WideIOT

NAT Coupler

User Manual

Document Version： V1.1

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

Contents

1. Product Introduction

1.1. Overview

The WideIOT NAT Coupler is a security isolation product designed for high-reliability production networks. It facilitates the integration of newly procured devices (e.g., PLCs, CNCs, DCS) by performing IP reassignment for seamless network access. It isolates broadcast and collision domains through network segmentation and enables bidirectional communication between devices across two different subnets. This solution is widely deployed for network isolation in smart factories, mines, oil wells, and other scenarios demanding high reliability.

2. Installation Guide

2.1. Installation Overview

The NAT Coupler must be installed correctly to achieve its designed functions.

⚠Warning:

Do not install the device while it is powered on.

2.2. Package Contents

For transportation safety, proper packaging is required. After unpacking the device, keep the packaging materials for future transportation needs.

It includes the following components:

✧1 NAT Coupler

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

✧1 power cable

✧1 Ethernet cable

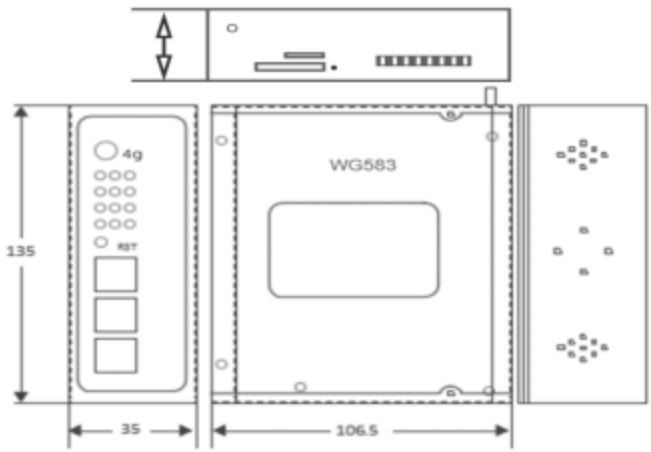
✧1 DIN rail clip

✧Product certification

✧ Warranty card

2.3. Installation and Cable Connection

Dimensions (Unit: mm)



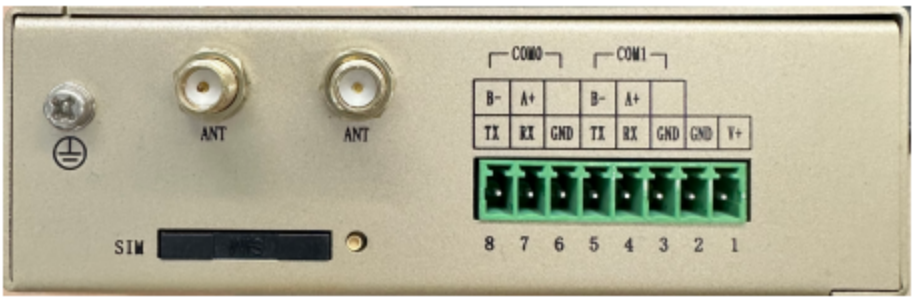
Antenna Installation：

The wireless WiFi antenna interfaces are 2 standard SMA male connectors (located on the top). Insert the WiFi antennas into these interfaces and ensure they are tightened to avoid affecting signal quality.

Ethernet Cable Connection :

Connect one end of the Ethernet cable to the LAN port of the NAT Coupler, and the other end to the Ethernet port of the user's device. The cable specification is defined 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	Connect to DC6-35V positive

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 RS232RX	Connect to device RS232TX	Connect to device RS232GND

2.4. Power Supply Description

The NAT Coupler is usually used in complex external environments. To adapt to the environment and improve system stability, this NAT Coupler 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. It is recommended to use the standard 12V DC / 1A power adapter provided with the device.

2.5. Indicator Light Description

The NAT Coupler is equipped with the following LED indicators:

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

Indicator	Status	Description
STATUS	Blinking	In operation
WARN	Steady on	Failed to connect to 4G network
	Steady off	4G connected / 4G 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

This NAT Coupler is equipped with a reset button marked "Reset", which is used to restore the device to factory settings.

Operation Steps:

Power off and then repower the NAT Coupler.

When the STATUS and WARN indicators start alternating blinking, immediately press and hold the RESET key.

Release the RESET key when the ERROR light enters slow blinking mode (or after holding for 3 seconds).

Press and hold the RESET key again until the ERROR light turns to fast blinking mode (or after holding for 3 seconds).

The NAT Coupler will then begin automatic resetting.

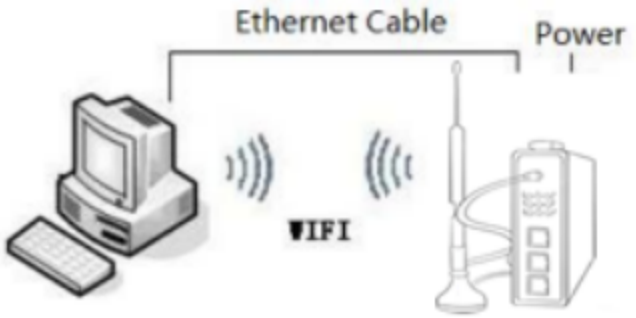
3. Configuration and Management

3.1. Configuration Connection

Connection Method Before NAT Coupler Configuration

Before configuring the NAT Coupler, use the provided network cable to connect it to the computer first.

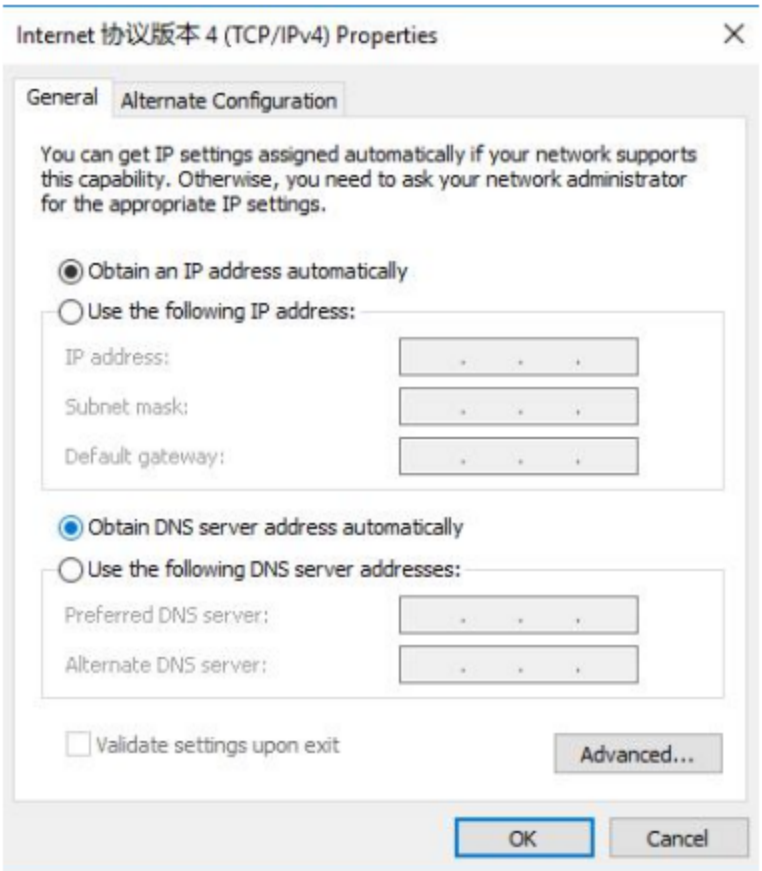
Wired connection: Insert one end of the network cable into any LAN port of the NAT Coupler, and the other end into the Ethernet port of the computer.



3.2. Accessing the Configuration Interface

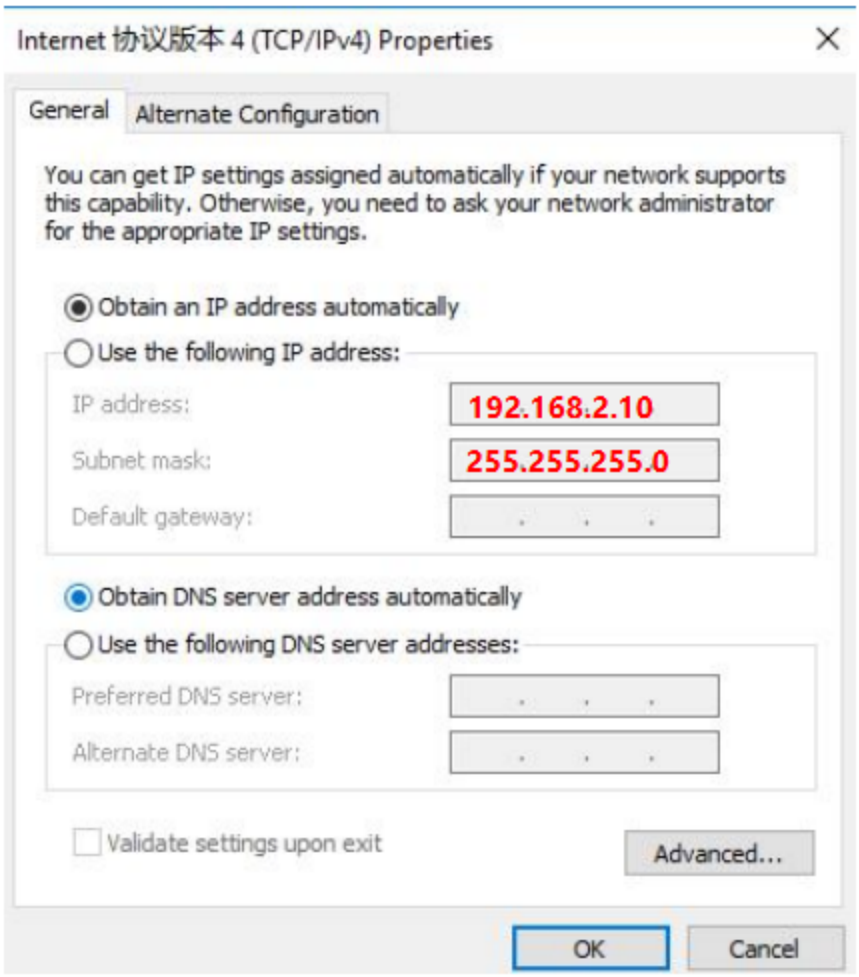
3.2.1. Computer IP Address Setting (Two Methods)

Method 1: Automatic IP Address Acquisition



Method 2: Static IP Address Settings

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



3.2.2. Logging in to the Configuration Interface

This chapter will introduce the main functions of each setting page. Users can access the configuration interface of the NAT Coupler 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 NAT Coupler IP address 192.168.2.1 in the address bar, and press Enter.

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

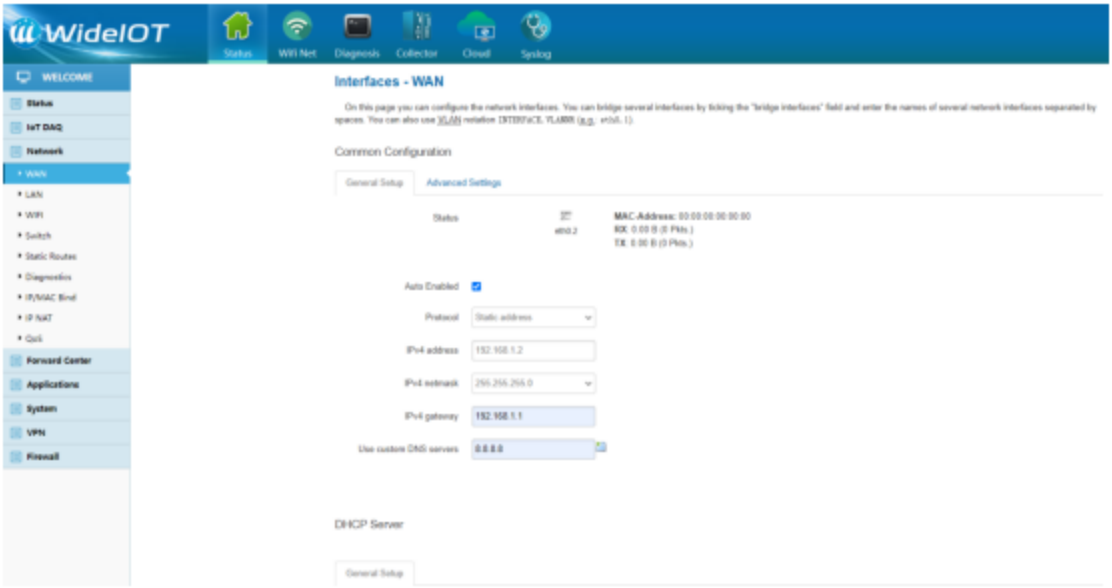
"WAN External Network" - This section is used to configure the way the NAT Coupler connects to the Internet. Specific parameter information can be obtained from your Internet Service Provider (ISP).

WAN Connection Type Setting

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 NAT Coupler.



Type 2: Automatic Configuration - DHCP

This is the default WAN connection type, which is used 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

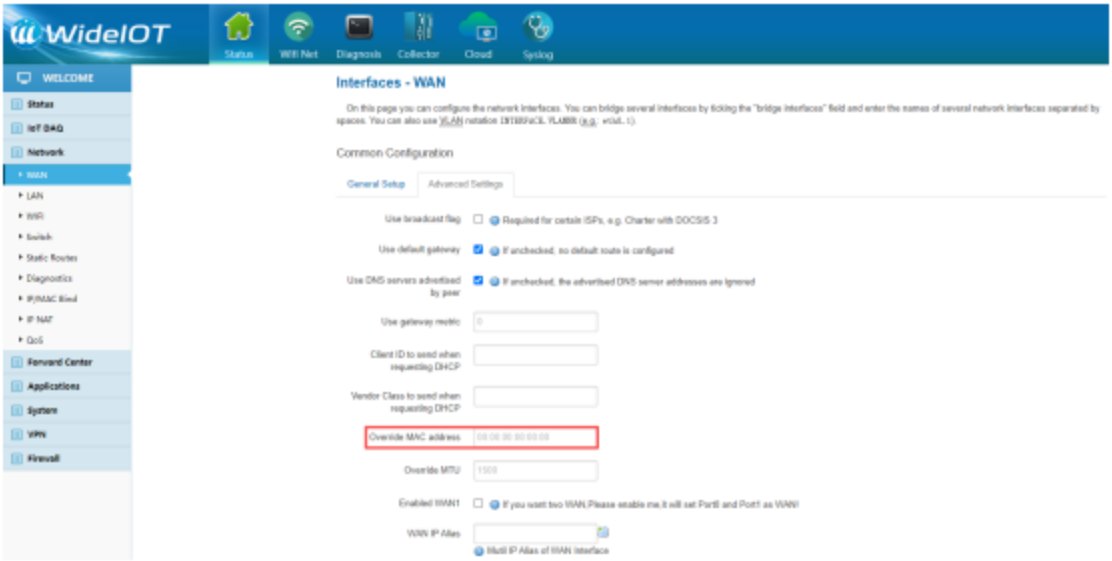
ADSL services of China Telecom and China Unicom usually use this connection type, and other operators may also use it. When using PPPoE connection, the Internet Service Provider (ISP) needs to provide the username, password and service name, and fill this information into the relevant setting fields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

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

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

2) MAC Address Cloning

Some Internet Service Providers (ISPs) require users to register the MAC address. If the user does not want to re-register the MAC address, the MAC address of the NAT Coupler 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

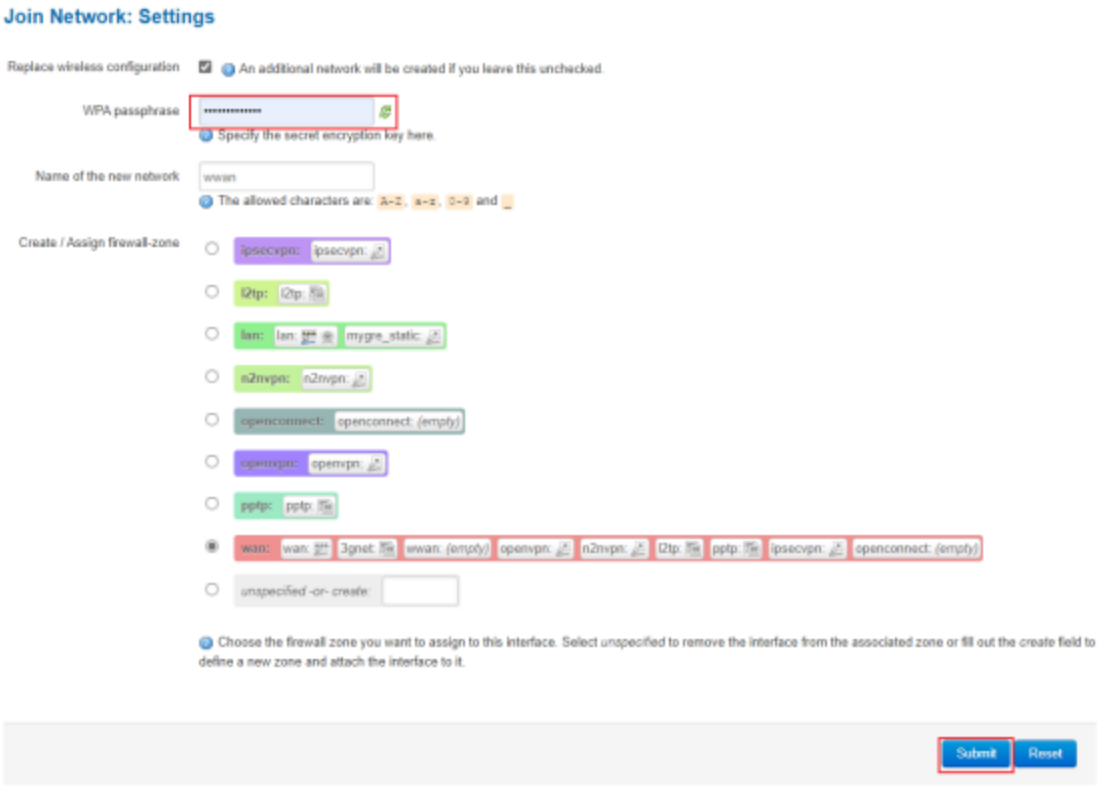
WiFi Network - Click to enable

Click "Advanced Options"

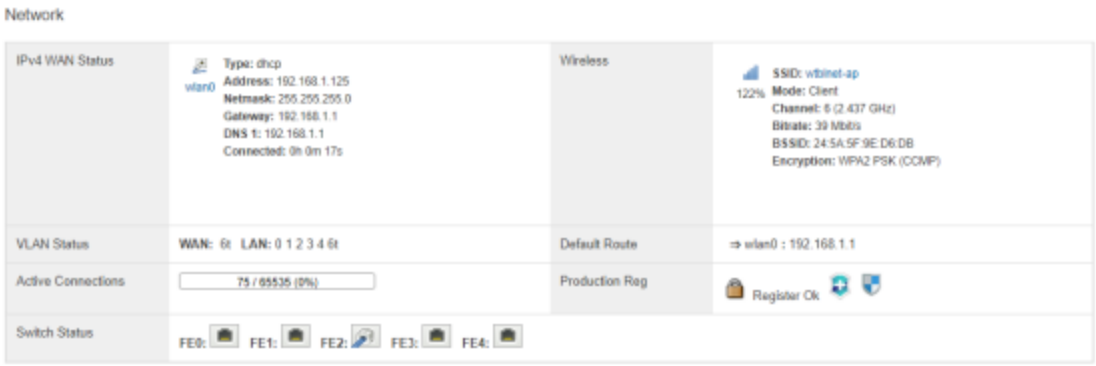
Click "Scan"

Click "Join Network"

Fill in the WiFi password and save



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



3.3.3. Security Settings

1) Firewall

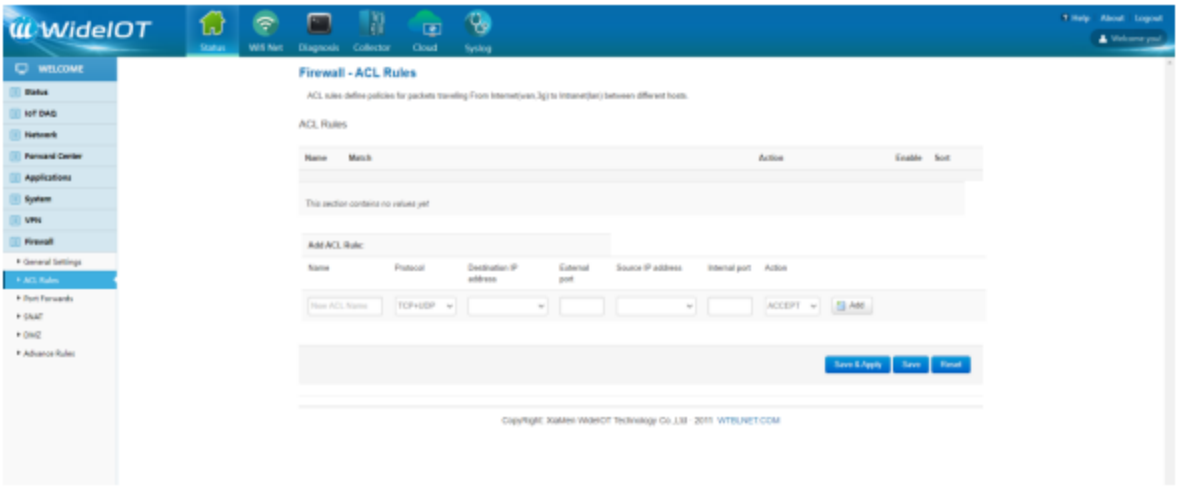
Firewall settings include parameter settings for basic settings, access control, port forwarding, SNAT, DMZ, advanced rules, etc.

Basic Settings

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

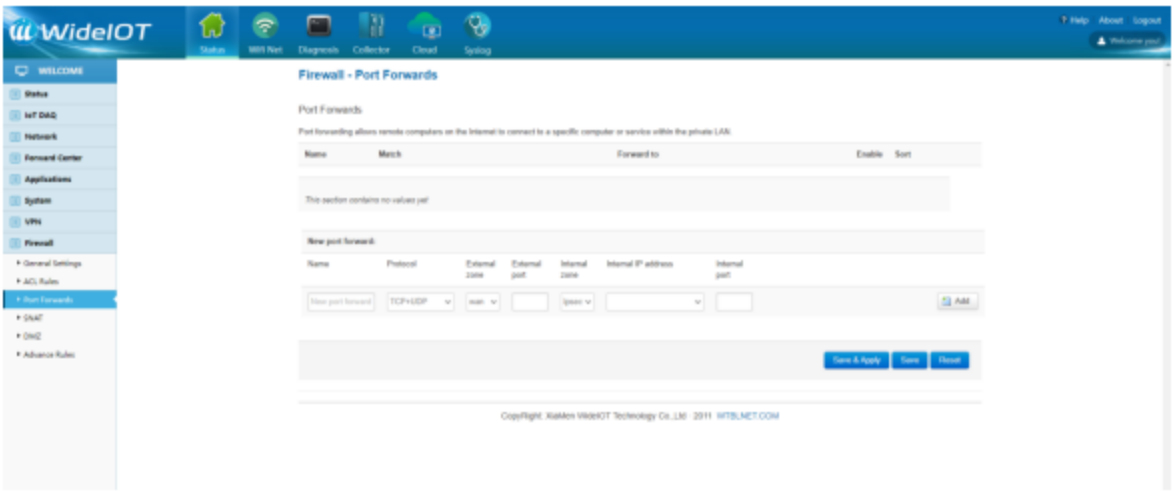
Access Control

This page is for basic access control settings. ACL rules (Access Control Lists) define the transmission policy for data packets entering the internal network from the external network, and can perform fine-grained control over protocols, destination IP addresses, external ports, source IP addresses, internal ports, and actions (accept, drop, reject).



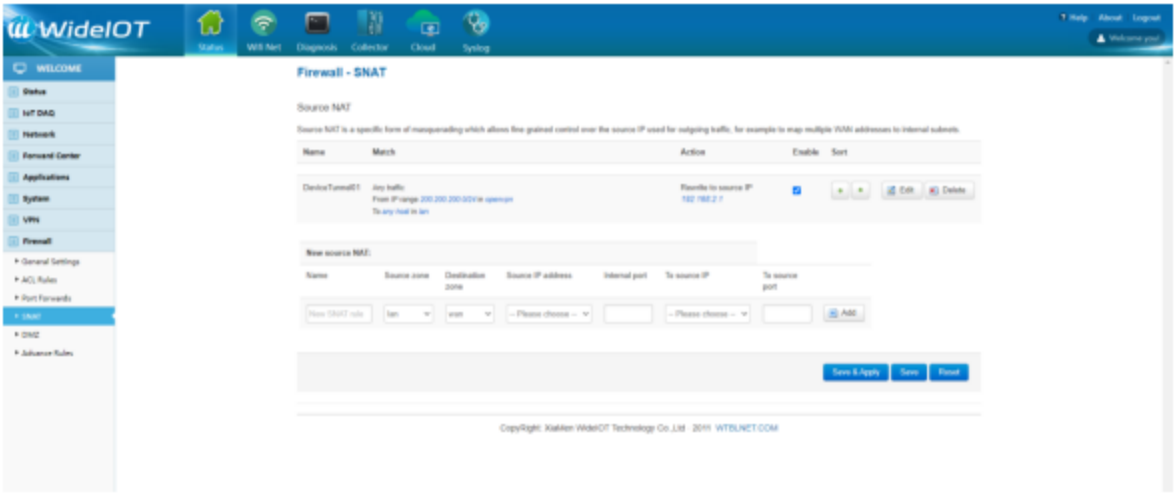
Port Forwarding

Port forwarding, also known as port mapping, maps 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 NAT Coupler automatically maps the request to the corresponding machine in the internal LAN. This is usually applied by opening a fixed port on the NAT gateway (NAT Coupler), then setting which internal IP and port the data received by this port should be forwarded to. This mapping relationship exists at all times regardless of connections, allowing the public network to actively access a computer in the internal network.



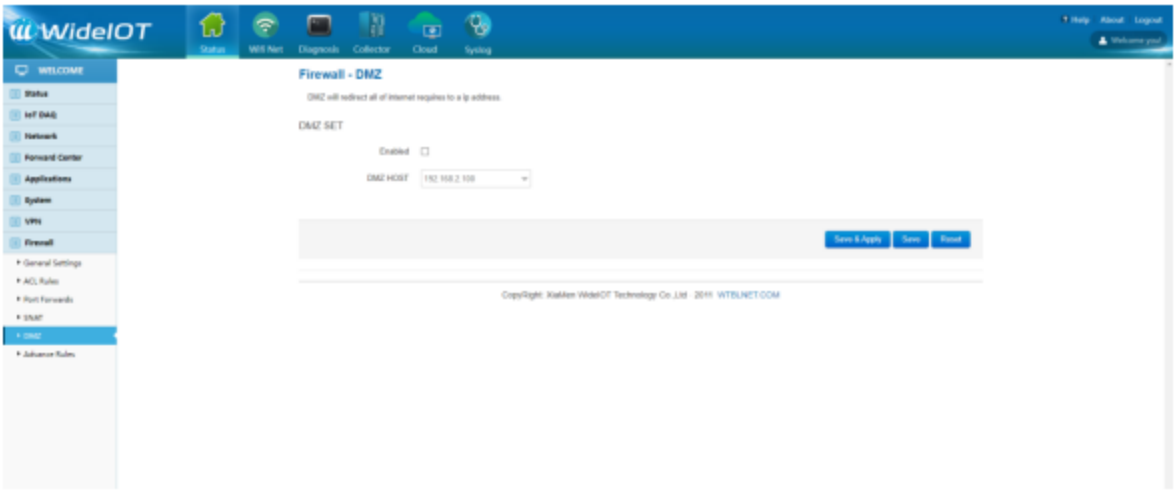
SNAT

SNAT (Source Network Address Translation) refers to replacing the source address and port in the data packet with the specified IP address and port when the data packet is sent from the NAT Coupler. In this way, the receiver will consider the source of the data packet as 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 highly secure. At the same time, it provides an area for placing public servers, effectively avoiding conflicts between the need to make some Internet applications public and internal security policies.

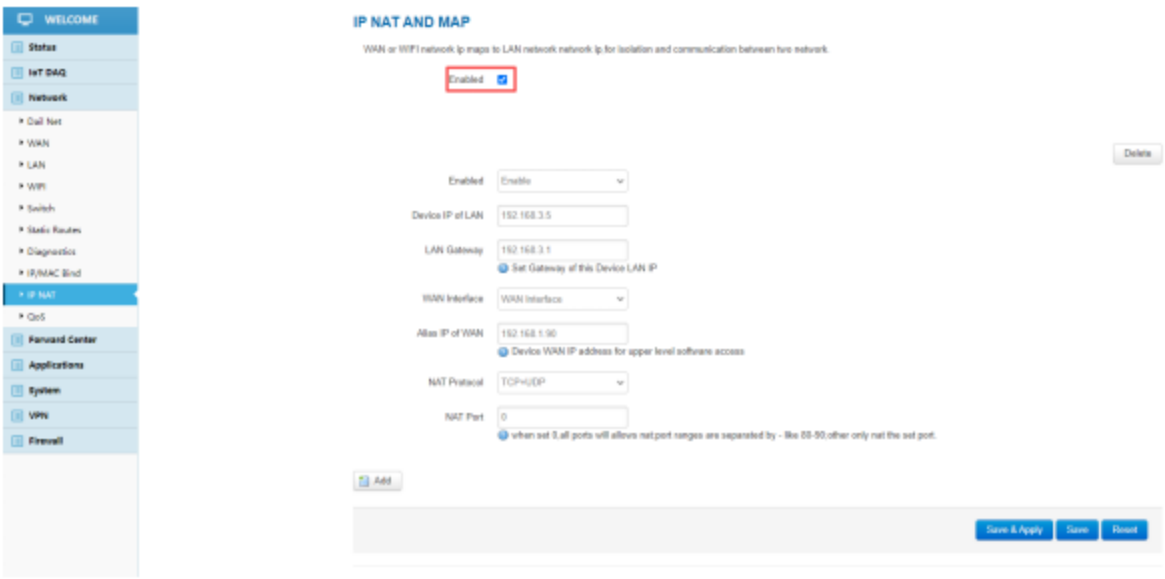


Advanced Rules

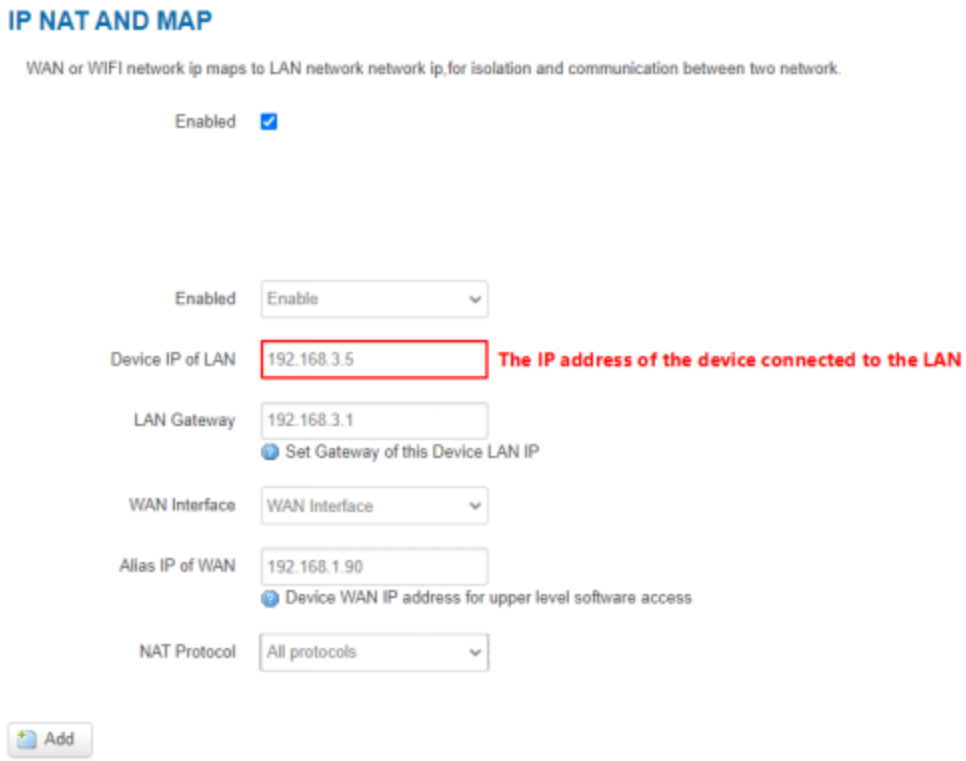
Advanced applications mainly provide more refined and flexible firewall control. There are several commonly used advanced rules by default, and these advanced rules should not be deleted.

3.4. IP Isolation and Conversion

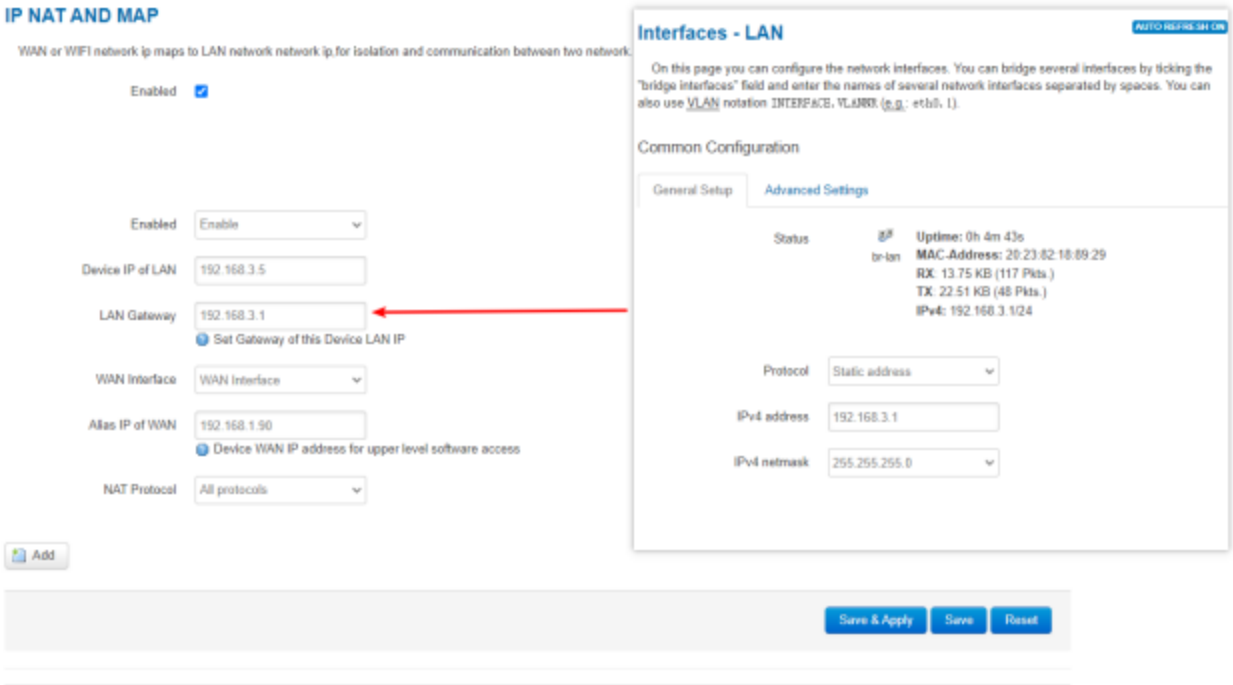
Here is an example: A PLC (IP: 192.168.3.5) is connected to the NAT Coupler LAN port (IP: 192.168.3.1), and the PLC's IP is mapped to the NAT Coupler WAN port (IP: 192.168.1.90). The upper computer (IP: 192.168.1.8) can access the PLC connected to the NAT Coupler LAN port through the NAT Coupler WAN port.



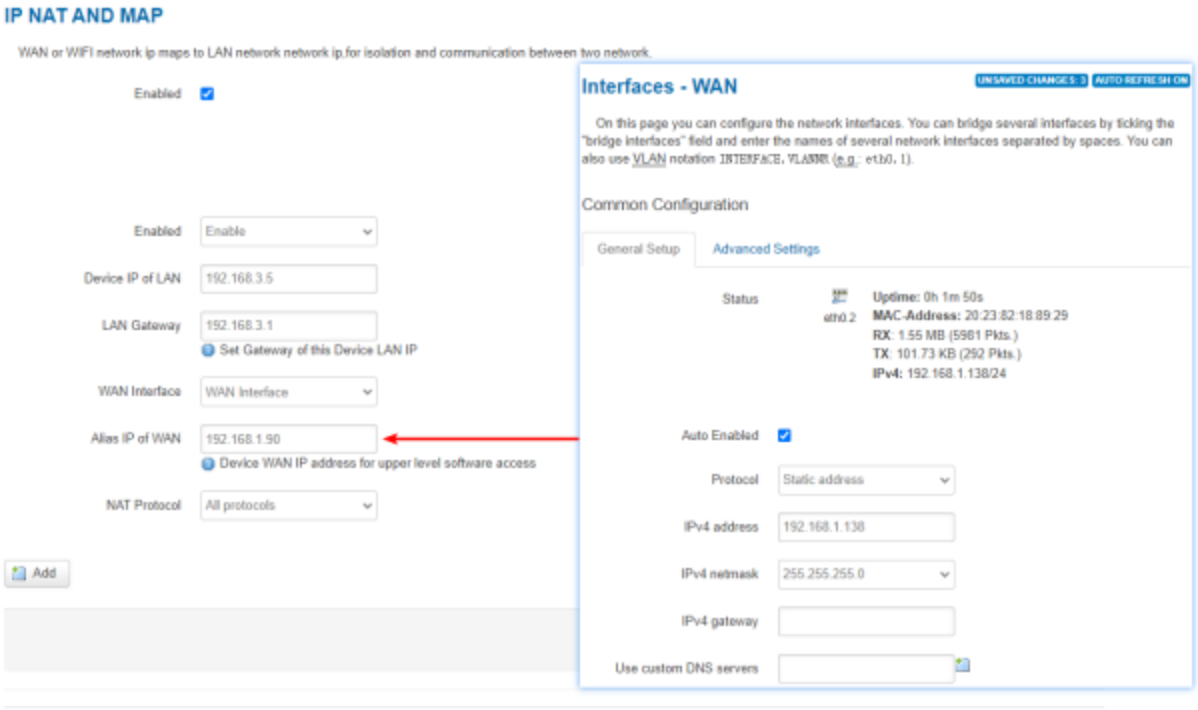
Fill in the IP address of the device connected to the NAT Coupler LAN port (do not be the same as the NAT Coupler LAN port IP)



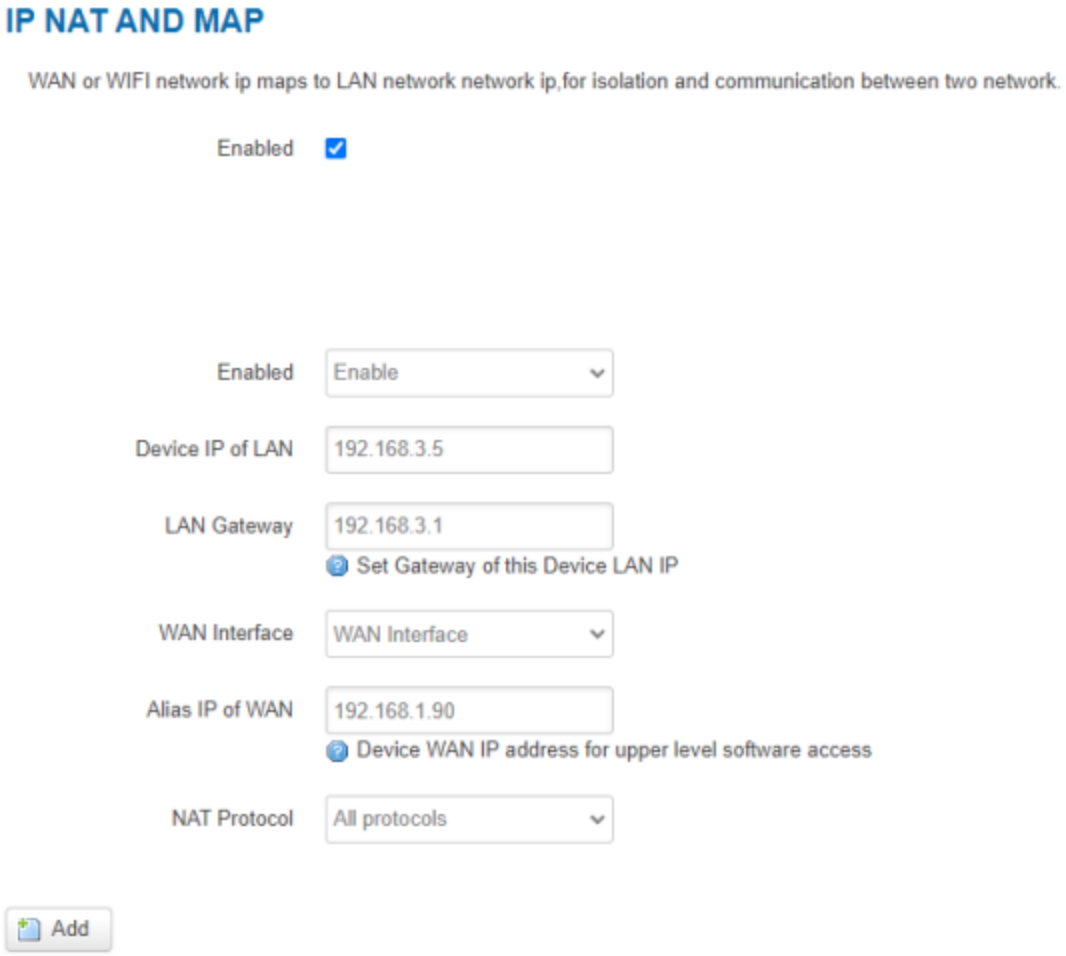
Fill in the NAT Coupler LAN IP



Fill in the mapped IP address after isolation and conversion of the connected device (must be in the same network segment as the WAN port, but not the same as the WAN port IP)



The default NAT protocol is "All protocols", then save and apply.



Note: Click the "Add" button below to add multiple configurations.

After completion, the upper computer can communicate with the PLC connected to the NAT Coupler LAN port by accessing the NAT Coupler WAN port IP.

Option Description

Option	Description
Enable	Whether to enable the function
Device IP (LAN)	The IP address of the device (e.g., PLC) connected to the NAT Coupler LAN port
LAN Gateway	The LAN port IP address of the NAT Coupler
WAN Network Interface	The mapped interface
Alias IP (WAN)	The IP address obtained after isolation and conversion for the subordinate device (cannot be the same as the NAT Coupler WAN external network configuration)
NAT Port	0: All ports are allowed Example 80: Only port 80 is opened Example 0-99: Ports 0~99 are opened
NAT Protocol	ALL protocols: All protocols are allowed to pass TCP+UDP: Only TCP and UDP protocols are allowed to pass TCP: Only TCP protocol is allowed to pass UDP: Only UDP protocol is allowed to pass ICMP: The upper computer can detect whether the subordinate device is online by pinging the corresponding isolated and converted IP

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