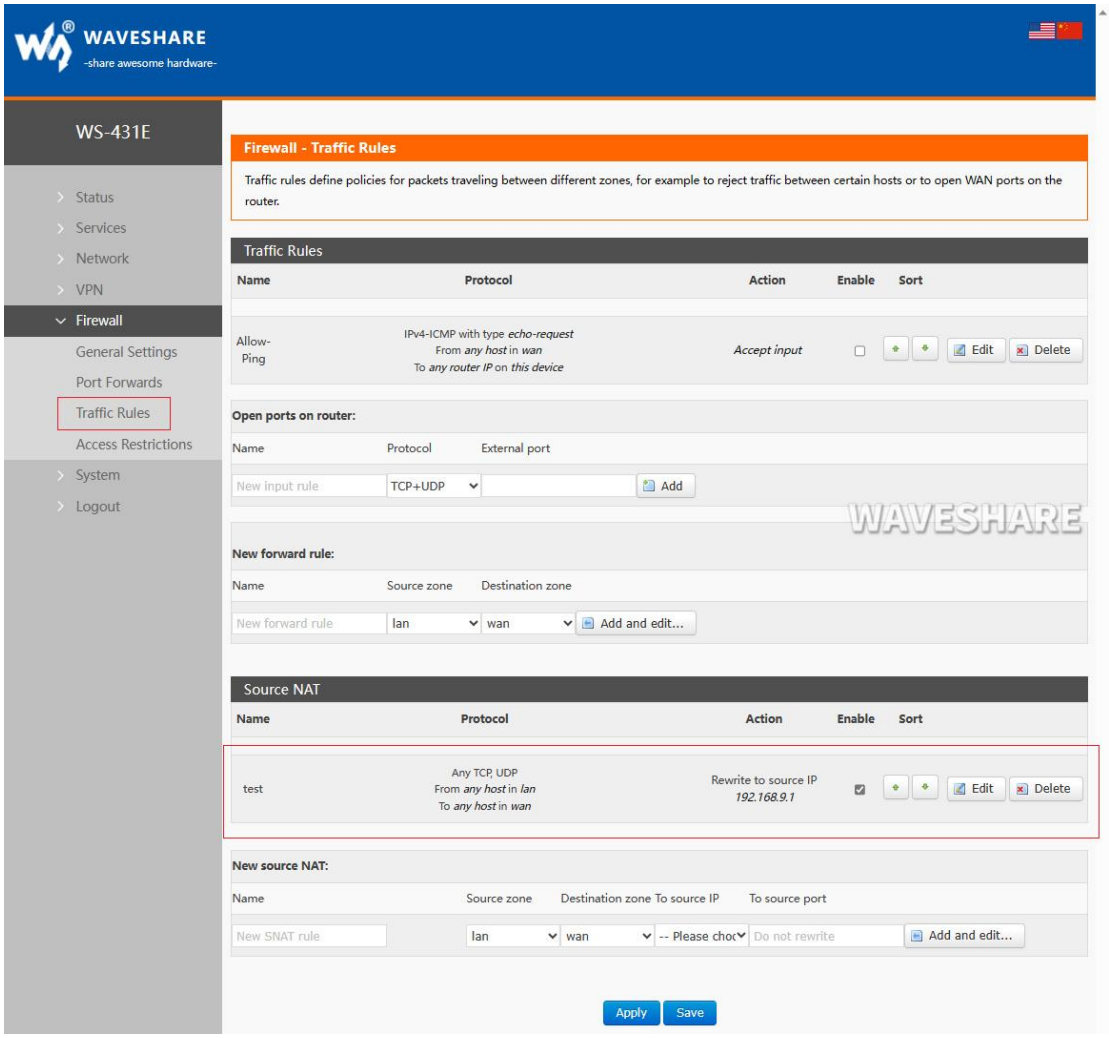



Figure 40 SNAT setting 4

3. Port forwarding

Port forwarding allows computers or services from the Internet to access computers or services within a private local area network (LAN). It involves mapping a specified port of the wide area network (WAN) address to a host within the internal network (LAN).

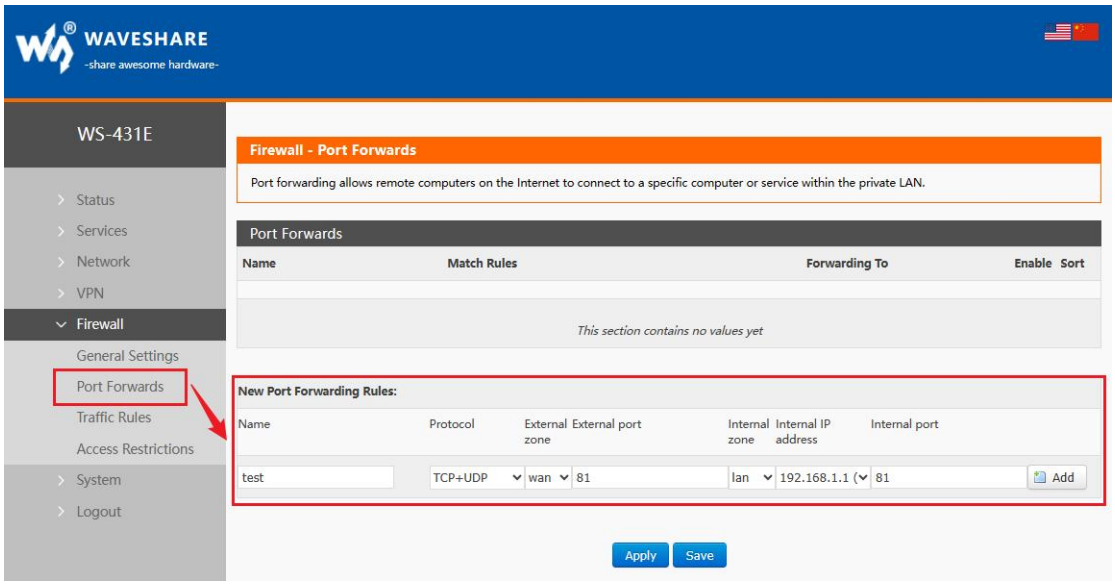



Figure 41 Port setting interface 1

After setting the forwarding rule, you need to click the "Add" button on the right, and then this rule will be displayed in the rule column.

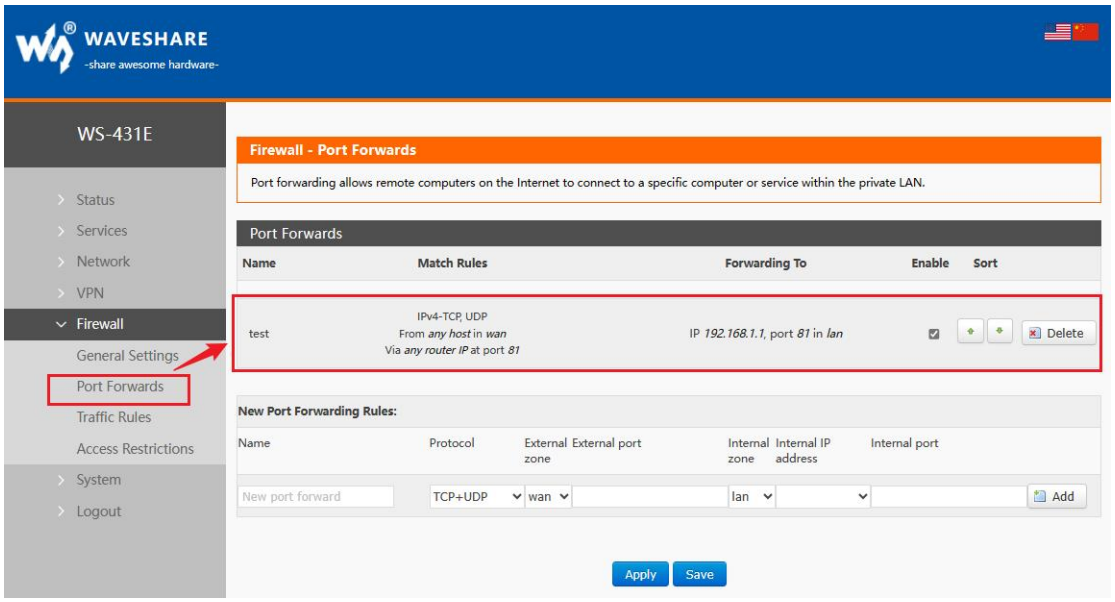



Figure 42 Port setting interface II

Then click the "Save & Apply" button in the lower right corner to make the settings take effect.

The above setting, 192.168.1.1:80 is the router's own web server. If we want to access a device within the local area network (LAN) from the Internet, we need to set up an external network to internal network mapping, also known as port forwarding. For example, we can set up the external network port as 81 and map it to the internal network IP address 192.168.1.1 with an internal network port of 80.

When we access port 81 from WAN, the access request will be transferred to 192.168.1.1:80.

< description >

You can add 20 rules to the upper limit of port forwarding rules.

| Name | Description | Default parameter |
|---|---|---|
| name | Name and character type of this port forwarding rule | empty |
| Protocol | Protocol type, which can be set as TCP+UDP/TCP/UDP. | TCP+UDP |
| External area | Include wired wan, 4G, VPN. | wan |
| External port | You can set a single port or port range, such as 8000-9000. Description: It is a DMZ function when the external port and the internal port are empty. | empty |
| Internal region | Router subnet area | lan |
| Internal IP | Router LAN area IP address | empty |
| Internal port | You can set a single port or port range, such as 8000-9000. Description: It is a DMZ function when the external port and the internal port are empty. | empty |

4. NAT DMZ

Port mapping is to map a designated port of the WAN port address to a host in the internal network. The function of DMZ is to map all ports of the WAN port address to a host, and the setting interface and port forwarding are in the same interface. When setting, the external port is left blank.

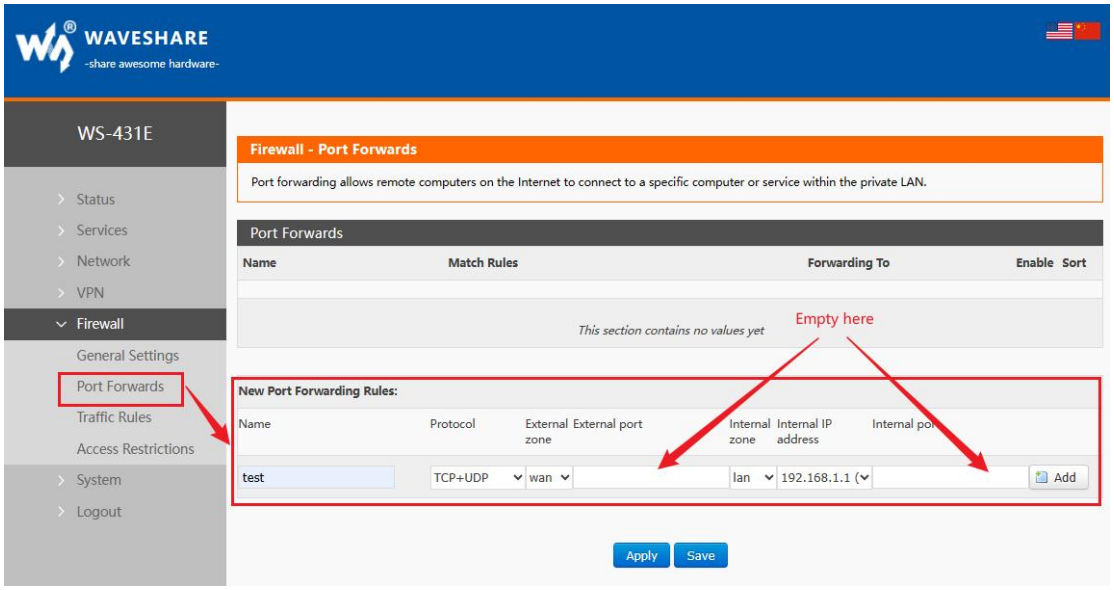



Figure 43 DMZ setting one

Click Add and save.

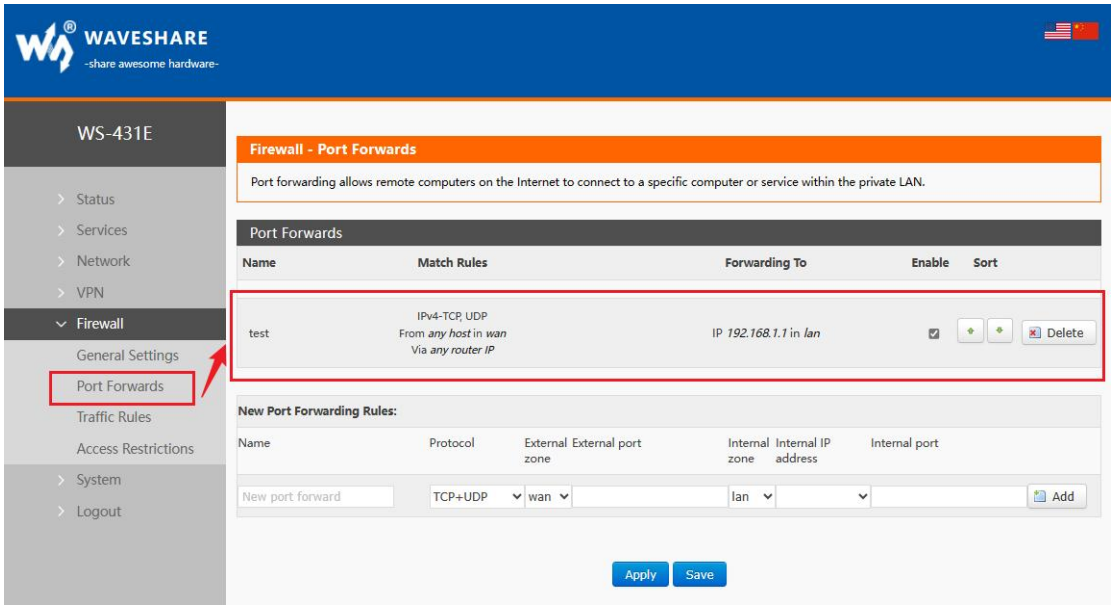



Figure 44 DMZ setting two

< Note >

Port mapping and DMZ functions cannot be used at the same time.

## 4.6.3. COMMUNICATION RULES

Communication rules can selectively filter specific Internet data types and prevent Internet access requests, and enhance network security through these communication rules. Firewall has a wide range of applications. Here are some common applications.

| Name | Description | Default parameter |
|---|---|---|
| name | Name and character type of this rule | - |
| Restricted address | Restrict IPv4 address | IPv4 address only |
| Protocol | The protocol type of the restriction rule can be selected from: TCP+UDP/TCP/UDP/ICMP | TCP+UDP |
| Matching ICMP type | Matching ICMP rules, just select any. | Any |
| Source region | Data stream source area, optional: any area, WAN, LAN.<br>LAN: indicate that rules for subnet access to external network.<br>WAN: indicates the rules for external network to access internal network. | LAN |
| Source MAC address | The source MAC that needs to match the rule can be multiple Macs. When there are multiple Macs, the Macs are separated by spaces.<br>Empty: indicates that all Macs are matched.<br>Note: When matching the source MAC address, the source IP address should be set to empty. | empty |
| Source IP address | The source IP that needs to match the rule can be an IP range.<br>Example of IP range: 192.168.1.100-192.168.1.200<br>Empty: indicates that all IPS are matched.<br>Note: When matching the source IP address, the source MAC address should be set to empty. | empty |
| Source port | The source port that needs to match the rule can be a port range.<br>Example of port range: 8000-9000<br>Empty: means to match all ports. | empty |
| Target area | Target area of data flow, optional: any area, WAN, LAN.<br>LAN: indicate that rules for subnet access to external network. | WAN |

| | | |
|---|---|---|
| | WAN: indicates the rules for external network to access internal network. | |
| Destination address | The destination IP address of the access.<br>Empty: Represents all addresses. | empty |
| Destination port | The destination port number of the access.<br>Empty: stands for all. | empty |
| action | You can choose to discard, accept, reject and do nothing when you receive such a packet.<br>Discard: packets that receive this rule will be discarded.<br>Accept: packets that receive this rule will be accepted.<br>Reject: packets receiving this rule will be rejected.<br>No action: no action will be taken when receiving this rule packet. | Accept |

1. IP Addresses Blacklist

First, enter the name of the new forwarding rule, and then click the "Add and Edit" button.

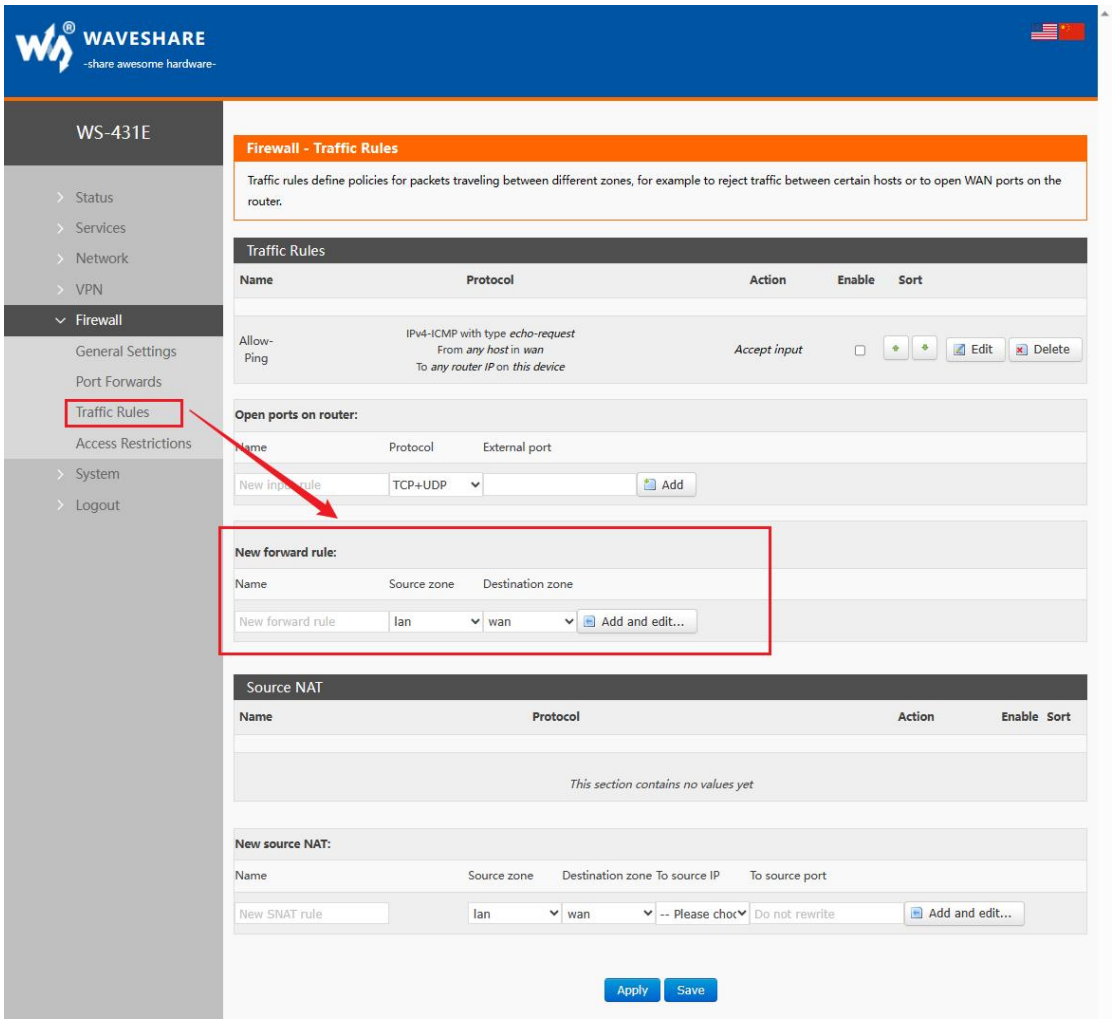



Figure 45 Firewall IP blacklist 1

In the jumped page, select “lan” as the source zone, and select “any” as the source MAC addresses and source IP address options (if only the specific IP in the local area network is restricted from accessing the specific IP of the external network, you need to fill in the IP address or MAC address here, one of which is "any" or the IP address corresponds to the MAC address, otherwise it will not take effect), as shown in the following figure.

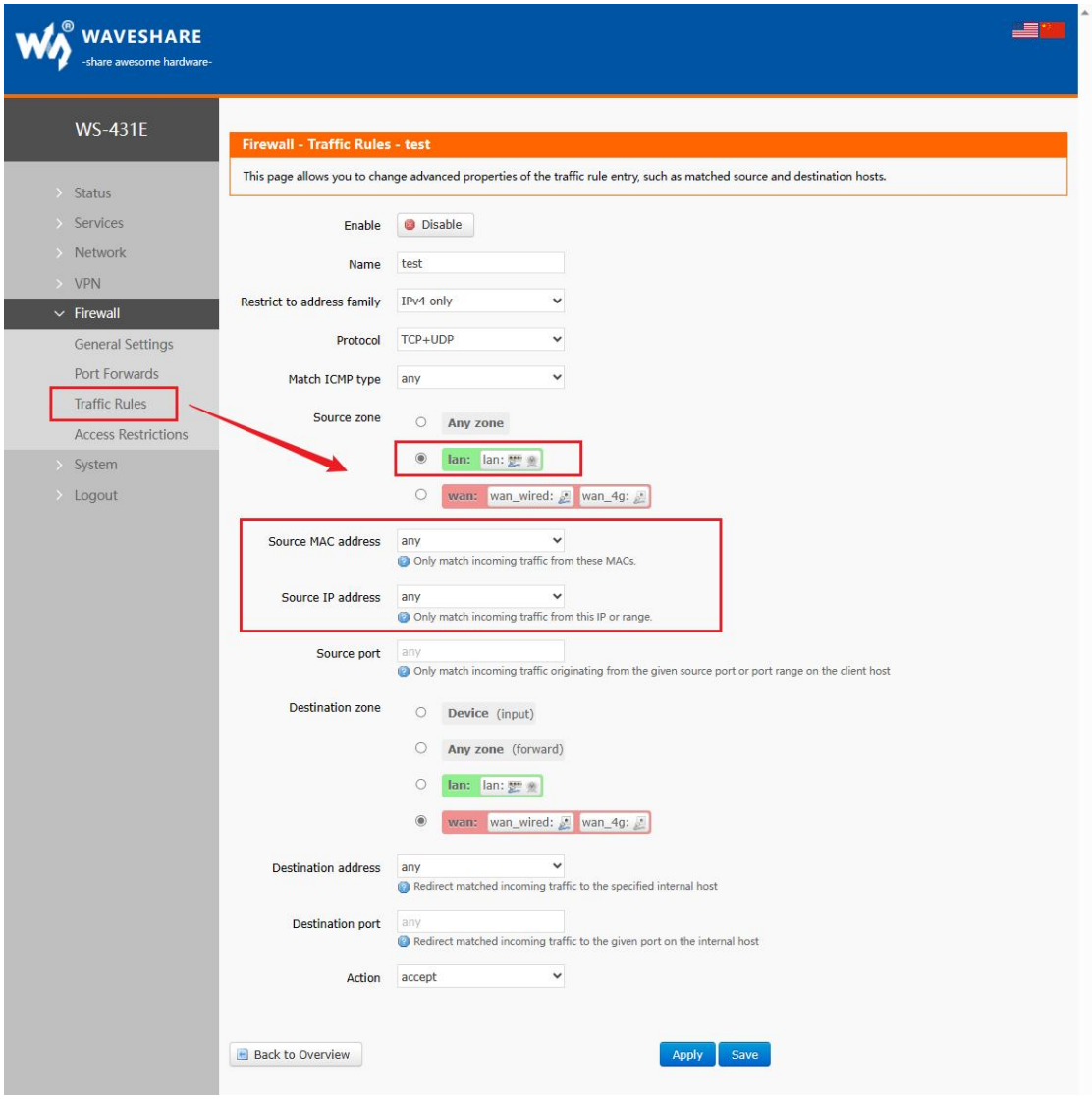



**Figure 46 Firewall IP blacklist 2**

Select WAN in the destination zone, fill in the destination address that is forbidden to access, and click "Save" and “Apply" after the setting of "Reject" is selected. As shown below.

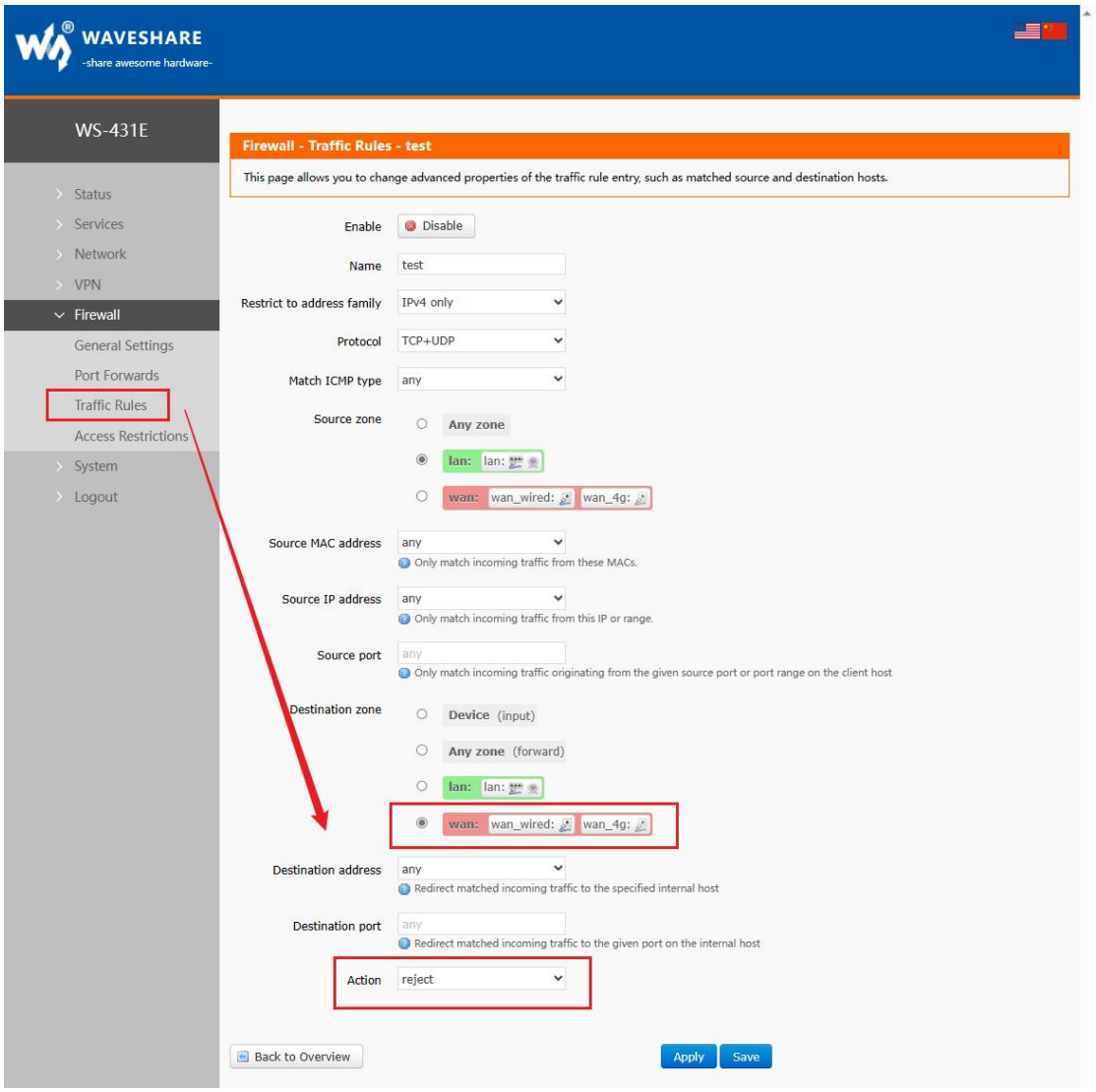



**Figure 47 Firewall IP blacklist 3**

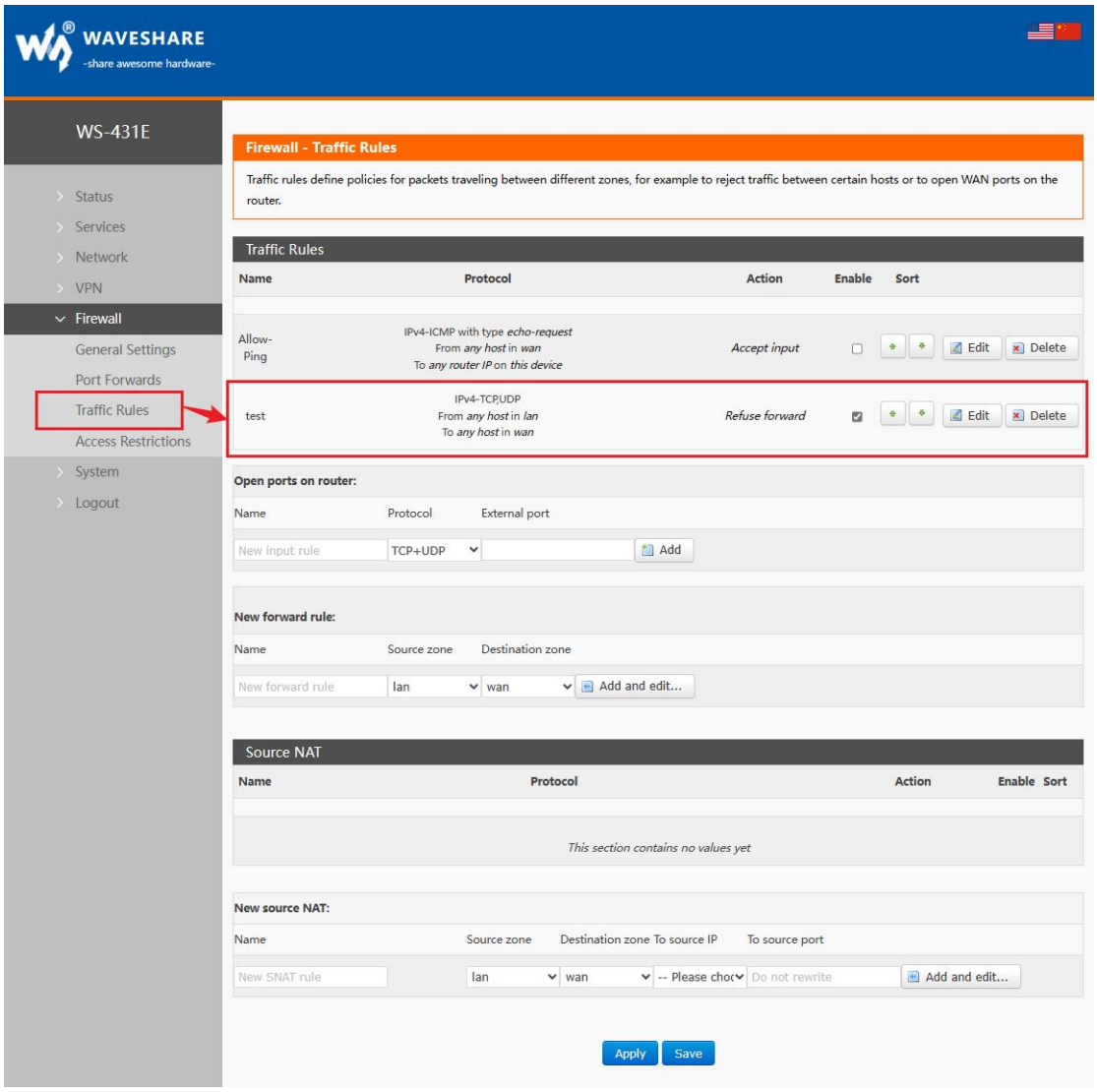



Figure 48 Firewall IP blacklist 4

Once this configuration is set up, the blacklist function will be implemented.

2. IP address Whitelist

First, add the communication rule of IP or MAC address to be whitelisted, enter the name of the rule in the new forwarding rule, and then click Add and Edit.

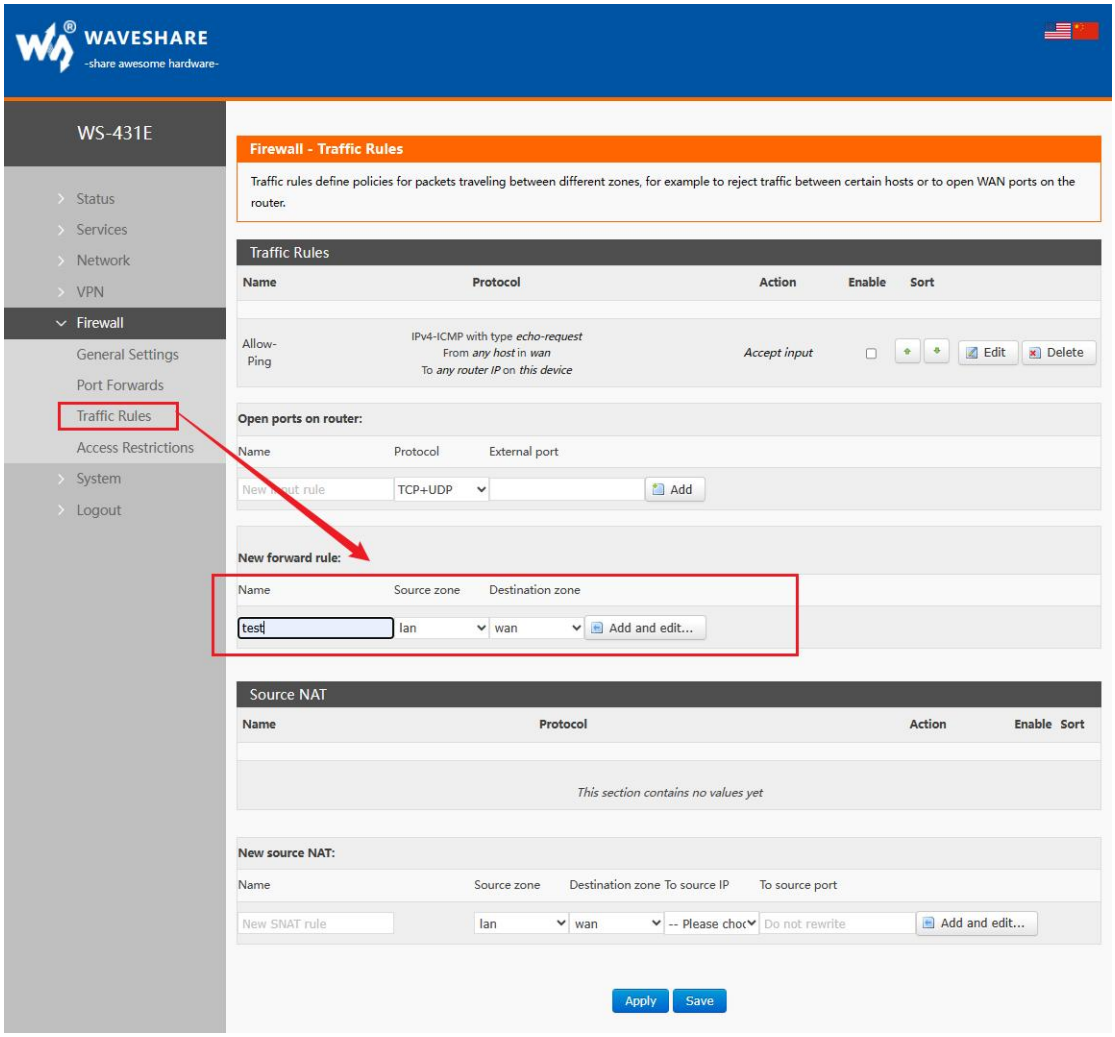



Figure 49 Firewall IP white list 1

In the jumped page, select “lan” as the source zone, and select “any” as the source MAC address and source address (if it is a specific IP that allows a specific IP in the LAN to access the external network, you need to fill in the IP address or MAC address here, one of which is "any" or the IP address corresponds to the MAC address, otherwise it will not take effect), as shown in the following figure.

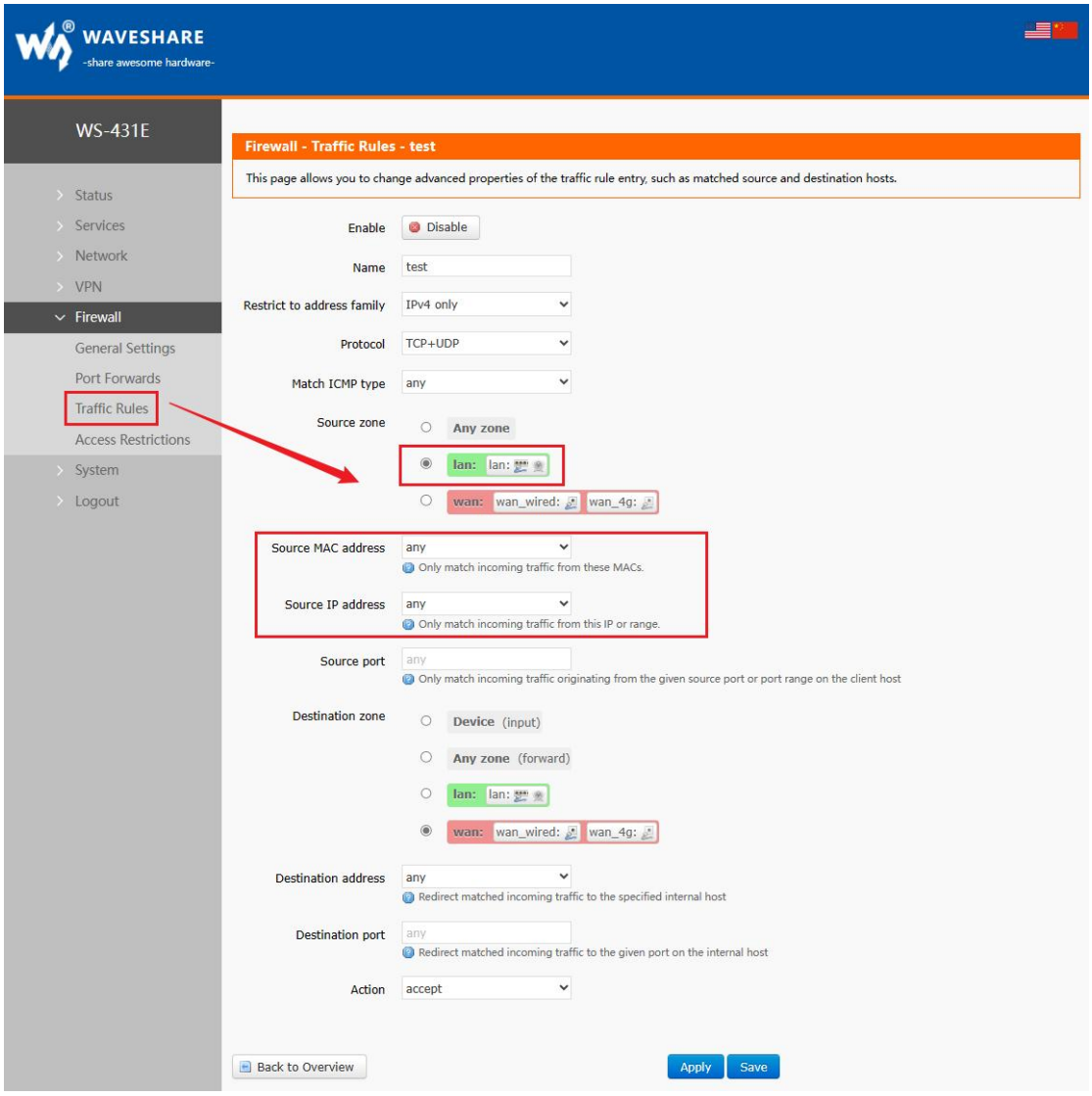



**Figure 49 Firewall IP white list 2**

Select WAN in the target zone, fill in the IP allowed to access in the target address, and click "Save" and “Apply" after the setting "Accept" is selected. As shown below.

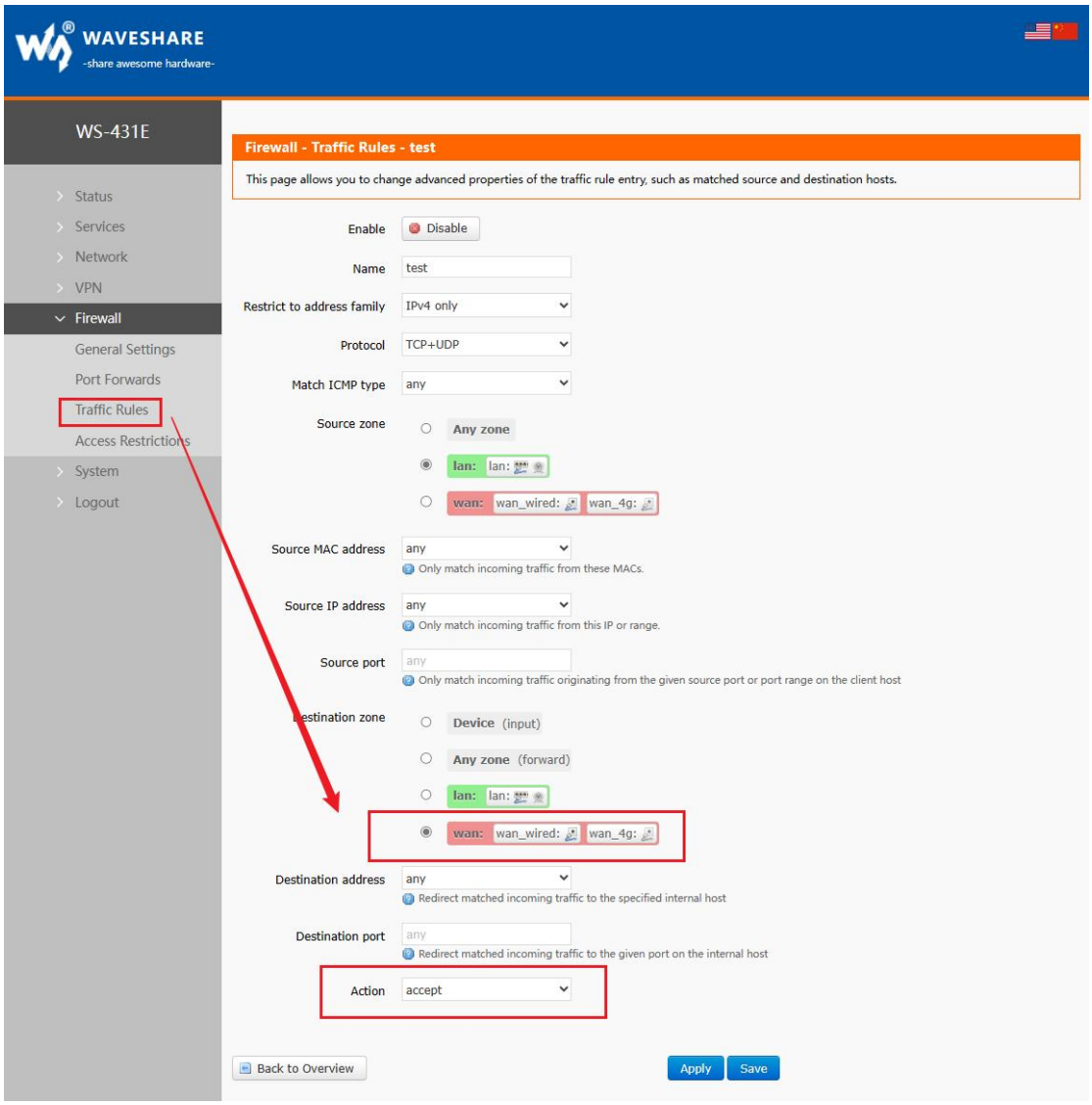



Figure 50 Firewall IP white list 3

Next, set a rule that all communications are rejected. The source address is set to “any”, the destination address is set to “any”, and the action is selected to Reject. Pay attention to the order of the two rules. The allowed rules must come first and the rejected rules must come last. After the overall setting is completed, the following figure is shown:

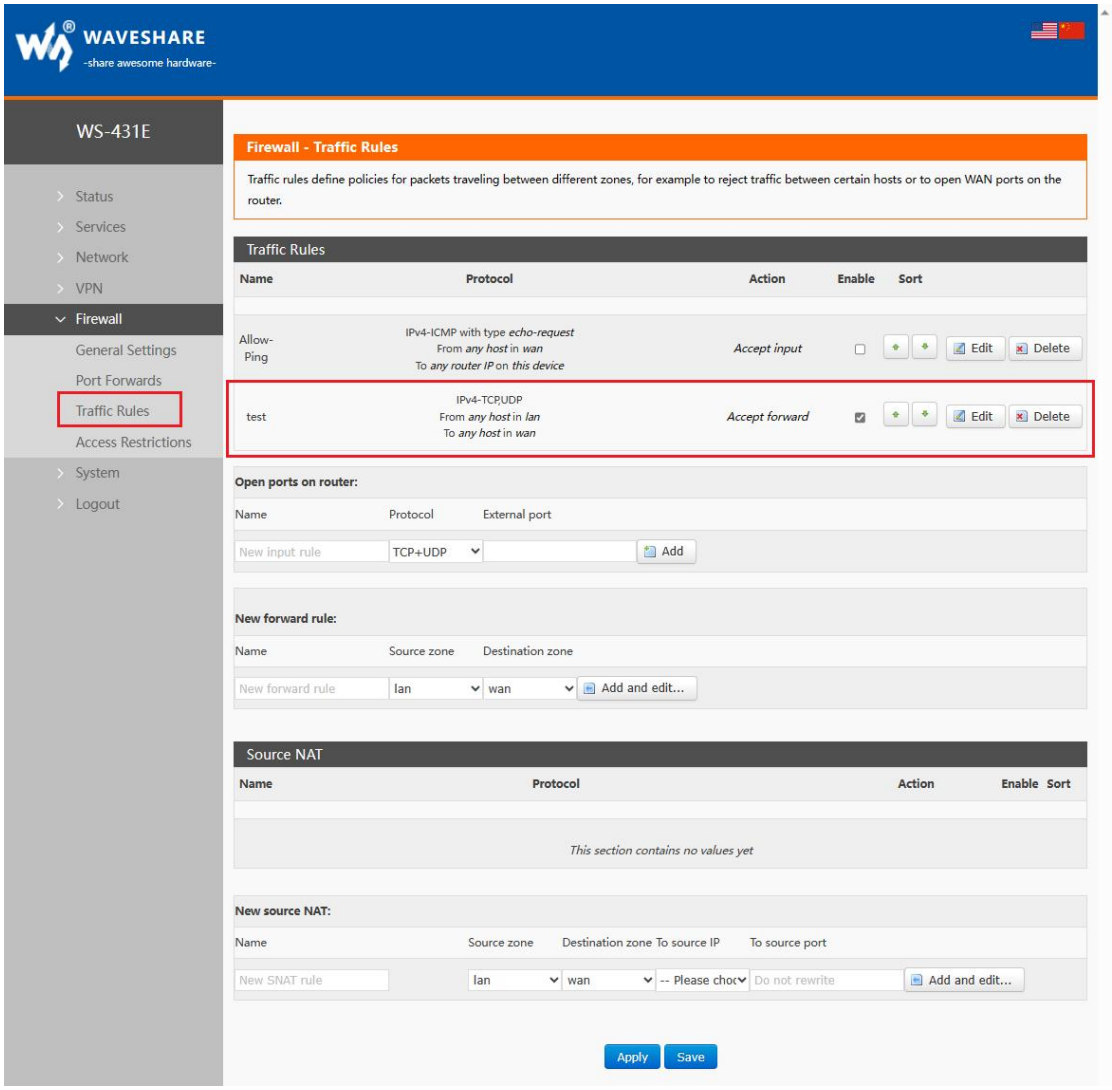



Figure 51 Firewall IP white list 4

3. Denies a subnet device access to a specified IP.

First add a forwarding rule.

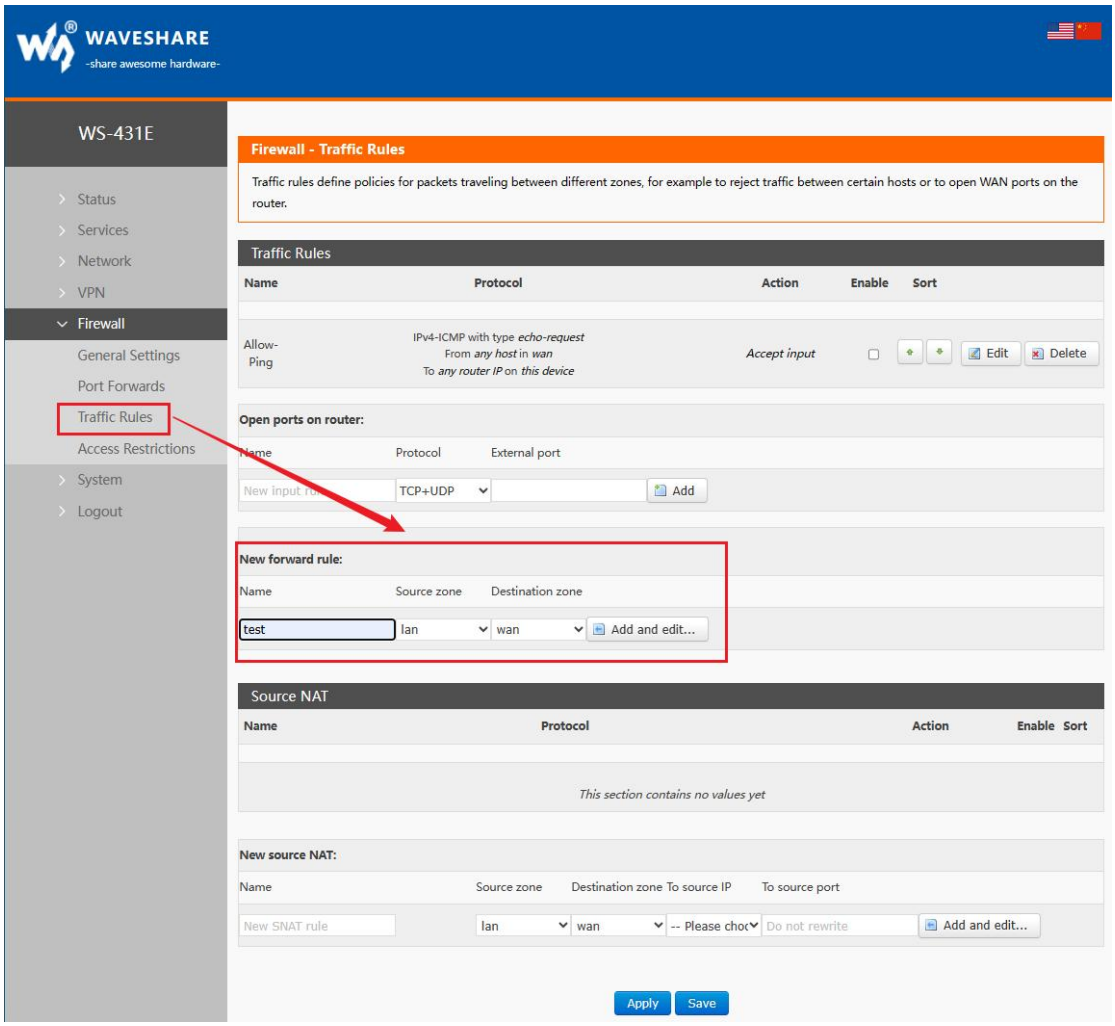



Figure 52 Firewall setting 1

- If TCP+UDP is selected as the protocol, the specified destination IP can be ping for the specified source IP, and the TCP/UDP connection cannot be established;
- If ICMP is selected as the protocol, the specified source IP cannot ping the specified target IP, and TCP/UDP connection can be established;
- If All protocols is selected, the specified destination IP cannot be ping for the specified source IP, and the TCP/UDP connection cannot be established.

< Note >

If you want to disable a port of a subnet device from accessing the specified target IP (or a port of the specified target IP), the protocol cannot choose All protocols or ICMP.

This example chooses TCP protocol.

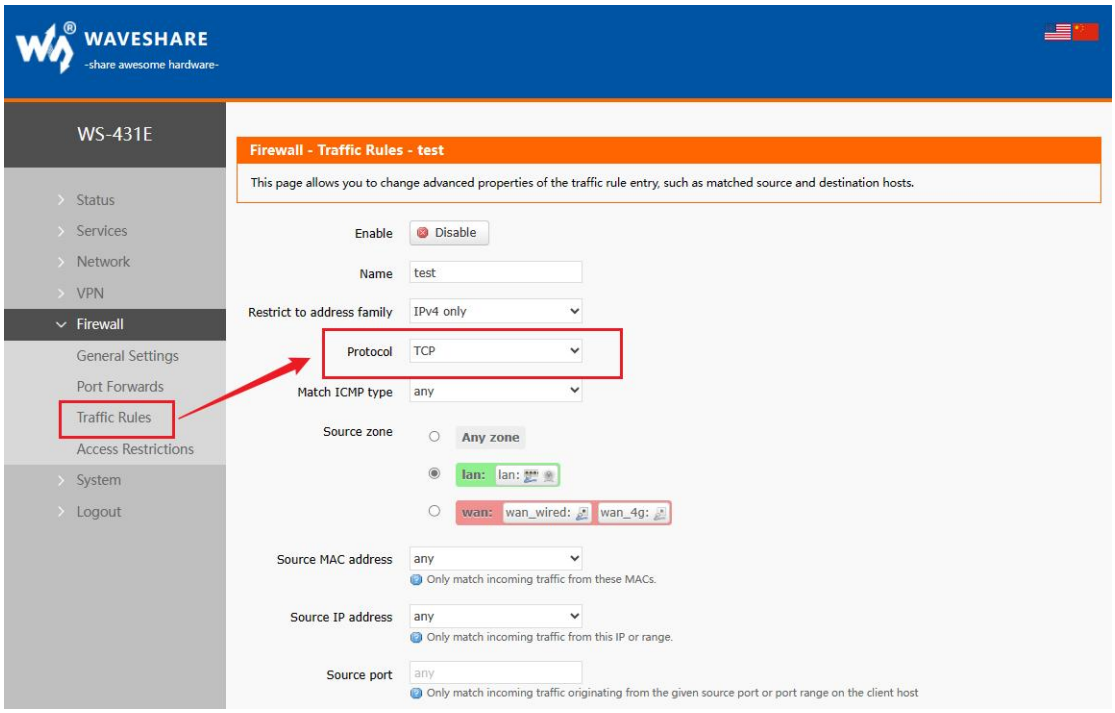



Figure 53 Firewall setting 2

Please keep the source area and destination area as the default, and select one of the source MAC and source IP. If both are filled in, please keep the MAC and IP corresponding, otherwise it will not take effect. The following example is to prohibit the 8899 port of a device with a source MAC of 48:95:07:AB:58:7B (if the port is left blank, it will be all ports by default) and to prohibit the establishment of a TCP connection with a destination address of 192.168.0.166 and a port of 9999 (if the port is left blank, it will be all ports by default). If both the source port and the destination port are left blank, it is forbidden to establish a TCP connection between a device with a source MAC of 48:95:07:AB:58:7B and a destination address of 192.168.0.166.

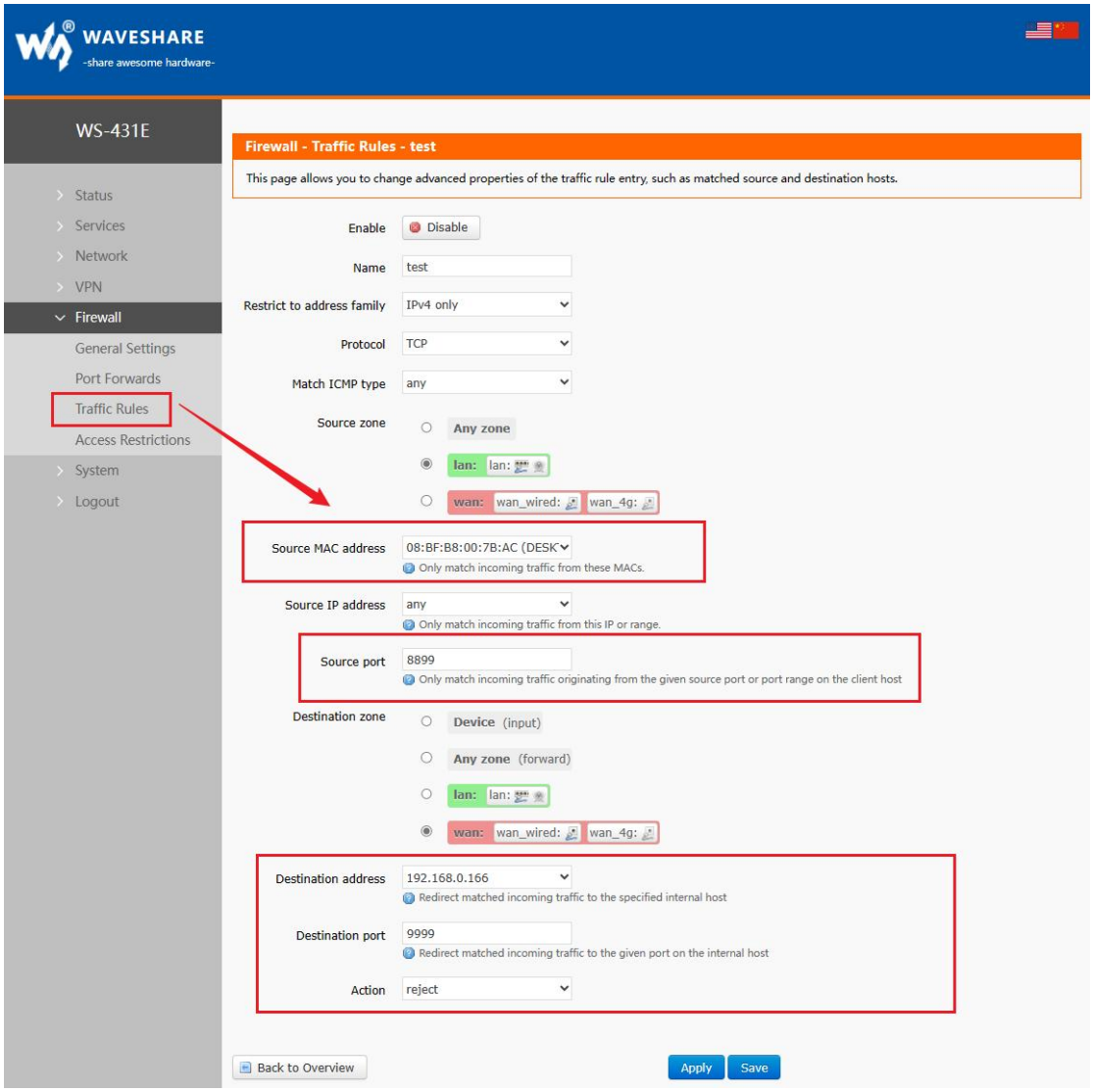



**Figure 54 Firewall setting 3**

4. Disable Ping function

First, add a forwarding rule.

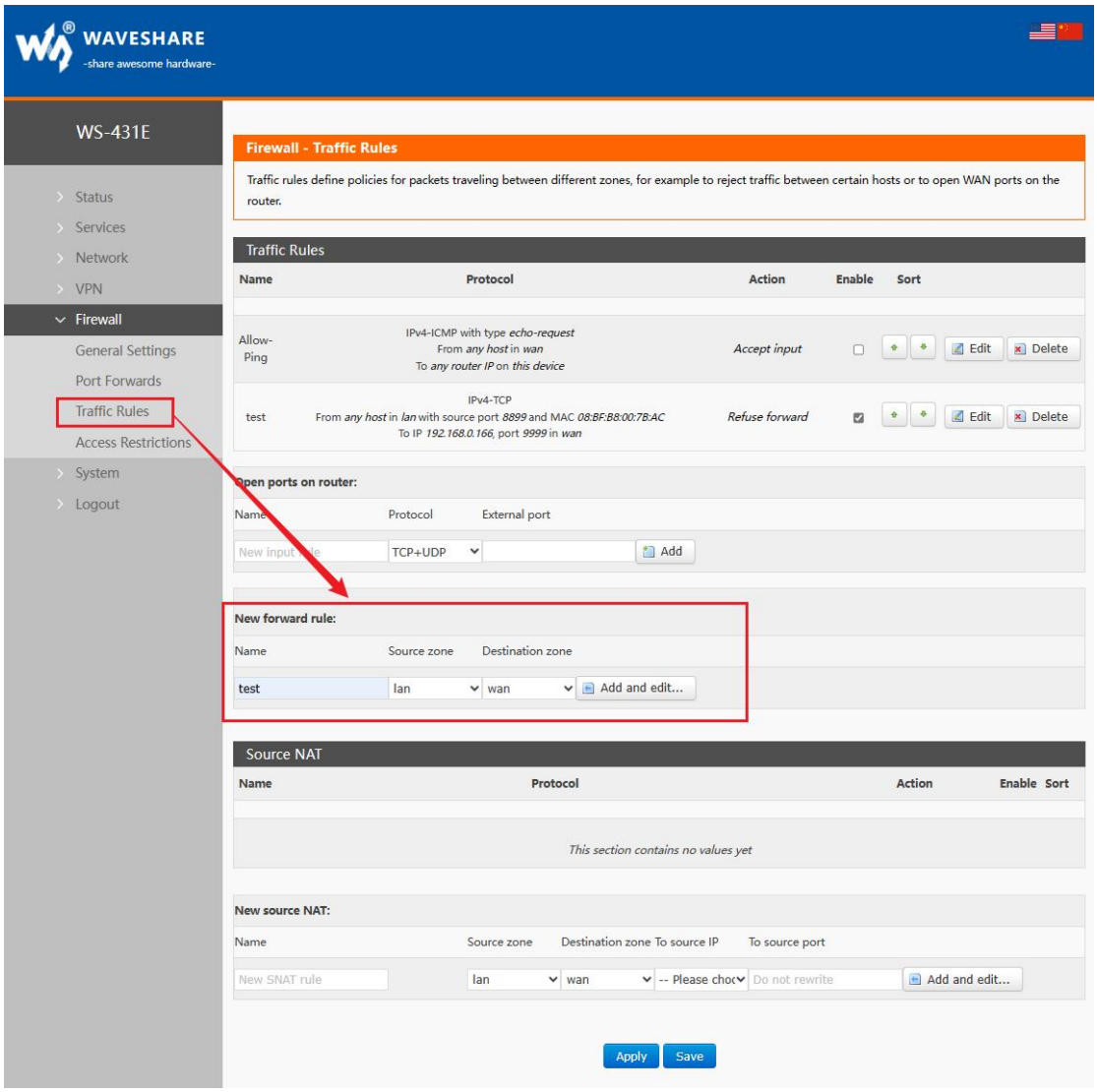



**Figure 55 Firewall setting 1**

Protocol selects ICMP

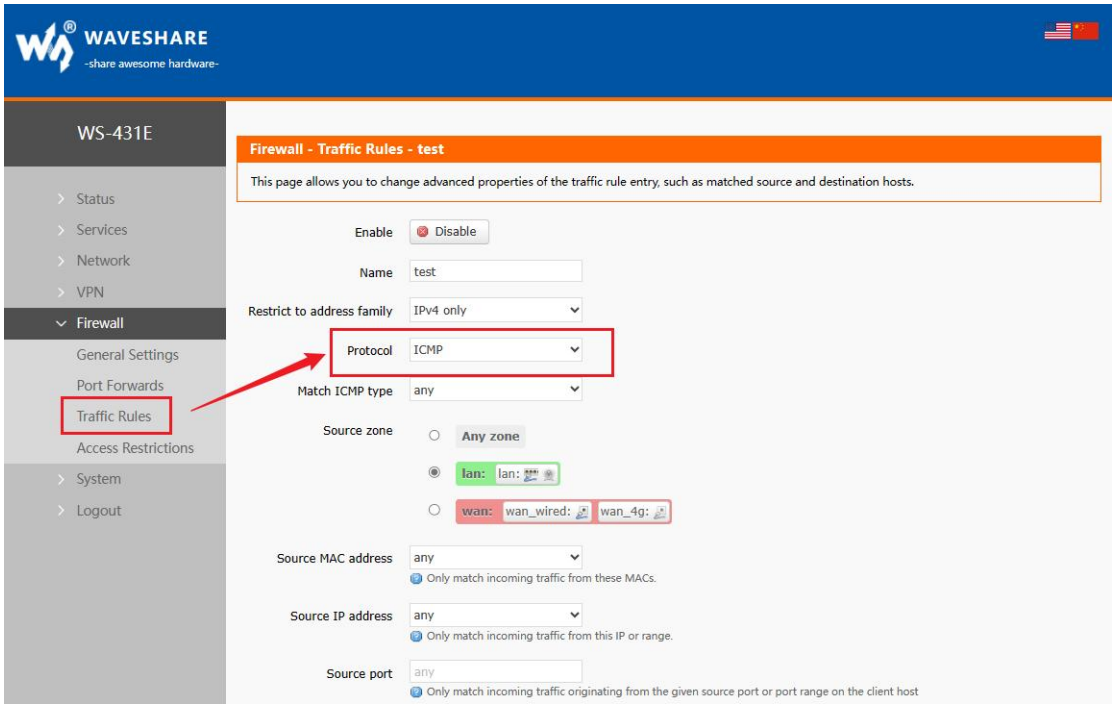



Figure 56 Firewall setting 2

The source zone and target zone can be defaulted.

Select all the source MAC and IP (according to whether all subnet devices are forbidden to ping according to the demand), and the source port number is not required to be filled in.

Select all the destination IP, and you can fill in whether ping to a certain IP is prohibited or ping detection to all IP is prohibited as required. The destination port should not be filled in.

<For example>

In this example, it is forbidden to ping devices with subnet IP of 192.168.1.133 to destination address of 192.168.0.100.

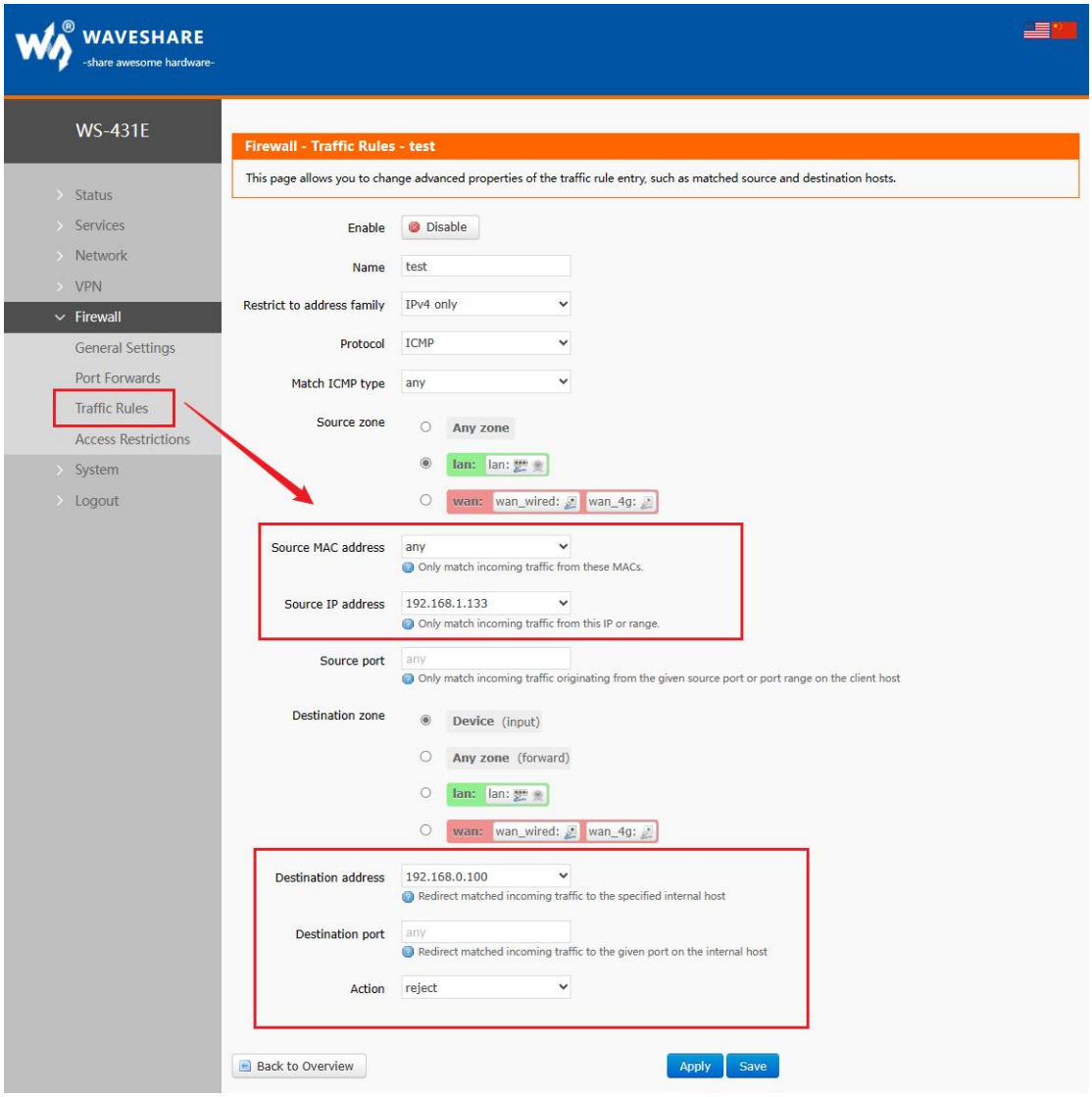



Figure 57 Firewall setting 3

Click Apply to take effect immediately after the setting is completed. To temporarily disable the "Ping" function or other firewall policy settings, uncheck the box on the right and click Apply. To enable it again, check the box and click Apply.

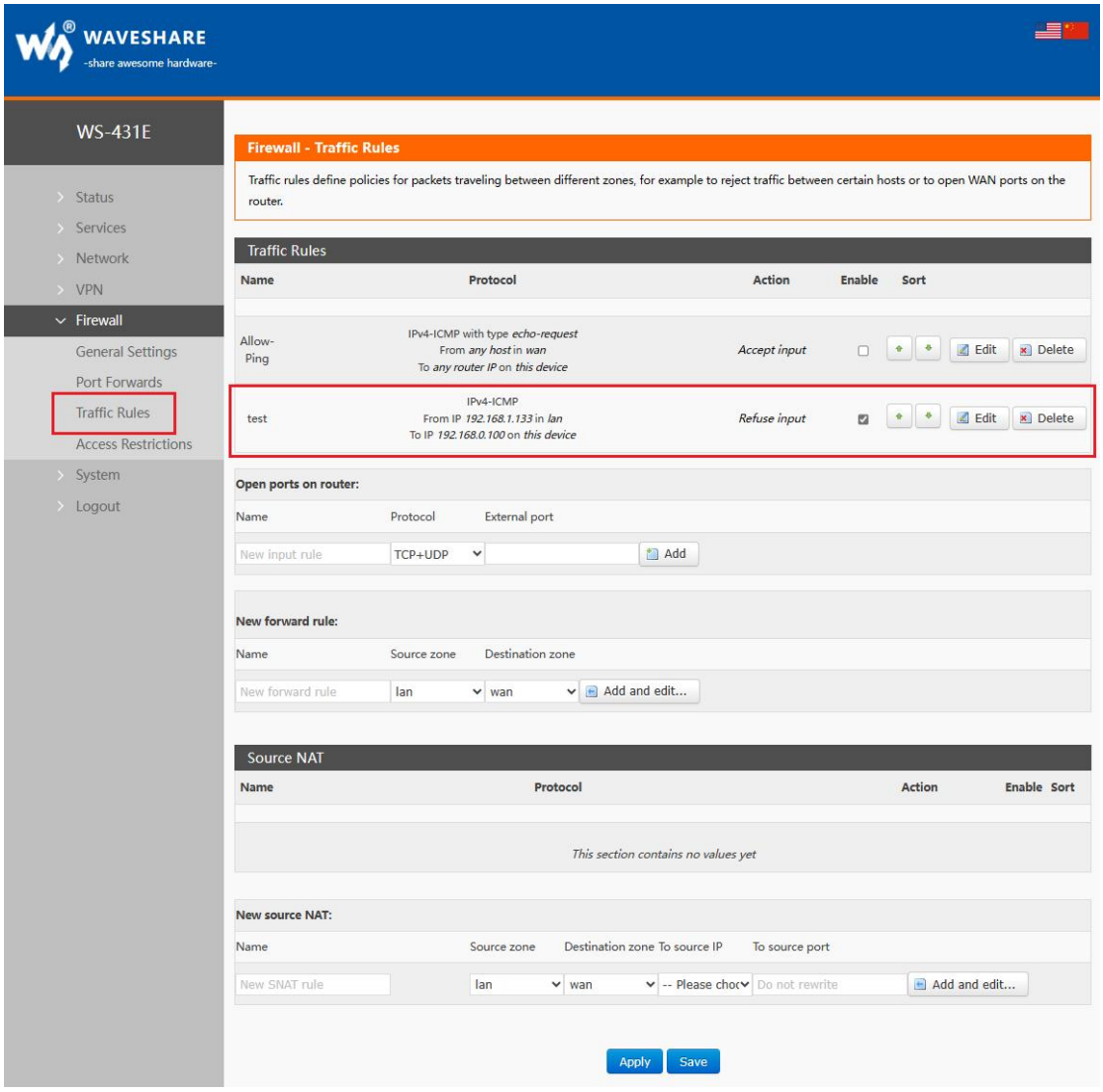



Figure 58 Firewall setting 4

No ping function takes effect.


Figure 59 Firewall setting 5

### 4.6.4. ACCESS RESTRICTION

Access restriction implements access restriction on specified domain names, and supports setting of blacklist and whitelist of domain names. When the blacklist is selected, devices connected to routers cannot access blacklisted domain names, but other domain names can be accessed normally. When whitelist is selected, devices connected to routers cannot access other domain names except those set in whitelist, and multiple blacklists and whitelists can be set. This function is turned off by default.

1. Domain name blacklist

First, select the blacklist in the mode option, click Add to enter the name and correct domain name of the rule, and then click Save. The rule will take effect immediately, and devices connected to the router will not be able to access the domain name. If blacklist is selected without adding rules, the default blacklist is empty, that is, all domain names can be accessed. As shown in the figure, except Google, other domain names can be accessed normally.

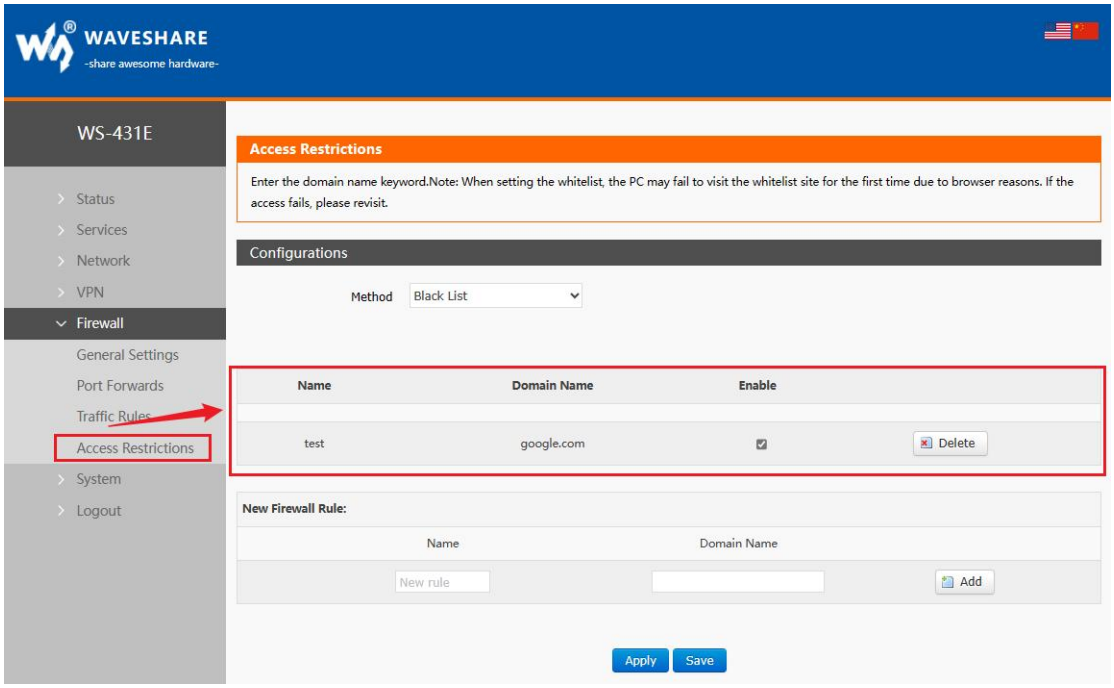



Figure 60 Domain name blacklist

2. Domain name whitelist

First, select the white list in the mode option, click Add to enter the name and correct domain name of the rule, and then click Save. The rule will take effect immediately, and the devices connected to the router will not be able to access other domain names except the domain name in the rule. If white list is selected without adding rules, the default white list is empty, that is, all domain names cannot be accessed. As shown in the figure, devices can access Google.

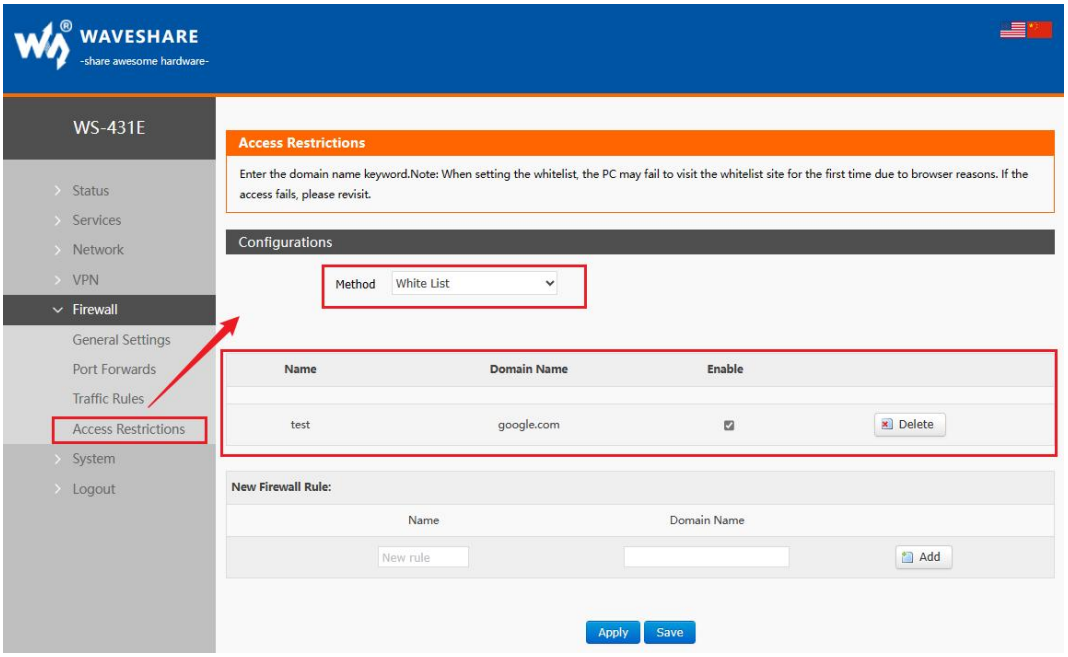



Figure 61 Domain name whitelist

## 4.7. VPN FUNCTION

VPN (Virtual Private Network) is divided into PPTP, L2TP, IPSec, OpenVPN, GRE, etc. Next, the principles of creating VPN by these protocols are introduced respectively.

PPTP: a point-to-point tunneling protocol, which uses a TCP (port 1723) connection to maintain the tunnel, uses the general routing encapsulation (GRE) technology to encapsulate the data into PPP data frames and transmit them through the tunnel, and encrypts or compresses the load data in the encapsulated PPP frames. The MPPE will encrypt the PPP frame through the encryption key generated by the MS-CHAP V2 authentication process.

L2TP: It is a Layer 2 tunneling protocol, similar to PPTP. At present, G806 supports tunnel password authentication, CHAP and other authentication methods, and the encryption method supports MPPE encryption and L2TP OVER IPSec pre-shared key encryption.

IPSec: Protocol is not a single protocol, it gives a set of architecture for application and network data security on IP layer, including network authentication protocols ESP, IKE and some algorithms for network authentication and encryption. Among them, ESP protocol is used to provide security services and IKE protocol is used for key exchange.

OpenVPN: Support certificate-based two-way authentication, that is, the client needs to authenticate the server, and the server needs to authenticate the client.

GRE: GRE (General Routing Encapsulation) protocol encapsulates data packets of some network layer protocols (such as IP and IPX) so that these encapsulated data packets can be

transmitted in another network layer protocol (such as IP). GRE adopts the technology of Tunnel, which is the third layer tunnel protocol of VPN.

Note: These protocols can build VPN, and you can choose a more suitable protocol according to your own needs.

### 4.7.1. PPTP CLIENT

Before application, you need to get the address, account, password and encryption method of VPN server, then enable PPTP client, and write other parameters in turn.

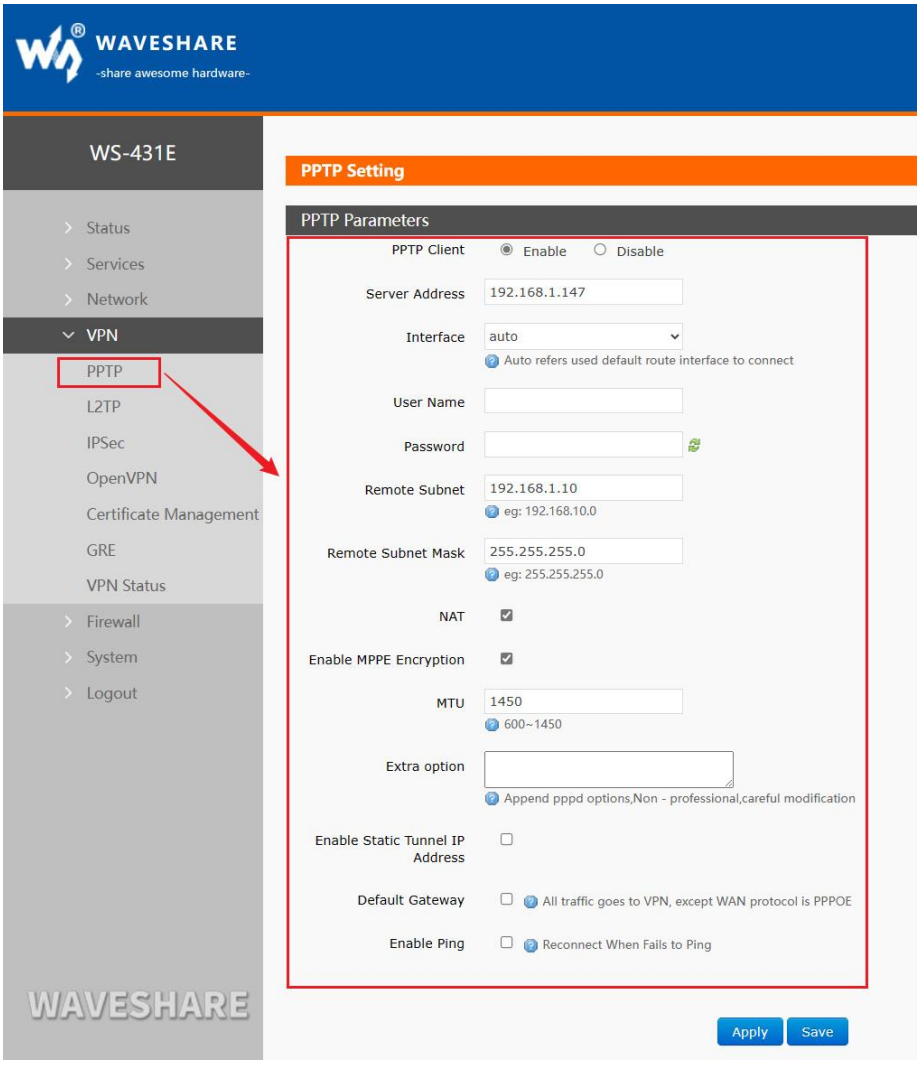



Figure 62 Router adds VPN operation 1

< Description >

- Server address: fill in the IP or domain name of the VPN server to be connected;

- Interface: wan_4G, wan_wired and automatic can be selected according to different networking modes;
- User name/password: obtained from VPN server;
- Encryption method: MPPE encryption, no encryption, obtained from VPN server, and checked or unchecked according to the actual situation;
- MTU: set the MTU value of the channel, which is 1450 by default. This setting should correspond to the VPN server;
- NAT: This function is turned on by default. When the content needs to communicate with the outside, replace the internal address with the public address. If this item is disabled, the network address translation function cannot be realized;
- Peer subnet & mask: after filling in correctly, the subnet interworking function under VPN can be directly realized when NAT function is turned on;
- Enable static tunnel IP address: it is not enabled by default, and the server automatically allocates IP. You can fill in the static tunnel IP here;
- Extra opption: append the PPPD parameters, magic words, etc. No operation is required by default;
- Enable ping: a real-time VPN online detection and reconnection mechanism. Ping custom IP to ensure stable connection. Disabled by default.

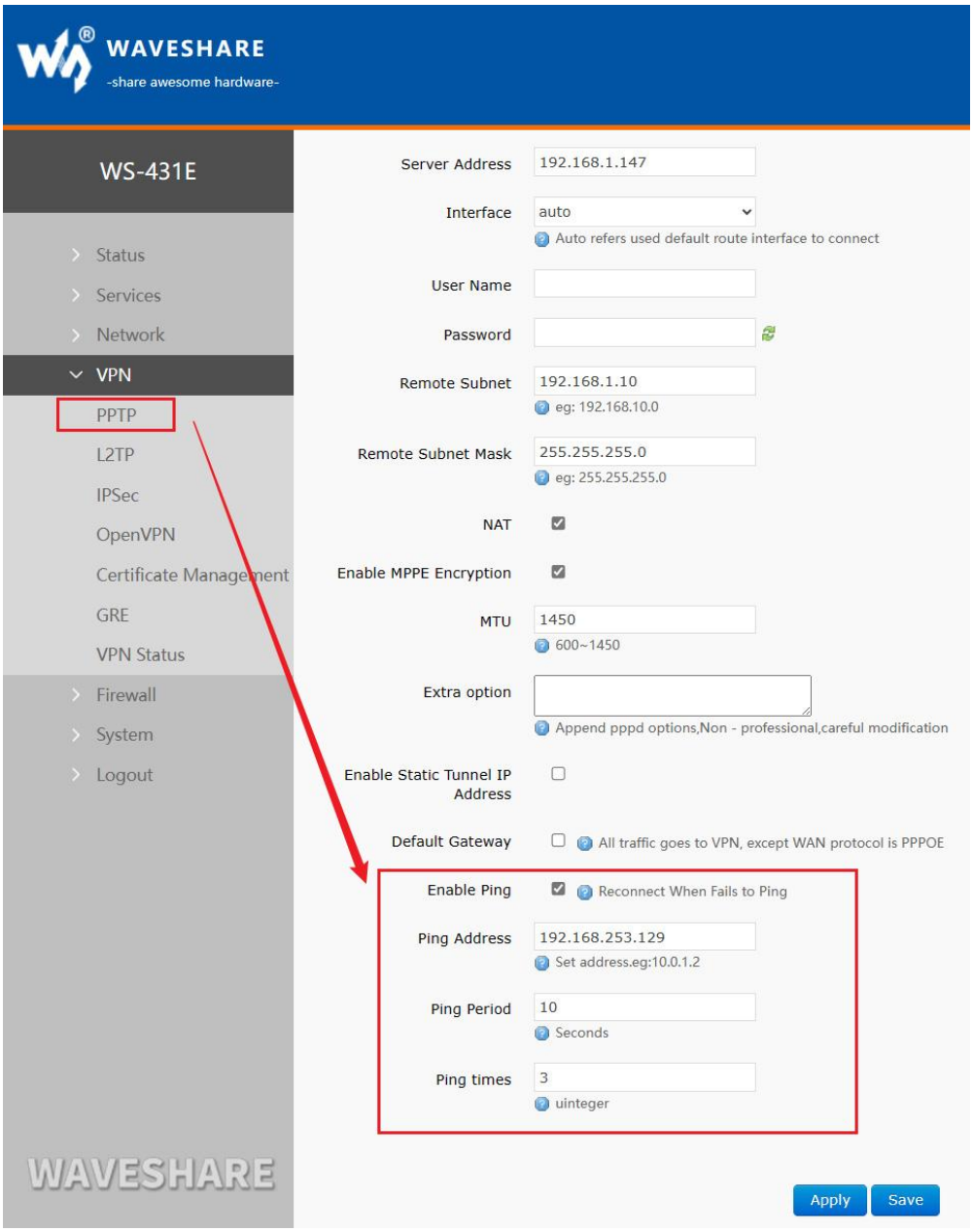



Figure 63 Router enables VPN state detection

## 4.7.2. L2TP CLIENT

L2TP is a Layer 2 tunneling protocol, similar to PPTP. At present, WS-431E supports tunnel password authentication, MPPE encryption and L2TP OVER IPSec pre-shared key encryption. Enter the VPN--L2TP interface, select Enable L2TP client, and fill in the parameters in turn.

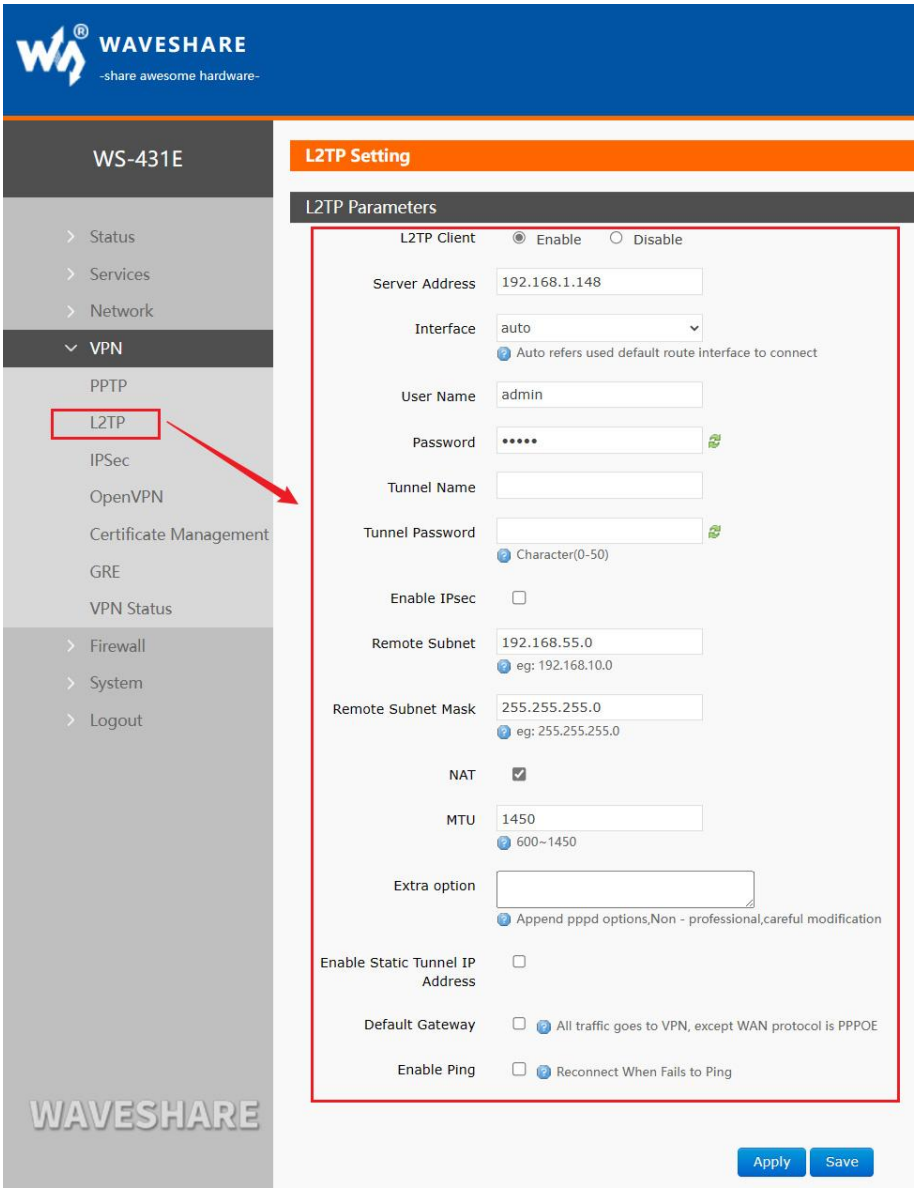



Figure 64 L2TP Client Enable Settings Interface

< Description >

- L2TP supports tunnel password authentication, MPPE encryption and L2TP OVER IPSec encryption;
- Server address: fill in the IP or domain name of the VPN server to be connected;
- Interface: wan_4G, wan_wired and automatic can be selected according to different networking modes;
- User name/password: obtained from VPN server;
- Encryption/authentication: tunnel password authentication, MPPE encryption and IPSec encryption, which are obtained from VPN server and filled in correctly;

- Enable static tunnel IP Address: it is not enabled by default, and the server automatically allocates IP. You can fill in the static tunnel IP here;
- Extra option: append the PPPD option, magic words, etc. No operation is required by default;
- NAT: This function is enabled by default. When the content needs to communicate with the outside, replace the internal address with the public address. If this item is disabled, the network address translation function cannot be realized;
- Peer subnet & mask: after filling in correctly, the subnet interworking function under VPN can be directly realized when NAT function is turned on;
- Enable ping: Real-time VPN online detection and reconnection mechanism. Not enabled by default. Checking this option indicates that the VPN will be reconnected if the ping fails.
- L2TP connection succeeded: after filling in the relevant parameters, save & apply, and enter VPN--VPN status to check the connection status.

### 4.7.3. IPSEC

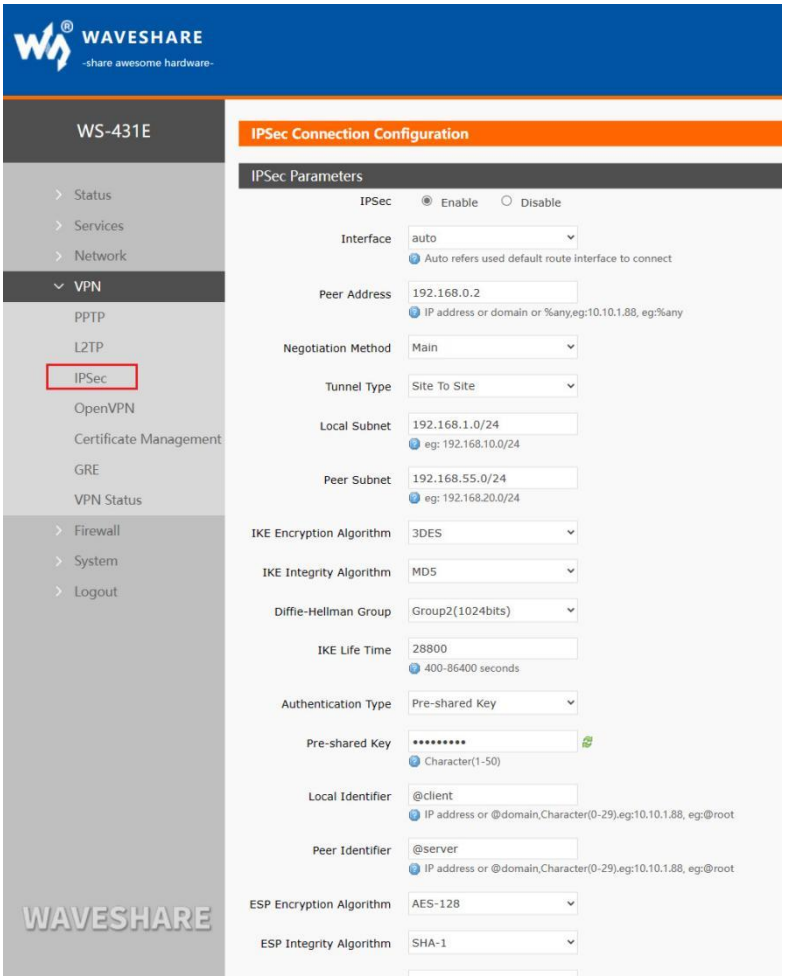



**Figure 65 Basic settings after enabling IPSec**

< Description >

- Interface: wan_4G, wan_wired and automatic can be selected according to different networking modes;
- Peer address: it can be divided into VPN client and VPN server. Please fill in the IP/ domain name of the peer;
- Negotiation mode: main mode, aggressive mode (aggressive negotiation mode), with main mode as the default;
- Tunnel types: subnet to subnet, subnet to host, host to subnet, host to host. Select one according to the actual application mode;
- Local subnet: IPSec local subnet and subnet mask;
- Local identifier: the local identifier of the channel, which can be IP or FQDN. Pay attention to adding @ when defining the domain name; IKE Encryption Algorithm: The first stage

includes encryption mode, integrity scheme and DH exchange algorithm in IKE stage; IKE life time: set the life cycle of IKE, in seconds, the default is 28800;

- Authentication type: currently, the authentication mode of pre-shared key is supported;
- ESP encryption algorithm: the second stage includes the encryption mode and integrity scheme;
- ESP life time: set the ESP life cycle in seconds, and the default value is 3600;
- Perfect Forward Secrecy (PFS) for Session Key Encryption: There are four options: disabled, DH1, DH2 and DH5. This setting should be consistent between this end and the peer.
- Enable DPD Detection: What action should be taken when the DPD declares the peer as dead.
- DPD detection period: Set the time interval of connection detection (DPD);
- DPD timeout: Set the connection detection (DPD) timeout;
- DPD operation: Set the operation of connection detection. Including restart, dismantle, keep, none, restart by default;
- IPSec Connection Successful: After successfully establishing an IPSec connection with the remote endpoint, navigate to the VPN-to-VPN Status section to check the connection status.

### 4.7.4. OPENVPN

Enable OpenVPN to build VPN, and you can choose TUN (routing mode) or TAP (bridge mode) internally:

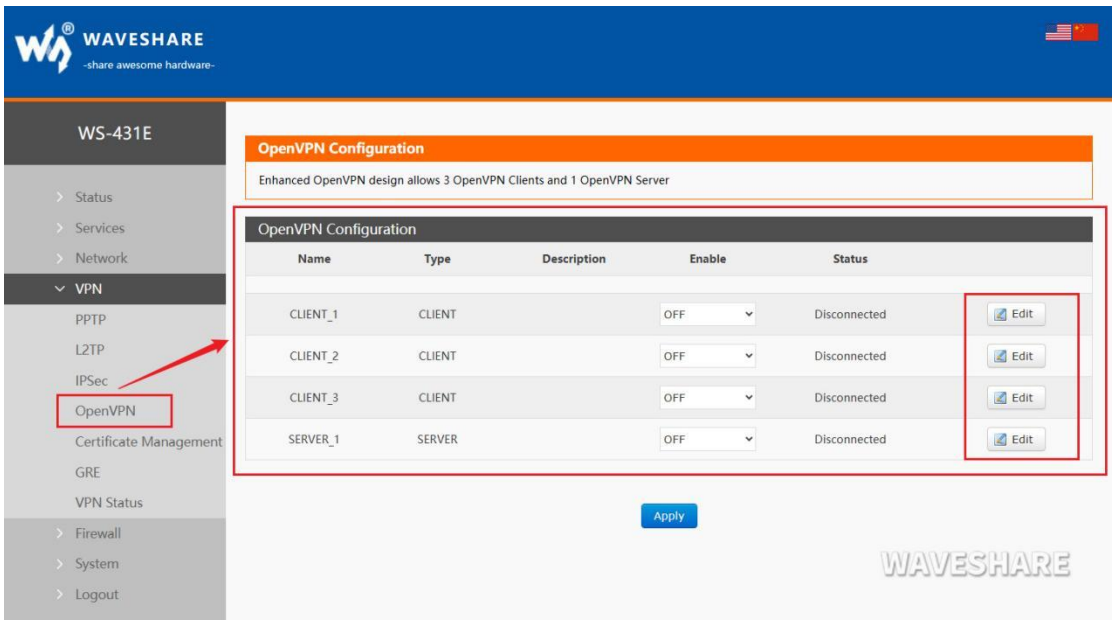


Figure 66 OpenVPN Enable Settings Interface

< Description >

- Device: TUN (routing mode) or TAP (bridge mode) can be selected;
- Channel protocol: UDP or TCP;
- Port: the listening port of OpenVPN client;
- VPN server address: IP/ domain name of OpenVPN server;
- Interface: wan_4G, wan_wired and automatic can be selected according to different networking modes;
- CA certificate: CA certificate common to both server and client;
- CRT public certificate: client certificate;
- Client private key: the key of the client;
- TLS authentication key: the authentication key of the secure transport layer;
- Encryption algorithms: None, Blowfish-128, DES-128, 3DES-192, AES-128, AES-192, AES-256. Hash algorithm: none, SHA1, SHA256, SHA512, MD5. Encryption and hash algorithms must be consistent with the VPN server.
- Use LZO Compression: Enable or disable the use of LZO compression for transmitting data.
- NAT Settings: This function is turned on by default. When the content needs to communicate with the outside, replace the internal address with the public address. If this item is turned off, the network address translation function cannot be realized;
- Enable Keepalive: enabled by default and configured as keepalive 10 120 by default. This setting should correspond to the VPN server;
- MTU setting: set the MTU value of the channel, which is 1500 by default. This setting should correspond to the VPN server; Enable Ping function: after setting the address of ping detection, vpn can be reconnected under abnormal disconnection;
- OpenVPN connection is successful: after successfully connecting with the VPN server, enter the VPN--VPN state to check the connection status.
- Note:
- Before the client connects with the server, CA certificate, client certificate, client key and TLS authentication key need to be provided by the server.

- After obtaining the certificate file, add different certificate contents to the configuration interface respectively.

### 4.7.5. GRE

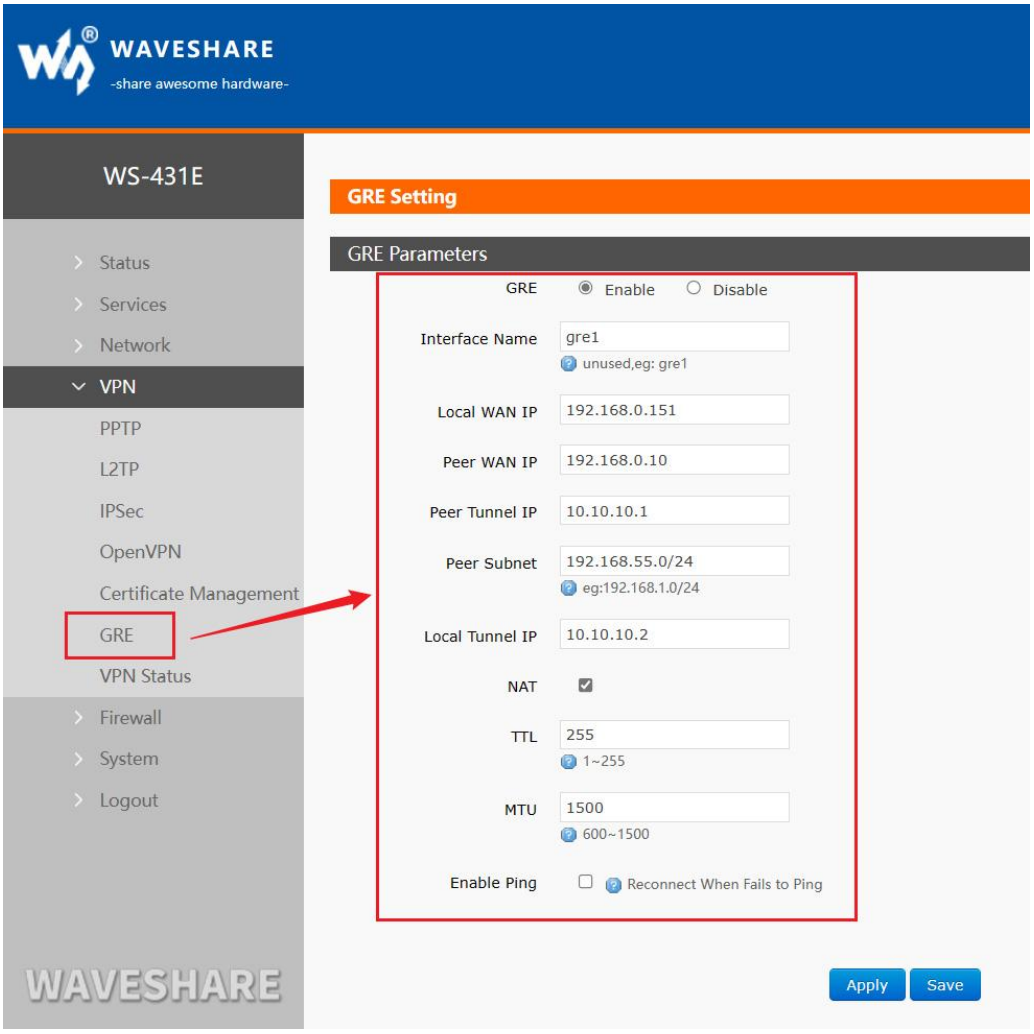



Figure 67 GRE basic configuration

< Description >

- Peer WAN IP: The WAN IP address of the remote GRE peer.
- Local WAN IP: the addresses of local wan_wired and wan_4G, which are input differently according to the networking mode;
- Remote Tunnel IP: The GRE tunnel IP address of the remote endpoint.
- Peer Subnet: setting subnet mask can be expressed as follows: 255.255.255.0 can be written as IP/24, 255.255.255 can be written as IP/32.

For example: 172.16.10.1/24, corresponding to IP of 172.16.10.1 and subnet mask of 255.255.255.0;

- Local tunnel IP: IP address of local GRE tunnel;
- TTL: set the TTL of GRE channel, which is 255 by default;
- Set MTU: set the MTU of GRE channel, and the default is 1450.