WideIOT

Industrial Routers

User Manual

Document Version : V1.1

Email: Info@wideiot.com
Website: www.wideiot.com
Xiamen WideIOT Technology Co., Ltd.

Contents

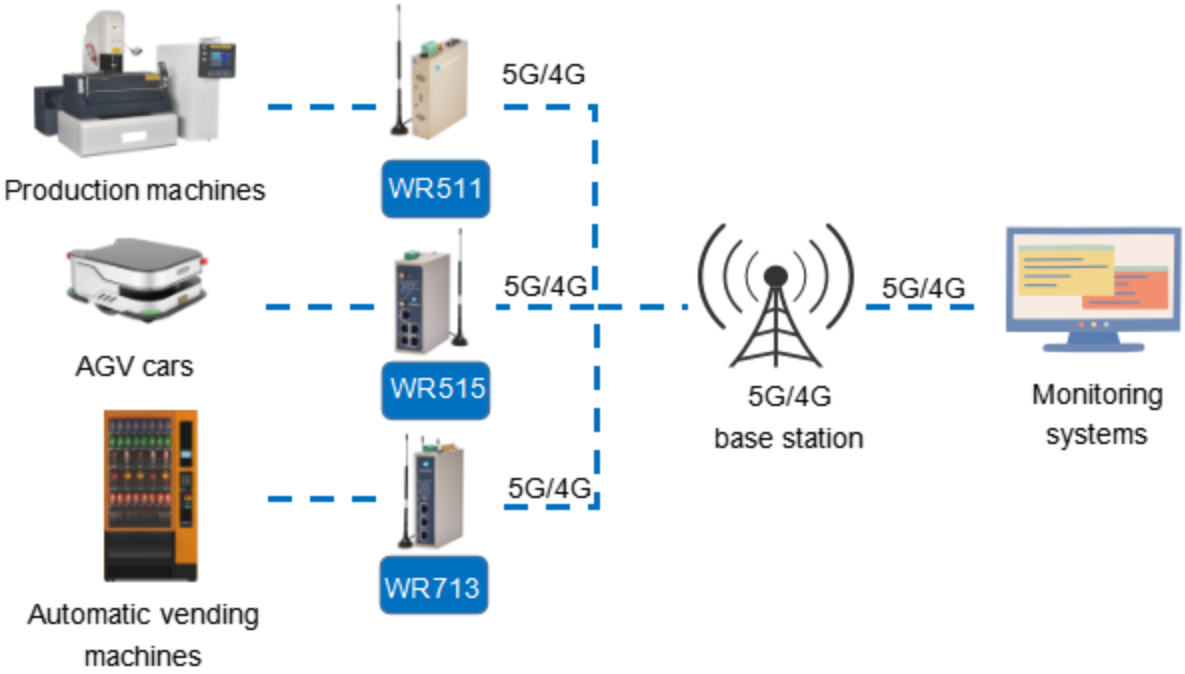
1. Product Overview

1.1. Overview

The WR series products are IoT wireless intelligent products integrating 5G/4G/3G/WiFi network, virtual VPN private network and other technologies, which meet the basic communication needs of industrial on-site applications. Among them, the 5G networking function supports high-bandwidth (up to 2.5Gbps), low-latency (up to 10ms level) and high-reliability access to 5G base stations; it supports 4G (TDD-LTE, FDD-LTE) and 3G (TD-SCDMA, CDMA 2000 EV-DO, HSPA+/WCDMA), and can be downward compatible with EDGE, CDMA 1X and GPRS networks respectively.

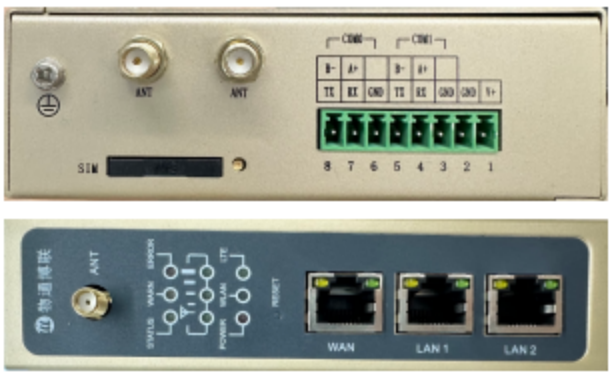
The design of this series of products fully meets the needs of industrial users. It adopts a software watchdog and software security guard to ensure the stability of the system and applications, a multi-level hardware and software detection mechanism, and a variety of VPN protocols to ensure the security of data transmission and prevent malicious access and tampering of data. The user-friendly WEB configuration interface design and multiple diagnosis and access methods facilitate user operation and project integration. It supports Wi-Fi function (optional) to provide wireless local area network access and wireless user identity authentication services for the customer's on-site environment. It supports connecting multiple network devices to realize multi-service processing.

It meets the needs of industrial users with low power consumption, an operating temperature range of -20℃ to 70℃, small size and light weight, which is convenient for application in harsh and narrow industrial environments, making it an ideal choice for industrial applications. This series is divided into multiple models according to the needs of the application site, including models classified by different network types, different numbers of network ports, different interfaces, different software functions, etc. For details, please consult technical engineers!



1.2. Technical Specifications

Product Interfaces



Note: Accessories and interfaces may vary by model, please refer to the actual product.

Power

Item	Content
Input Voltage	DC 12V
Acceptable Voltage Range	DC 6~35V

Power Consumption

Operating Mode	Power Consumption
Standby	80mA~120mA@12V
Communication	200mA~220mA@12V
Peak	240mA@12.0V

Physical Characteristics

Item	Content
Housing	Metal case (golden), IP30 protection level, suitable for most industrial control applications.
Dimensions	136x106.5x35(mm)
Weight	500g

Others

Item	Content
Operating Temperature	-20℃ ~ 70℃
Storage Temperature	-40 ℃~ 85℃
Relative Humidity	5% ~ 95% (no condensation)

2. Installation Guide

2.1. Installation Overview

The router can only realize its designed functions after correct installation.

⚠Warning:

Do not install the device when it is powered on.

2.2. Package Contents

For transportation safety, you need proper packaging. After unpacking the device, please keep the packaging materials for future transportation needs.

It includes the following components:

✧1 router

✧1 wireless cellular antenna (if the model has 4G function)

✧2 WiFi antennas (if the model has WiFi function)

✧1 power cable

✧ 1 Ethernet cable

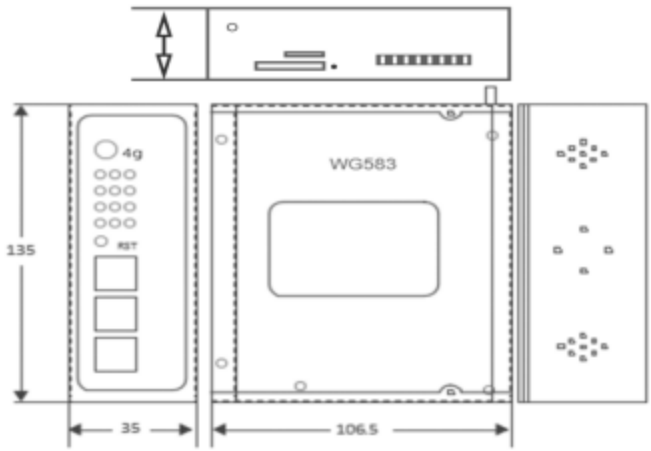
✧1 DIN rail clip

✧Product certification

✧Warranty card

2.3. Installation and Cable Connection

Dimensions (Unit: mm)



Antenna Installation：

The wireless 4G antenna interface is a standard SMA female interface (on the side). Insert the cellular antenna into this interface and ensure it is tightened to avoid affecting signal quality.

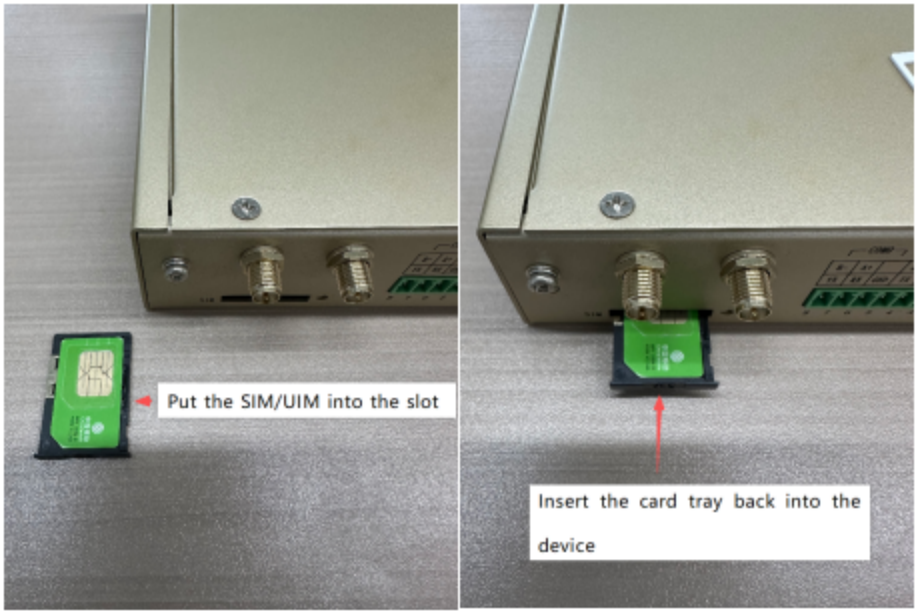
The wireless WiFi antenna interfaces are two standard SMA male interfaces (on the top). Insert the WiFi antennas into these interfaces and ensure they are tightened to avoid affecting signal quality.

Note: Do not mix 4G antennas with WiFi antennas, otherwise the device may not work properly.

SIM/UIM Card Installation Steps:

Gently press the circular pop-up button on the left side of the card slot, and the SIM/UIM card tray will pop out automatically. During installation, place the SIM/UIM card into the tray, ensuring the metal chip side faces outward, then insert the tray back into the device.

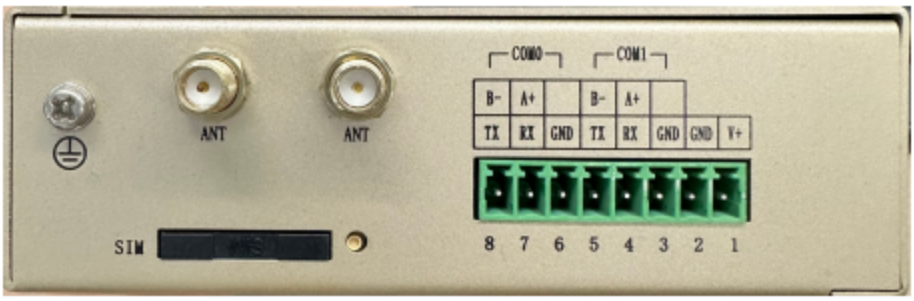
(The following is an example of the single-card version)



Ethernet Cable Connection :

Connect one end of the Ethernet cable to the LAN port of the router, and the other end to the Ethernet port of the user's device. The cable specification definition is as follows:

LAN1	LAN2	Color
1	1	White/Orange
2	2	Orange
3	3	White/Green
4	4	Blue
5	5	White/Blue
6	6	Green
7	7	White/Brown
8	8	Brown



3.5mm Terminal Block Interface Definition :

This 8-pin terminal block includes POWER (power supply) and RS485 (RS232) functions, with specific definitions as follows:

Power Wiring		
Terminal	GND	VIN
	V-	V+
Description	Connect to DC6-35V negative pole	Connect to DC6-35V positive pole

RS485 Wiring		
Terminal	B-	A+
	T/B	R/A
Description	Connect to device RS485-	Connect to device RS485+

RS232 Wiring			
Terminal	TX	RX	GND
	T/B	R/A	GND
Description	Connect to device RS232 RX	Connect to device RS232 TX	Connect to device RS232 GND

2.4. Power Supply Description

Routers are usually used in complex external environments. To adapt to the environment and improve system stability, the intelligent router adopts advanced power supply technology. Users can use the standard 12V DC / 1A power adapter provided with the device, or directly use a 6－35V wide-voltage DC power supply to power the device.

If users use other power supplies, they must ensure stable output (ripple less than 300mV, instantaneous voltage not exceeding 35V) and power greater than 8W. We recommend using the standard 12V DC / 1A power adapter provided with the device.

2.5. Indicator Light Description

The router is equipped with the following LED indicators:

"STATUS", "WARN", "ERROR", 3*4G signal strength indicators, "POWER", "WLAN" and "LTE".

Indicator	Status	Description
STATUS	Blinking	In operation
WARN	Steady on	Failed to connect to 4G network
	Steady off	4G connected / not enabled
ERROR	Steady on	Abnormal operation
	Steady off	Normal operation
POWER	Steady on	Normal power supply
WLAN	Steady on	WiFi enabled
	Steady off	WiFi disabled
LTE	Steady on	4G enabled
	Steady off	4G disabled

2.6. Reset Function

The router is equipped with a reset button marked "Reset", which is used to restore the device to factory settings.

Operation Steps:

Power off and then power on the router again.

When the STATUS and WARN indicators start to flash alternately, immediately press and hold the RESET key;

Release the key when the ERROR light enters the slow blinking state (or hold for 3 seconds and then release);

Press and hold the RESET key again until the ERROR light turns to fast blinking, then release (or hold for 3 seconds and then release);

At this point, the router will start to reset automatically.

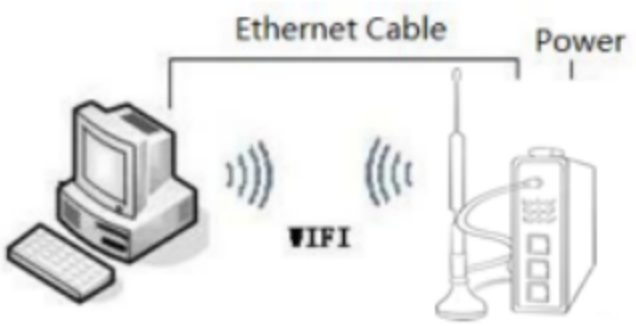
3. Configuration and Management

3.1. Configuration Connection

Connection Method Before Router Configuration

Before configuring the router, please connect it to the computer using the provided network cable.

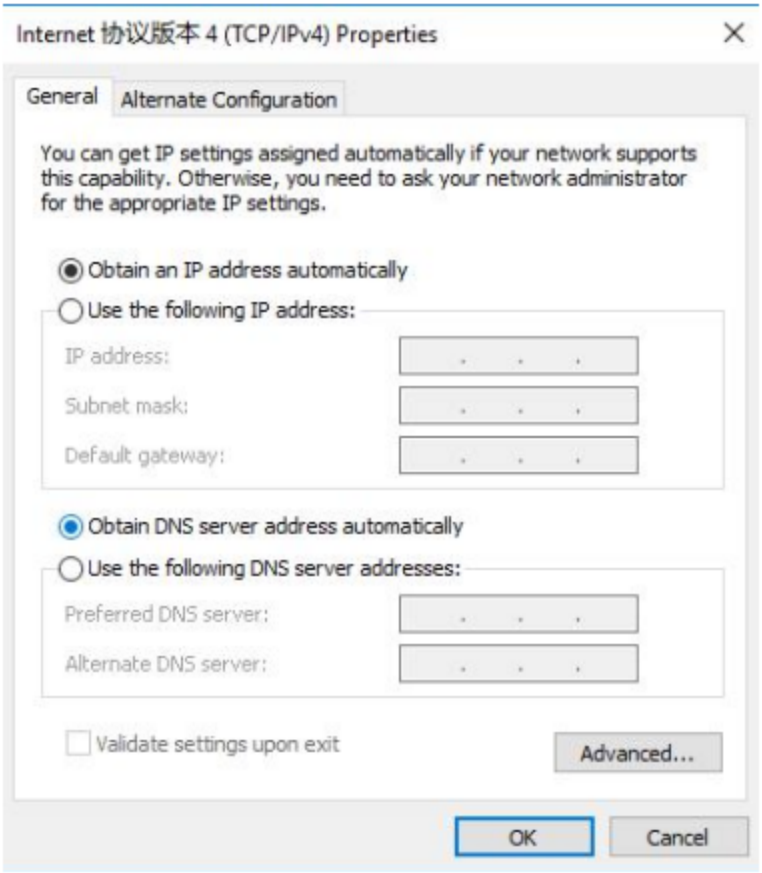
Wired connection: Insert one end of the network cable into any LAN port of the router, and the other end into the Ethernet port of the computer.



3.2. Accessing the Configuration Interface

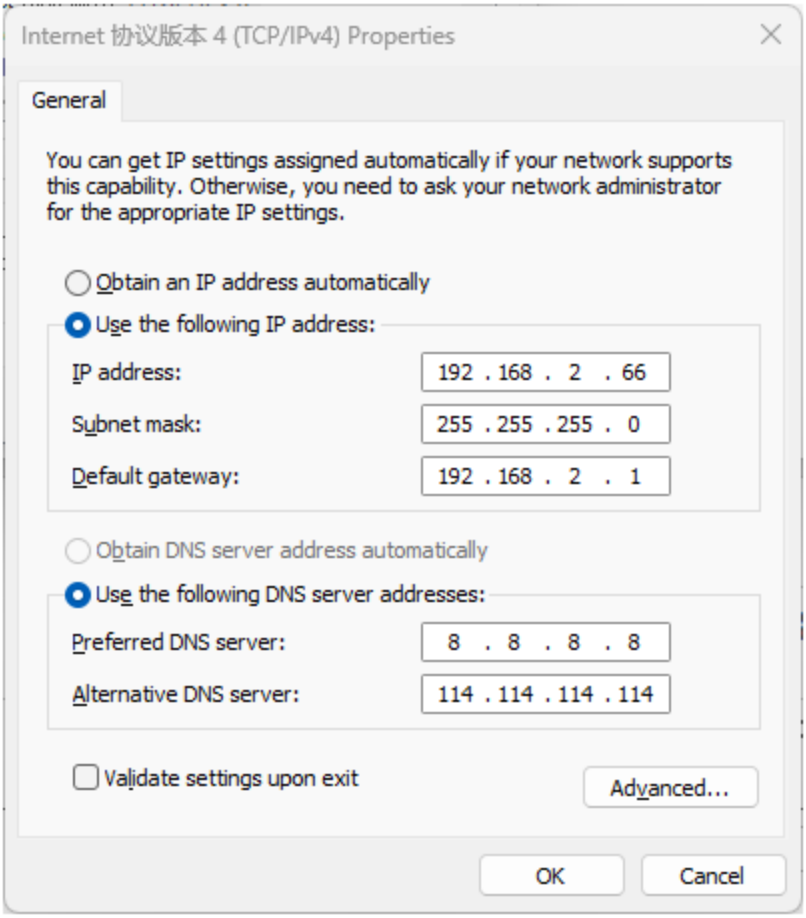
3.2.1. Computer IP Address Setting (Two Methods)

Method 1: Obtain IP Address Automatically



Method 2: Static IP Address Setting

Set the computer's IP address to 192.168.2.10 (or other IP addresses in the 192.168.2 network segment), set the subnet mask to 255.255.255.0, and set the default router to 192.168.2.1. The DNS can be set to any available DNS server in the local area.



3.2.2. Logging in to the Configuration Interface

This chapter will introduce the main functions of each setting page. Users can access the router's configuration interface through a web browser on the connected computer. The configuration interface includes 11 main pages: Setup, Wireless, Services, VPN, Security, Access Restrictions, NAT, QoS Setting, Applications, Administration and Status.

To access the web-based configuration tool, open IE or another browser, enter the default router IP address 192.168.2.1 in the address bar, and press Enter.

Please enter the correct username and password, then click "Login". The default username is "admin" and the default password is "123456". You can modify the default username and password in the "System" section.

3.3. Configuration and Management Functions

3.3.1. Ethernet Settings

1) Basic Settings

"WAN (Wide Area Network)" - This section is used to configure the way the router connects to the Internet. Specific parameter information can be obtained from your Internet Service Provider (ISP).

WAN Connection Type Setting

Please select the required connection type from the drop-down menu. There are 3 optional types: Static IP, Automatic Configuration-DHCP, and PPPoE.

Type 1: Static IP

This connection type is usually used for dedicated line access, such as enterprise or commercial optical fiber. The Internet Service Provider (ISP) will provide you with detailed network parameters, such as IP address, subnet mask, gateway and DNS information. You need to use these parameters to configure the router.

Type 2: Automatic Configuration - DHCP

This is the default WAN connection type, which is adopted by some wired network service providers and home broadband Internet services.

The IP address of the WAN port will be automatically obtained through DHCP.

Type 3: PPPoE

ADSL services of China Telecom and China Unicom usually adopt this connection type, and other operators may also use this type. When using PPPoE connection, the Internet Service Provider (ISP) needs to provide the username, password and service name, and fill this information into the relevant setting fields of the router.

PAP/CHAP Username: The username used to log in to the Internet

PAP/Password: The password used to log in to the Internet

2) MAC Address Cloning

Some Internet Service Providers (ISPs) require users to register a MAC address. If the user does not want to re-register the MAC address, the router's MAC address can be cloned to the MAC address that has been registered with the ISP.

3.3.2. Wireless WiFi Settings

1) Basic Settings

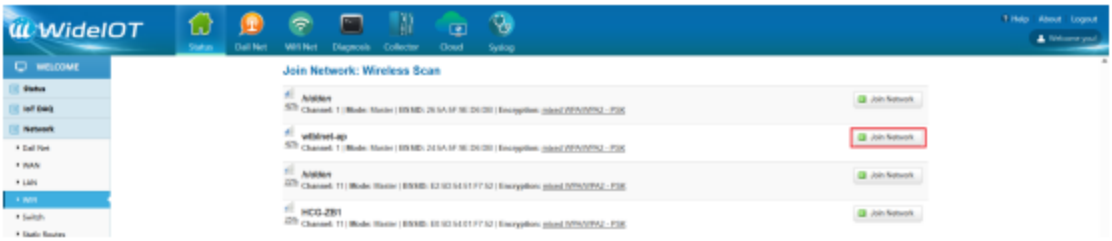
WIFI client Configuration

WiFi Network - Click to enable

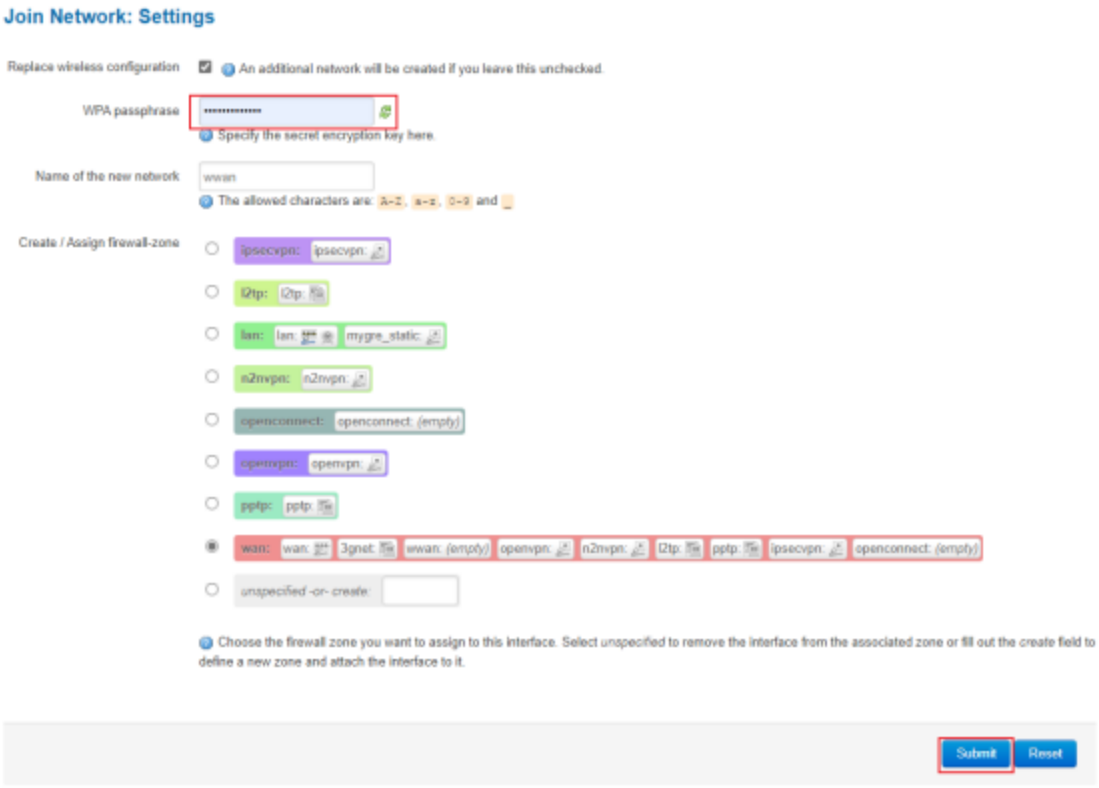
Click "Advanced Options"

Click "Scan"

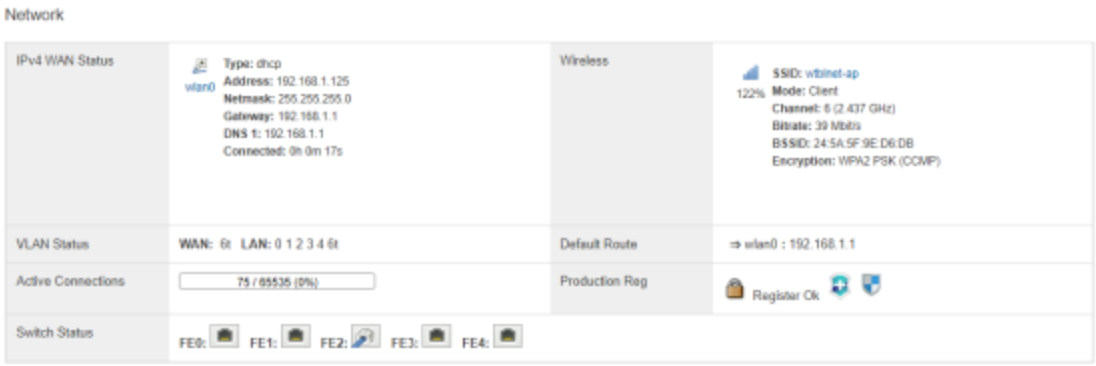
Click "Join Network"



Enter the WiFi password - Save to complete the configuration



Click "Status" - Scroll down to check the WiFi connection status. The following figure indicates that WiFi is connected.

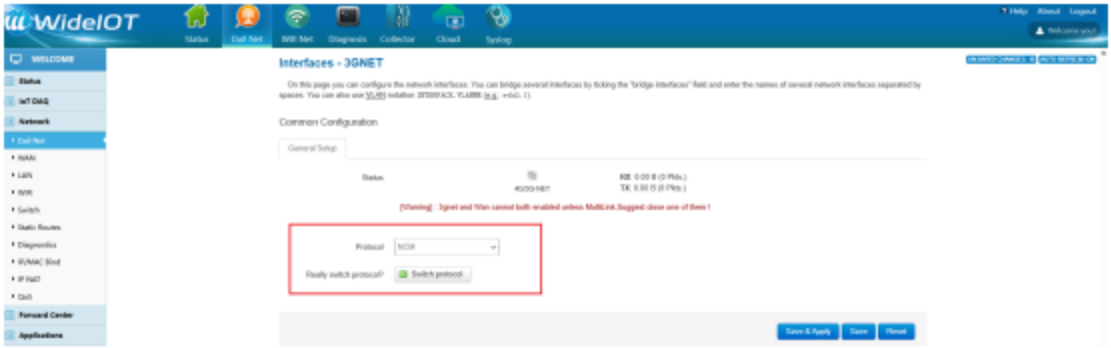


3.3.3. Dial-up Network Settings

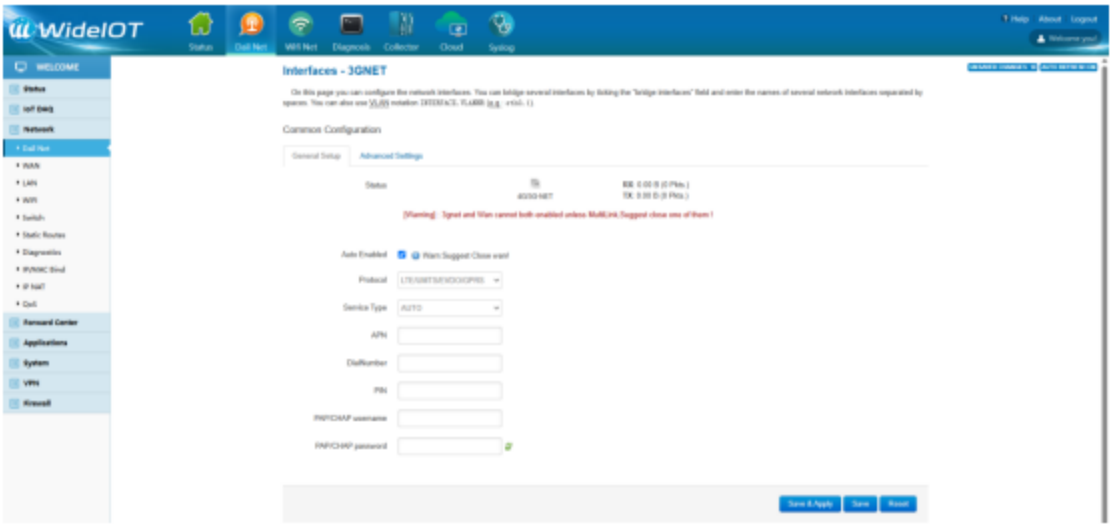
1) Basic Settings

Data Card Internet Configuration

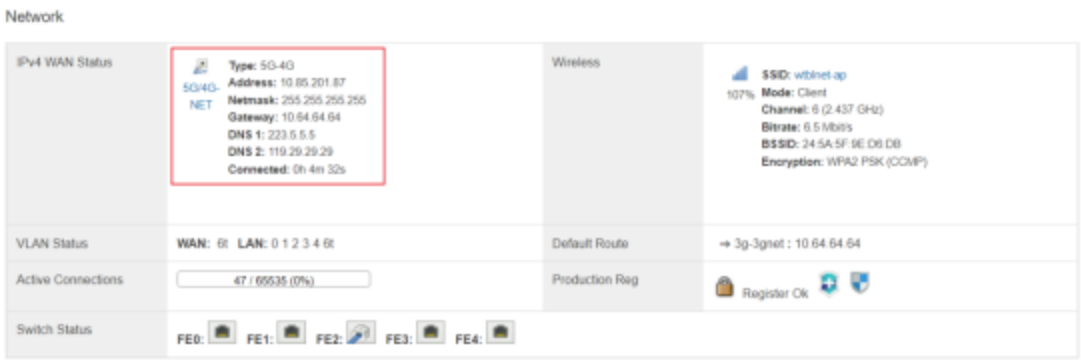
For WR7 series dial-up network - Switch the communication protocol to NCM (5G mode), click "Save & Apply". The dial-up network is checked by default at the factory.



For WR5 series dial-up network - Switch the communication protocol to LTE (4G mode), click "Save & Apply". The dial-up network is checked by default at the factory.



Click "Status" - "Overview" - "Network Interface" - Check the network connection information



Use the diagnostic command PING to test Baidu to confirm Internet access is available.

Note: If no card is inserted, the SIM card is in poor contact, no antenna is connected, or the data card is in arrears, the system will restart irregularly.

3.3.4. VPN Configuration

1) PPTP

PPTP (Point-to-Point Tunneling Protocol) is a protocol that can be used for secure transmission (by establishing a VPN network). It is an extended protocol of the PPP protocol. Different from the PPP data link layer, it encapsulates PPP data packets (such as dial-up authentication, IP allocation, etc.) in IP data packets of the TCP/IP network. PPTP can also be used in private LAN-To-LAN networks.

Basic Settings

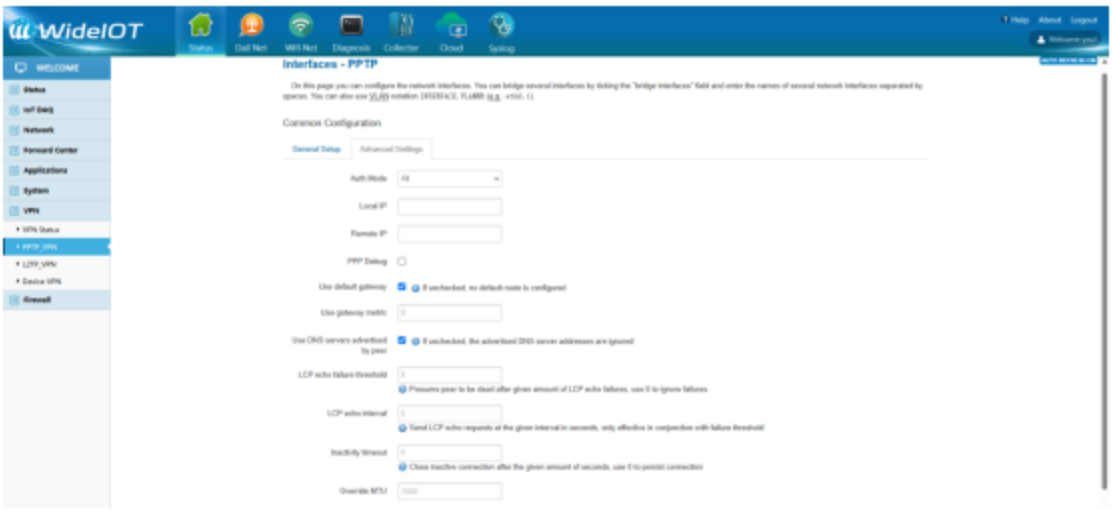
Enable "Auto Enabled", enter the VPN server address, client username, and client user password.

Advanced Settings

Authentication Mode

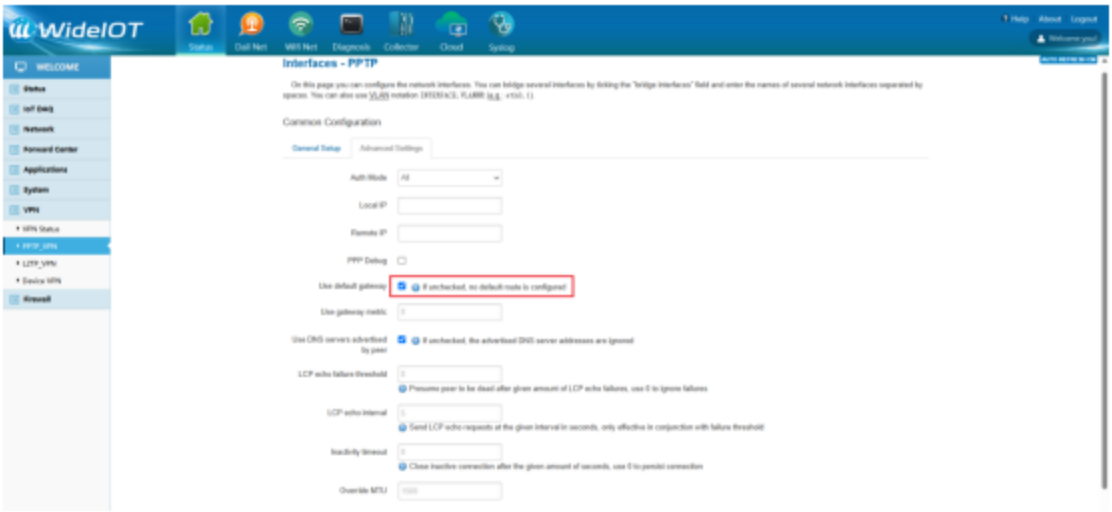
When accessing a VPN server based on the Linux system, select: ALL/pap/chap.

When accessing a VPN server based on the Windows system, select: Mschap/Mschap-v2.



Dual-channel Mode

Dual-channel Internet access: To access both the public network and use the VPN service, you need to uncheck the "Use default gateway" option of PPTP.

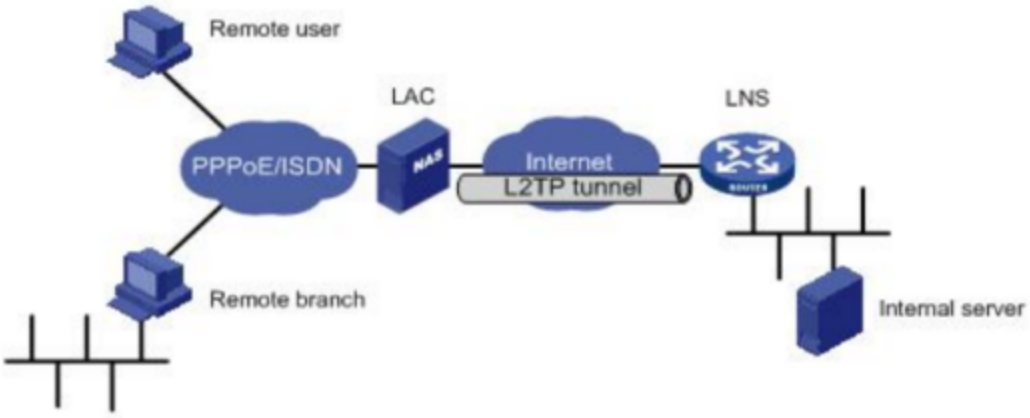


Specify the client tunnel address. After completing the basic settings and advanced settings, you can click "Save & Apply".

```
pptp-pptp Link encap:Point-to-Point Protocol
          inet addr:100.100.100.2  P-t-P:100.100.100.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1200  Metric:1
          RX packets:574 errors:0 dropped:0 overruns:0 frame:0
          TX packets:687 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:50091 (48.9 KiB)  TX bytes:55970 (54.6 KiB)
```

2) L2TP

L2TP (Layer 2 Tunneling Protocol) is a type of VPDN (Virtual Private Dial-up Network) tunneling protocol. VPDN refers to using the dial-up function of the public network to access the public network and realize a virtual private network, thereby providing dedicated network access services for industrial on-site equipment. That is, VPDN provides an economical and effective point-to-point connection method between remote users and private enterprise networks.。



Basic Settings

Check "Auto Enabled", enter the "L2TP Name", enter the public IP address or domain name of the VPN server in the "L2TP Server" field; enter the username and password created earlier on the VPN server in the "Username" and "Password" fields, which need to be consistent;

Advanced Settings

According to the type of L2TP server, more in-depth configuration can be performed in the advanced options. Generally, only basic configuration is required. The L2TP server of the Linux embedded system generally uses the CHAP authentication mode, and Windows generally selects Mschap-V2. If you are not sure, please select ALL, then click "Save".

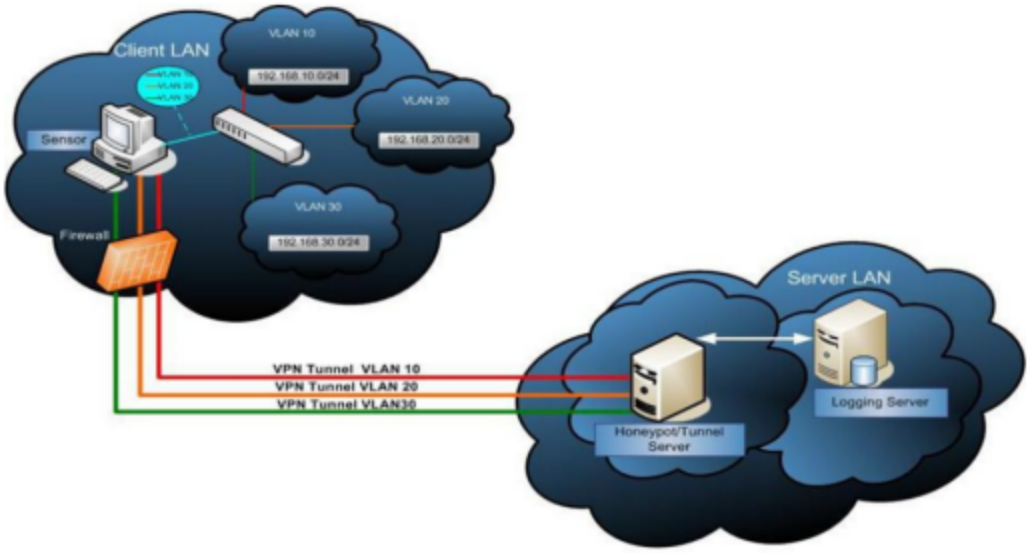

```
l2tp-l2tp Link encap:Point-to-Point Protocol
          inet addr:200.200.200.12  P-t-P:200.200.200.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1200  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:46 (46.0 B)  TX bytes:572 (572.0 B)
```

3) OPEN VPN

VPN technology establishes a private tunnel on the public network through key exchange, encapsulation, authentication, and encryption methods to ensure the integrity, privacy, and validity of transmitted data.

OpenVPN uses a virtual network card to implement the function of SSLVPN in a new way, which can adapt to almost all applications above the IP layer. All communications of OpenVPN are based on a single IP port. By default and recommended to use UDP protocol for communication, and TCP is also supported. OpenVPN connections can pass through most proxy servers and work well in NAT environments. The server has the function of "pushing" certain network configuration information to the client, which includes: IP address, routing settings, etc. OpenVPN provides two types of virtual network interfaces: general Tun/Tap drivers, through which a three-layer IP tunnel or a virtual two-layer Ethernet can be established. The latter can transmit any type of two-layer Ethernet network data. The transmitted data can be compressed through the LZO algorithm. The official port assigned by IANA (Internet Assigned Numbers Authority) to OpenVPN is 1194.

The feature that OpenVPN uses general network protocols (TCP and UDP) makes it an ideal alternative to protocols such as IPsec, especially when the ISP (Internet Service Provider) filters certain specific VPN protocols.



Configuration Parameters

Description of relevant parameters for configuring OpenVPN on the router.

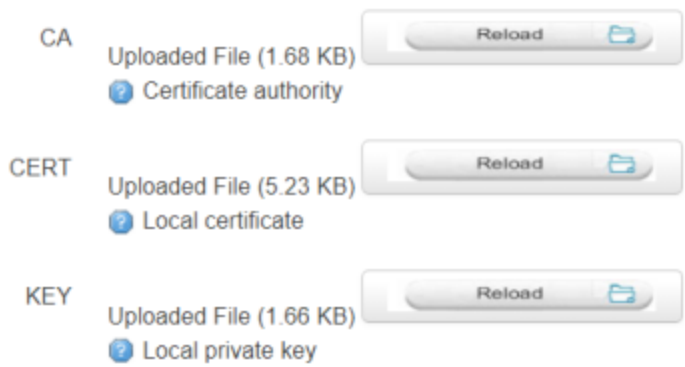
OpenVPN Configuration Parameters		
No.	**Configuration Parameter**	**Description**
1	remote port	192.168.1.15 1194
2	proto	udp tcp
3	nobind	Do not bind
4	remote_random	None
5	comp_lzo	yes

6	tun_ipv6	None
7	verb	6
8	ca	ca.crt
9	dh	dh2048.pem
10	cert	some-client.crt
11	key	some-client.key
12	auth_user_pass	Not set (non-password)
13	username	Not set (non-password)
14	password	Not set (non-password)
15	keepalive	10 60
16	pkcs12	some-client.pk12 (None)
17	secret	secret.key (None)

VPN Configuration

Enter the IP address and port number of the local machine on the server in the "Remote Host" field, and select TCP as the communication protocol.

Upload the computer client CA root certificate, local certificate, and local private key, and finally click "Save & Apply".



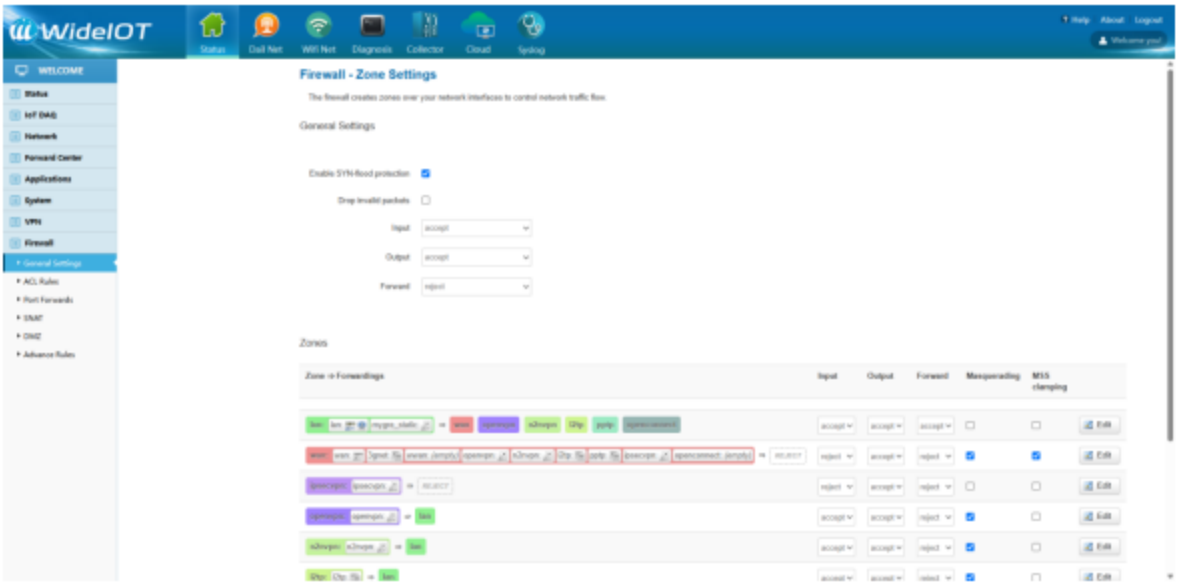
3.3.5. Security Settings

1) Firewall

Firewall settings include parameter settings for basic settings, access control, port forwarding, SNAT, DMZ, advanced rules, etc.

Basic Settings

This page is for basic settings, and in most cases, there is no need to configure this part of the content.



Access Control

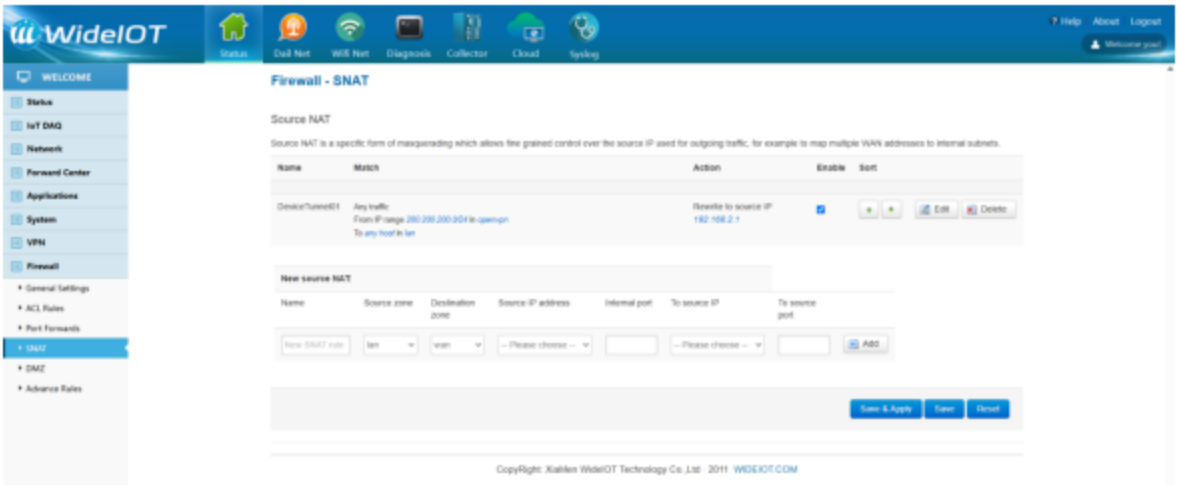
This page is for basic access control settings. ACL (Access Control List) rules are used to define the transmission policy of data packets entering the internal network from the external network, and can perform fine-grained control over the protocol, destination IP address, external port, source IP address, internal port, and action (accept, drop, reject).

Port Forwarding

Port forwarding, also known as port mapping, is to map a port of the external network host's IP address to a machine in the internal network for corresponding services. When a user accesses this port of the IP, the router automatically maps the request to the corresponding machine in the internal LAN. The common application is to open a fixed port on the router, then set which internal IP and port the data received by this port should be forwarded to. This mapping relationship will exist all the time regardless of whether there is a connection. This allows the public network to actively access a computer in the internal network.

SNAT

SNAT (Source Network Address Translation) refers to replacing the source address and port in the data packet with the specified IP address and specified port when the data packet is sent from the router. In this way, the receiver will think that the source of the data packet is the host and port corresponding to the replaced IP. Source NAT is a special form of packet masquerading, which allows fine-grained control over the source IP of outgoing traffic.



DMZ

The DMZ (Demilitarized Zone) firewall solution adds an additional security barrier to the internal network to be protected and is generally considered very secure. At the same time, it provides an area for placing public servers, which can effectively avoid conflicts between the need for some Internet applications to be public and the internal security policy.

Advanced Rules

Advanced applications mainly provide more refined and flexible firewall control. There are several commonly used advanced rules by default, and these advanced rules should not be deleted.

WideIOT

-Industrial IoT product and digital solution

Website

Xiamen WideIOT Technology

www.wideiot.com

+86-592-2031080

info@wideiot.com

Xiamen softpark III ,Fujian,China