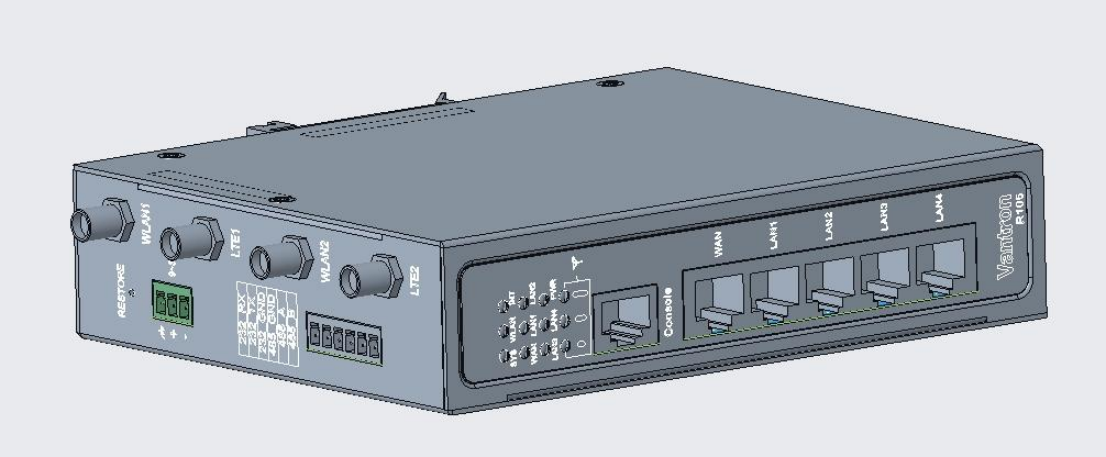
R105 Industrial Router



User Manual

Version: 1.3

© Vantron Technology, Inc. All rights reserved.

Revision History:

No.	Software Version	Description	Date
V1.0	V200R003	First release	Jun. 2, 2023
V1.1	V200R003	1. Deleted Firewall zone related description as per design change; 2. Added blacklist and whitelist description to the Firewall section.	Apr. 4, 2023
V1.2	V200R003	1. Modified Overview menu description; 2. Deleted Quick Start for networking; 3. Modified Auto routing description; 4. Updated 4G/LTE description; 5. Added Diagnostic description; 6. Added IPSec setup description.	Jul. 11, 2023
V1.3	V200R003	1. Updated Product appearance diagram; 2. Updated Ethernet port status indicator description;	Dec. 5, 2023

Table of Contents

Foreword 1
CHAPTER 1 HARDWARE DESCRIPTION 5
1.1 Product Overview 6
1.2 Unpackaging 7
1.3 Specifications 8
1.4 Definition of Interfaces 9
1.4.1 Front view 9
1.4.2 Left side view 11
1.4.3 Right side view 12
1.4.4 Back view 12
1.5 Serial Port Description 13
CHAPTER 2 GETTING STARTED 14
2.1 Setting up the Router 15
2.2 Router Login 19
2.3 Password Change 20
2.4 Language Change 20
2.5 Interfacing with Vantron Gateway Management Platform 21
CHAPTER 3 ROUTER SETUP VIA VANTRONOS 22
3.1 Introduction to VantronOS 23
3.2 Status 24
3.3 Quick Start— Auto Routing 26
3.4 Virtual Tunnel 29
3.4.1 OpenVPN Server 29
3.4.2 VPN Client 31
3.5 IPSec Connection 32
3.5.1 Prerequisites 32
3.5.2 Certificate Setup 34
3.5.3 Secret Setup 36
3.5.4 IPSec Connection Setup 38
3.6 Network 61
3.6.1 Interfaces 61
LAN 62
WAN 65
3.6.2 Wireless (WIFI) 69
Wi-Fi – AP Mode (General settings) 69
Wi-Fi – AP Mode (Advanced setting) 70
Wi-Fi – Client Mode 71
Wi-Fi – AP + Client Mode 72
3.6.3 4G/LTE 73
3.6.4 Static Routes 76
3.6.5 Firewall 78
3.7 Diagnostics 83
3.8 VTShark 83

3.9 User Management 86
3.10 Customization 87
3.10.1 Custom Program 87
3.10.2 IPK Installer 88
3.10.3 Manufacturer Info Customization 89
3.10.4 DMP Agent 90
3.11 Hardware 91
3.11.1 Ser2TCP 91
3.11.2 Ser2net Environment Setup and Verification 91
3.11.3 Protocol comparison 97
3.12 Services 98
3.12.1 Dynamic DNS 98
3.12.2 RC to PLC 98
3.13 System 100
3.13.1 System 100
3.13.2 Netlink Bandwidth Monitor (NBM) Setting 102
3.13.3 Administration 104
SSH Access 104
3.13.4 Terminal 106
3.13.5 Mount Points 107
3.13.6 Backup/Flash Firmware 109
3.13.7 Reboot 112
3.14 Logout 112
CHAPTER 4 DISPOSAL AND PRODUCT WARRANTY 113
4.1 Disposal 114
4.2 Warranty 115
Appendix Regulatory Compliance Statement 116

Foreword

Thank you for purchasing R105 Industrial Router ("the Router" or "the Product"). This manual intends to provide guidance and assistance necessary on setting up, operating or maintaining the Product. Please read this manual and make sure you understand the structure and functionality of the Product before putting it into use.

Intended Users

This manual is intended for:

- Network architects
- Network administrators
- Technical support engineers
- Other users

Copyright

Vantron Technology, Inc. ("Vantron") reserves all rights of this manual, including the right to change the content, form, product features, and specifications contained herein at any time without prior notice. An up-to-date version of this manual is available at www.vantrontech.com.

The trademarks in this manual, registered or not, are properties of their respective owners. Under no circumstances shall any part of this user manual be copied, reproduced, translated, or sold. This manual is not intended to be altered or used for other purposes unless otherwise permitted in writing by Vantron. Vantron reserves the right of all publicly released copies of this manual.

Disclaimer

While all information contained herein has been carefully checked to assure its accuracy in technical details and typography, Vantron does not assume any responsibility resulting from any error or features of this manual, nor from improper uses of this manual or the software.

It is our practice to change part numbers when published ratings or features are changed, or when significant construction changes are made. However, some specifications of the Product may be changed without notice.

Technical Support and Assistance

Should you have any question about the Product that is not covered in this manual, contact your sales representative for solution. Please contain the following information in your question:

- Product name and PO number;
- Complete description of the problem;
- Error message you received, if any.

Vantron Technology, Inc.

Address: 48434 Milmont Drive, Fremont, CA 94538

Tel: (650) 422-3128

Email: sales@vantrontech.com

Regulatory Information

The Product is designed to comply with:

- Part 15 of the FCC Rules
- IC
- PTCRB

Please refer to **Appendix** for Regulatory Compliance Statement.

Symbology

This manual uses the following signs to prompt users to pay special attention to relevant information.

	Caution for latent damage to system or harm to personnel
	Attention to important information or regulations

General Safety Instructions

The Product is supposed be installed by knowledgeable, skilled persons familiar with local and/or international electrical codes and regulations. For your safety and prevention of damage to the Product and other equipment connected to it, please read and observe carefully the following safety instructions prior to installation and operation. Keep this manual well for future reference.

- Do not disassemble or otherwise modify the Product. Such action may cause heat generation, ignition, electronic shock, or other damages including human injury, and may void your warranty.
- Keep the Product away from heat source, such as heater, heat dissipater, or engine casing.
- Do not insert foreign materials into any opening of the Product as it may cause the Product to malfunction or burn out.
- To ensure proper functioning and prevent overheating of the Product, do not cover or block the ventilation holes of the Product.
- Follow the installation instructions with the installation tools provided or recommended.
- The use or placement of the operation tools shall comply with the code of practice of such tools to avoid short circuit of the Product.
- Cut off the power before inspection of the Product to avoid human injury or product damage.

Precautions for Power Cables and Accessories

⚠ Use proper power source only. Make sure the supply voltage falls within the specified range. Always check whether the Product is DC powered before applying power.

⚠ Place the power cable properly at places without extrusion hazards.

⚠ Use only approved antenna(s). Non-approved antenna(s) may produce spurious or excessive RF transmitting power which may violate FCC limits.

⚠ Cleaning instructions:

- Power off before cleaning the Product
- Do not use caustic or aggressive liquids, vapor, or spray
- Clean with a damp cloth
- Do not try to clean exposed electronic components unless with a dust collector

⚠ Power off and contact Vantron technical support engineer in case of the following faults:

- The Product is damaged
- The temperature is excessively high
- Fault is still not solved after troubleshooting according to this manual

⚠ Do not use in combustible and explosive environment:

- Keep away from combustible and explosive environment
- Keep away from all energized circuits
- Unauthorized removal of the enclosure from the device is not allowed
- Do not change components unless the power cable is unplugged
- In some cases, the device may still have residual voltage even if the power cable is unplugged. Therefore, it is a must to remove and fully discharge the device before replacement of the components.

CHAPTER 1 HARDWARE DESCRIPTION

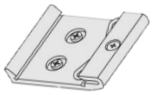
1.1 Product Overview

Vantron R105 industrial router offers different options for industrial IoT connectivity, including cellular, Wi-Fi, Ethernet, and virtual private network (VPN) to meet diversified networking requirements. It offers mid- and high-speed CAT 4 cellular networks with major carriers supported. It implements 5 gigabit Ethernet jacks. With Wi-Fi IEEE 802.11 b/g/n/ac supported, R105 offers IEEE 802.11ax (Wi-Fi 6) as an option to customers to meet higher communication needs.

R105 industrial router supports multi-channel failover to maintain secure and stable network access. With BlueSphere GWM, a web-based cloud platform for centralized management of mass routers and gateways, you can further configure and manage the router remotely. R105 is very suitable for application in industrial automation, smart home, smart city, etc.

1.2 Unpackaging

The Product has been carefully packed with special attention to quality. However, should you find any component damaged or missing, please contact your sales executive in due time.

Standard accessories		Optional accessories	
	1 x R105 router		1 x 12V DC Power adapter & power cord
	2 x 4G LTE antenna (magnetic stick)		1 x DC power connector
	2 x Wi-Fi antenna (rubber stick)		2 x 4G LTE antenna (rubber sucker)
	1 x DIN rail mounting bracket (attached)	/	/

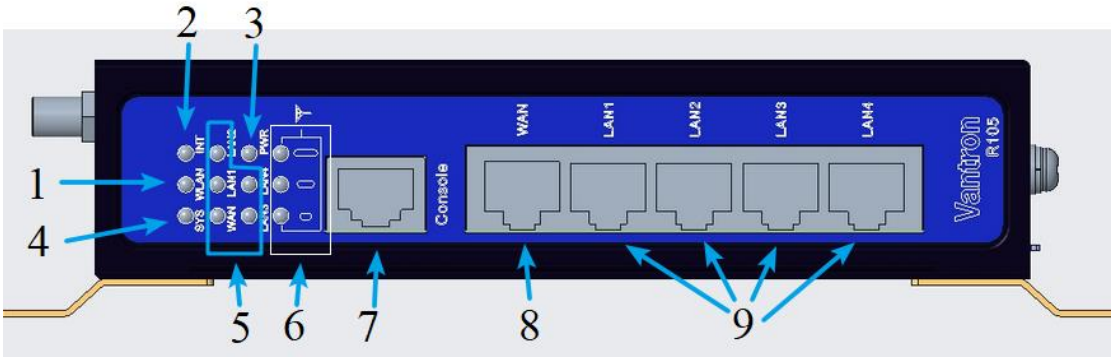
Actual accessories might vary slightly from the list above as the customer order might be different from the standard configuration options.

1.3 Specifications

R105			
Communication	Ethernet	5 x RJ45, 10/100/1000Mbps (1 x WAN & 4 x LAN)	
	Wi-Fi	2.4GHz & 5GHz, IEEE 802.11 b/g/n/ac, AP & Client Optional: Wi-Fi 6, IEEE 802.11 b/g/n/ac/ax	
	4G LTE	LTE CAT 4, multi-carrier supported	
	WAN protocol	PPP, DHCP	
I/Os	Console	1 x Console for local configuration	
	Serial port	1 x RS485, isolated 1 x RS232, isolated	
	SIM slot	2 x SIM slot	
	Antenna (SMA conn.)	2 x LTE antenna	2 x Wi-Fi antenna
	Grounding	Enclosure & PCB	
	Power in	1 x 3.81mm Phoenix terminal block	
System Control	LED indicator	3 x Cellular signal strength indicator 1 x Power indicator 1 x System indicator	1 x Internet indicator 1 x WLAN indicator 1xWAN indicator 4xLAN indicator
	Button	1 x Pinhole reset button	
Mechanical	Dimensions	150mm x 115mm x 35mm	
	Enclosure	Metal	
	Installation	DIN rail mounting, panel mounting, wall mounting	
	IP rating	IP30	
	Drop test	6 ft. drop test	
	Cooling mode	Fanless	
Power	Input	9-36V DC, over-current protection, reverse polarity protection	
Software	OS	VantronOS	
	Network management	SNMP v2c/v3	
	Networking protocol	IPV4, HTTPS, TCP & UPD, NTP client and server, ARP, TLS	
	VLAN	Supported	
	Device management platform	BlueSphere GWM	
	Link detection	Heartbeat detection, automatic re-connection	
	Device log	Retrievable	
	Network reliability	Multi-channel failover, backup between Ethernet, Wi-Fi, 4G LTE	
	Dual SIM	Dual SIM failover, automatic switch	
	IP application	Ping, Traceroute, DHCP Server/Client, DDNS	
	IP Routing	Static routing, dynamic routing	
	NAT	Supported	
Security	Firewall	Supported (Stateful)	
	Access control	MAC address, IP address	
	Data security	PPTP, L2TP, GRE, IPSec, OpenVPN	
	Wi-Fi security	64/128-bit WEP, TKIP, WPA, WPA2, WPA3, AES, WPS	
Environment Condition	Temperature	Operating: -20℃~+60℃	Storage: -40℃~+70℃
	Humidity	Storage: RH 5%~95% (non-condensing)	
	Certification	FCC, IC, PTCRB, AT & T, Verizon, T-Mobile	

1.4 Definition of Interfaces

1.4.1 Front view



Indicator/Interface	Description
1	Wi-Fi status indicator
2	Network connectivity indicator
3	Power indicator
4	System status indicator
5	Ethernet port status indicator
6	4G LTE signal strength indicator
7	Console port for debugging the device (baud rate: 57600)
8	WAN port, mapped as **eth0.2** in VantronOS, working in the WAN area by default
9	4 x LAN port, mapped as **eth0.1** in VanrteonOS, working in the LAN area by default

Description of the LED indicators

1. Wi-Fi status indicator

Wi-Fi status	Description
The Wi-Fi module is turned on	The indicator turns solid green
There is Wi-Fi connectivity	The indicator blinks
The Wi-Fi module is turned off	The indicator is off

2. Network connectivity indicator

Network connectivity of the Router	Description
There is no internet access through any of the available connectivity routes	The indicator is off
The router has internet access from any of the routes	The indicator blinks at an interval of 1 second

3. Power indicator

   When the Router is powered on, the power indicator will turn solid green.

4. System status indicator

System action	Description
System bootup in process	The indicator is off
System running properly	The indicator blinks at an interval of 1 second
System reboot, upgrade or factory reset	The indicator blinks quickly at an interval of 0.3 seconds

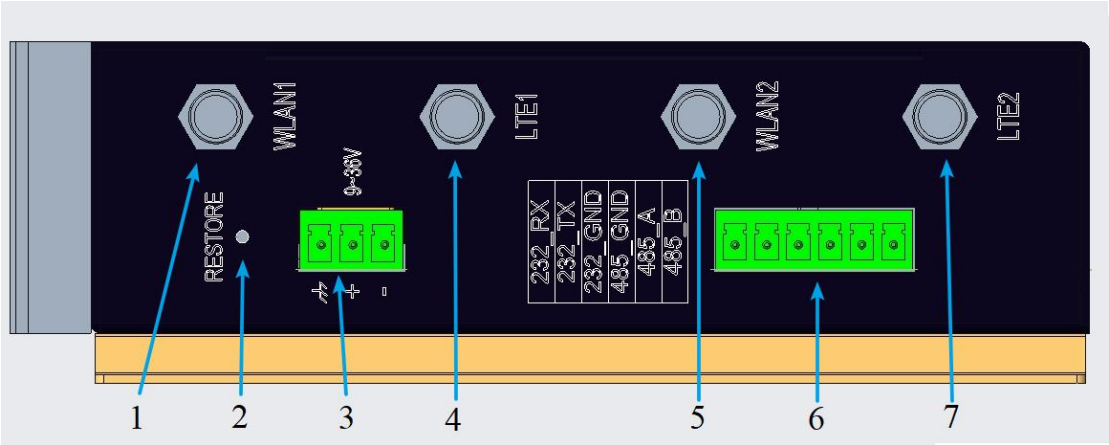
5. 4G LTE signal strength indicator

Signal strength	Description
>67%	The three indicators turn solid green
Between 38% and 67%	The bottom two indicators turn solid green
<38%	The bottom indicator blinks

6. Ethernet port status indicator

When these Ethernet ports are successfully connected, the LED corresponding to the interface will turn solid green, and the indicator blinks when date is transmitted.

1.4.2 Left side view

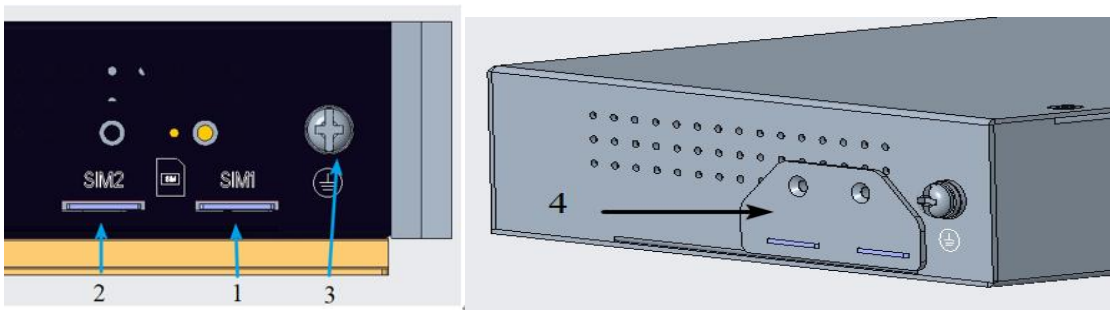


Interface	Description
1	Wi-Fi antenna connector 1
2	Pinhole RESET button
3	Power terminal (9V-36V DC)
4	Primary 4G LTE antenna connector
5	Secondary 4G LTE antenna connector
6	RS232 & RS485 serial connectors
7	Wi-Fi antenna connector 2

Description of the RESET button

1. A short press of the button for 0 ~ 2 seconds will restart the Router.
2. A long press of the button for 3 ~ 6 seconds will factory reset the Router.
3. A long press of the button for 6 ~ 10 seconds will factory reset the Router with all user data cleared.

1.4.3 Right side view

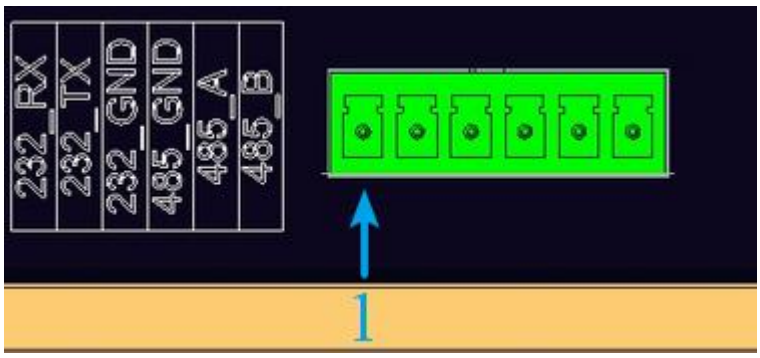


Interface	Description
1	Micro SIM slot 1
2	Micro SIM slot 2
3	Grounding screw
4	SIM slot baffle

1.4.4 Back view

Interface	Description
1	DIN rail bracket

1.5 Serial Port Description



The terminal block incorporates an RS232 port and an RS485 port with pinout description as follows:

No.	Signal	Device name	Port	Type	Description
1	RX	/dev/ttyS1	COM1	I	RS232 receive signal
2	TX			O	RS232 transmit signal
3	232. GND			NC	RS232 isolated ground
4	485. GND	/dev/ttyS2	COM2	NC	RS485 isolated ground
5	A			I/O	RS485 A signal
6	B			I/O	RS485 B signal

For RS232 port connection: RX-TX, TX-RX, GND-GND

For RS485 port connection: A-A, B-B, GND-GND

Input the following command to open the serial port with a serial port communication program (e.g., microcom):

COM1:

```
~# microcom /dev/ttyS1 -s 115200
```

COM2:

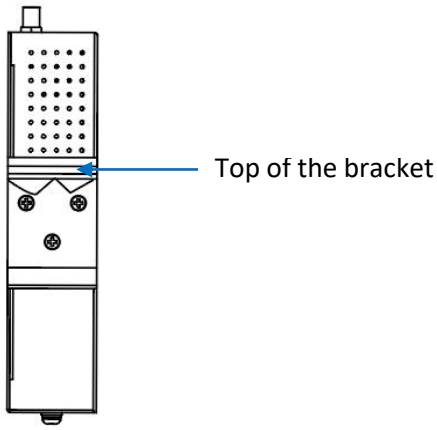
```
~# microcom /dev/ttyS2 -s 115200
```

CHAPTER 2 GETTING STARTED

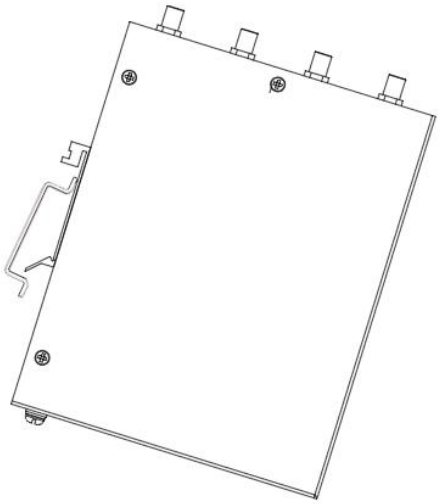
2.1 Setting up the Router

Before you proceed with configuration of the Router, follow the steps below to finish hardware connection.

1. Hold the Router uprightly;

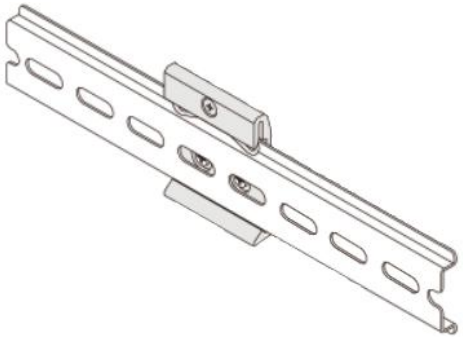


2. Place the Router on the DIN rail at an angle;
3. Fit one side of the DIN rail to the clip at the top of the DIN rail bracket, behind the triangle fixer;

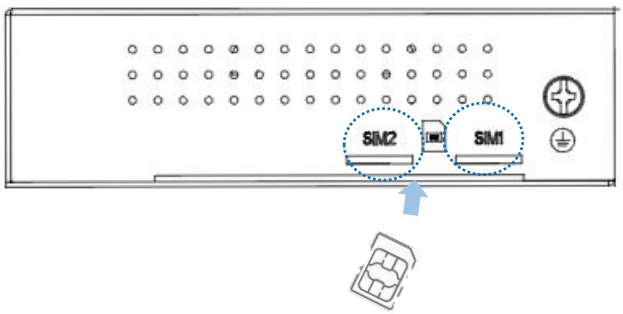


4. Push the Router down to compress the bracket;

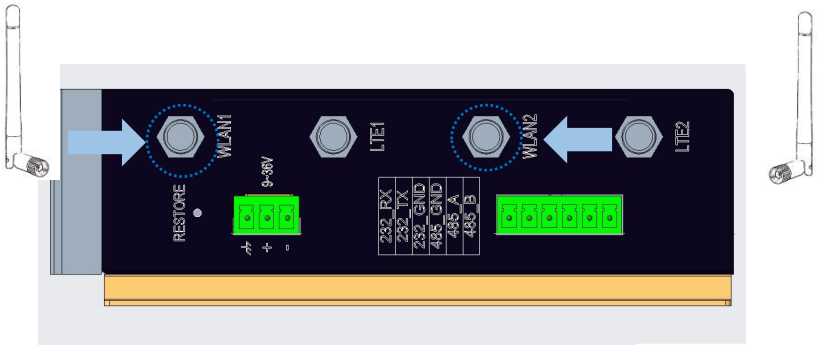
5. Release the Router when there is enough space for the other side of the DIN rail to fit in the downside of the DIN rail bracket;



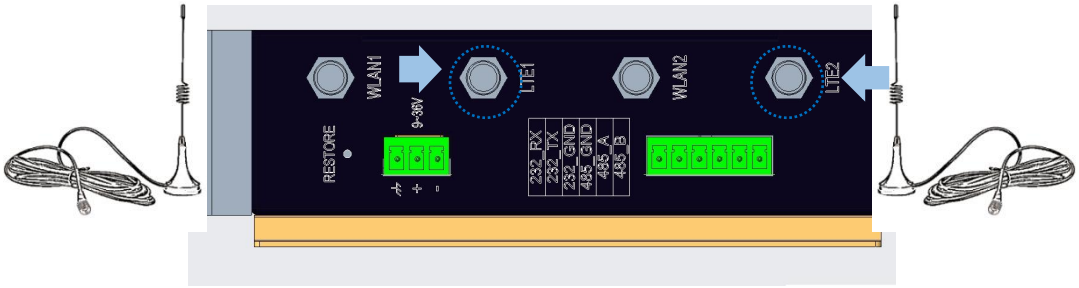
6. Gently swing the Router to make sure the it is fastened on the DIN rail;
7. Insert an activated Micro SIM card into either of the SIM slots with the gold-colored contacts facing up and the clipped side inward;



8. Push the Micro SIM card in to secure it;
9. Install the Wi-Fi antennas (rubber stick) to the WLAN antenna connectors;

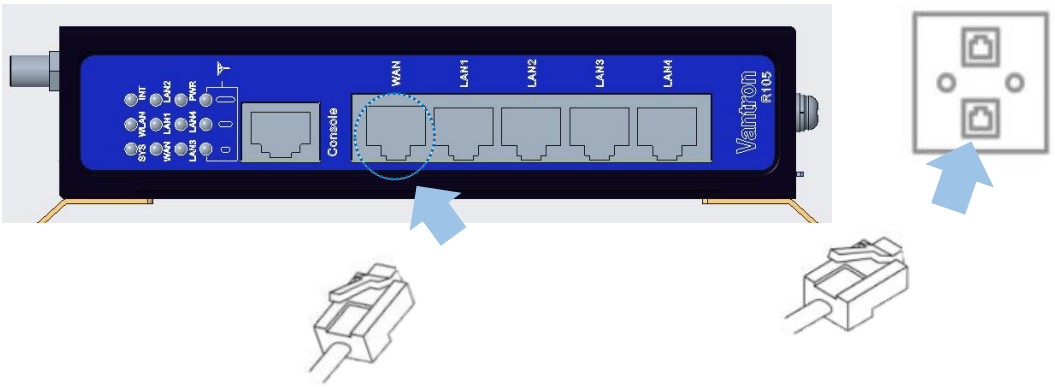


10. Install the LTE antennas (rubber stick /magnetic sucker) to the LTE antenna connectors (if only one antenna is shipped, install to the LTE 1 connector);

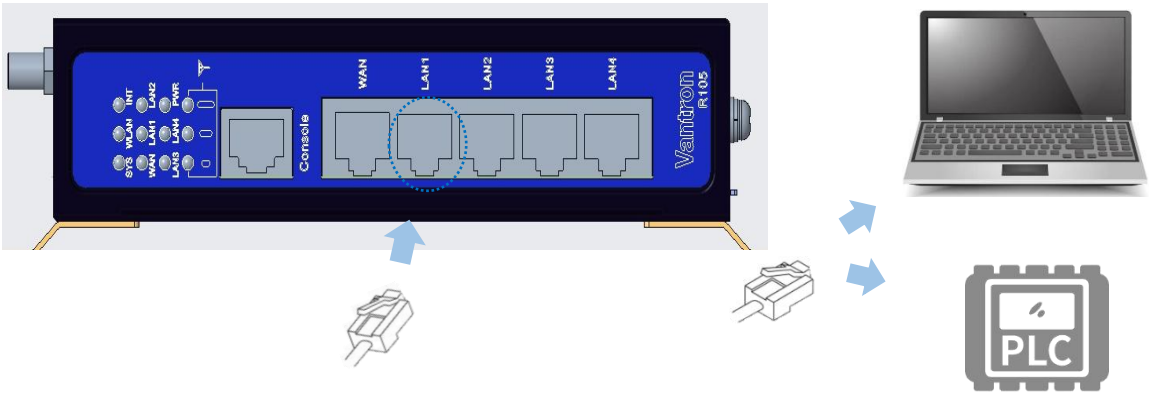


11. Tighten the rotating heads to secure the antennas in proper position;

12. Connect one end of an Ethernet cable to the WAN port of the Router and the other to a live Ethernet port;

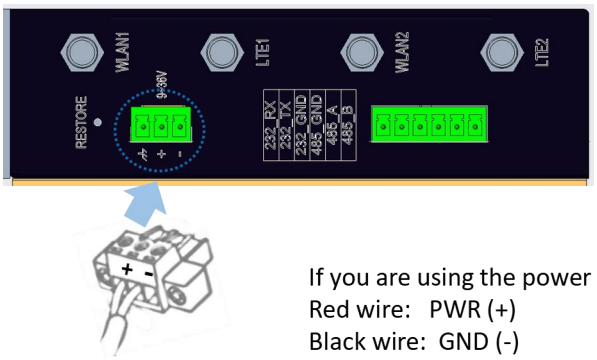


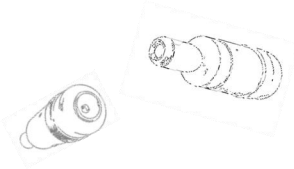
13. Connect one end of another Ethernet cable to a LAN port of the Router and the other to a host computer or client device depending on your use;



Skip the Ethernet connection steps if you choose wireless network connection.

14. Connect the terminal end of the DC power connector to the power terminal of the Router and the round end to the adapter;





If you are using the power connector supplied by Vantron:
Red wire: PWR (+)
Black wire: GND (-)

15. Plug the adapter to a DC power outlet that meets the supply voltage requirement (9V to 36V) to turn on the Router;

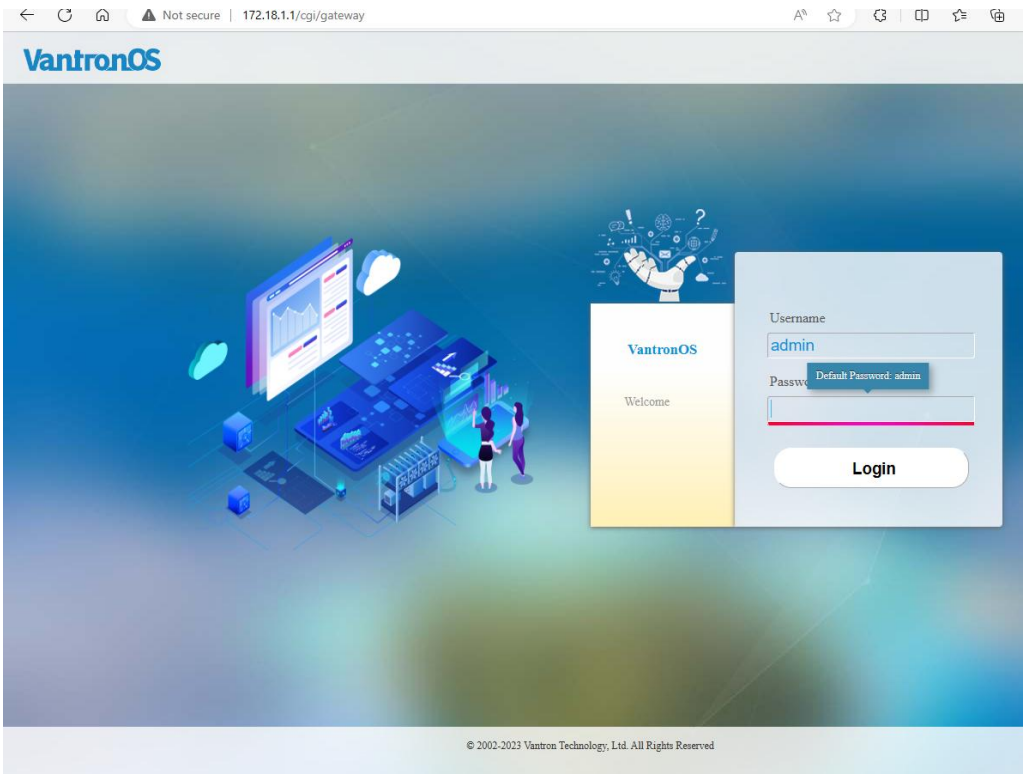
16. The power indicator will turn solid green upon power application.

The antennas might be different from what used for illustration here. Should you have any trouble installing the antennas, please contact the sales executive for solution.

2.2 Router Login

The Router is designed to allow network connectivity with minimal configuration. That being said, you can configure the network settings and customize the Router from VantronOS interface.

1. Input the LAN port IP address of the Router in your browser to log in the VantronOS web interface (default: http://172.18.1.1/).
   - Default user: **admin** / Super user: **root**
   - Default password: **admin** / Super user password: **rootpassword**



2. For SSH login, use the LAN port IP address (default: http://172.18.1.1/).
   - Port: **22**
   - Account: **root**
   - Password: **rootpassword**

The web login address coincides with the LAN port IP address of the Router, so you might have to change the login address when you reset the IP address.

*SSH login is disabled by default, refer to **SSH Access** included in 3.13.3 for more details.*

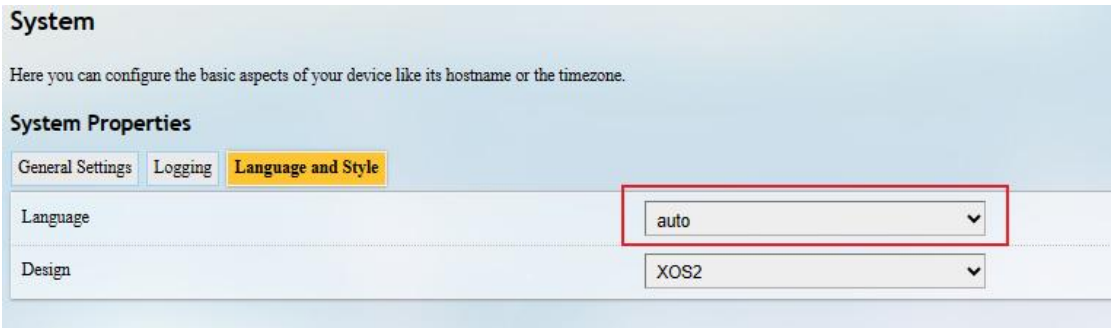
2.3 Password Change

It is up to you to decide whether you would like to change the login password after logging in VantronOS.

1. Navigate to **System > Administration**;
2. Input the original password for the current user;
3. Input a new password and confirm the password;
4. Save the settings and apply;
5. The system will log out automatically;
6. Log in with the new password.

2.4 Language Change

Currently the system supports simplified Chinese and English. The system language is set to automatically follow your browser language by default. You can change the system language by navigating to **System > System > Language and Style**.



Auto: System language based on the browser language (default)

English: English interface

Simplified Chinese: Simplified Chinese interface

2.5 Interfacing with Vantron Gateway Management Platform

BlueSphere Gateway Management Platform ("GWM") is a cloud-based management portal that empowers organizations to seamlessly provision, monitor, and manage Vantron IoT communication devices, including gateways, routers, and DTUs. By leveraging BlueSphere GWM, organizations can streamline device setup, ensure real-time visibility into device performance, and effortlessly control device configurations. This contributes to enhanced operational efficiency and improved decision-making.

Before you can use the BlueSphere GWM for remote management of Vantron IoT devices, please make sure the following prerequisites are met:

- You have obtained a license for login to the BlueSphere GWM
- The DMP agent is installed on the device for remote management
- The DMP agent is “enabled” (Refer to 3.10.4 DMP Agent for the configuration)
- The serial number of the device is added to the BlueSphere GWM

CHAPTER 3 ROUTER SETUP VIA VANTRONOS

3.1 Introduction to VantronOS

VantronOS is an intelligent operating system developed by the Vantron team, featuring independent system and function development. It is built upon the Linux system and optimized for embedded hardware. The operating system follows a modular design and plug-in expansion approach, utilizing the Linux kernel with a built-in firewall to ensure secure internet connectivity for Vantron IoT communication devices, protecting them from potential attacks.

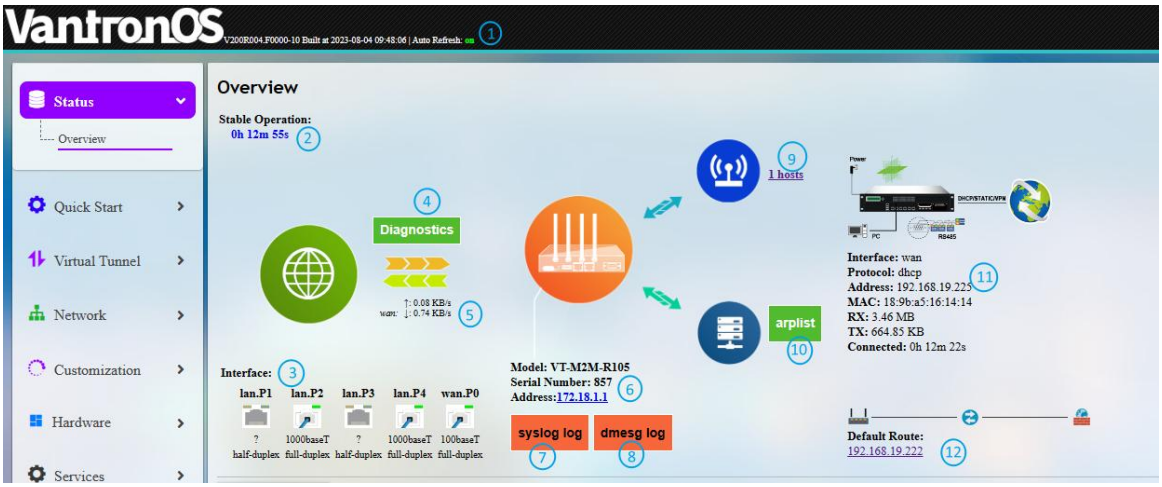
VantronOS incorporates a user-friendly UI interface based on the MVC framework, providing a simple and efficient setting entry for users. Additionally, it offers seamless interfacing with various cloud management platforms, including the self-developed BlueSphere GWM, as well as popular platforms like Azure, Alibaba Cloud, Huawei Cloud, and RootCloud. This enables users to remotely monitor, operate, and diagnose devices without the need for on-site technical support engineers. VantronOS facilitates the interconnection and interaction between users and the Industrial Internet of Things, enhancing the overall efficiency and convenience of device management.

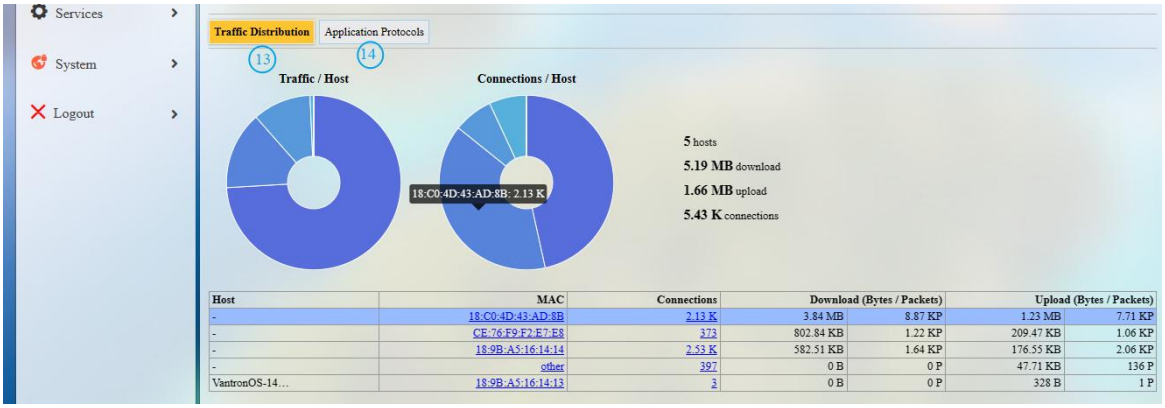
In the following sections, should you find any features not displayed in the VantronOS interface as an 'admin' user, please log in with the root account.

Make sure to save all settings and changes before exit to let them take effect.

3.2 Status

This page provides the overall information of the Router, including stable operation duration, number of devices connected to the Router via wireless or Ethernet connection, default routing, hardware information, traffic statistics, etc.





Description of the numbered areas

1. Firmware version and auto refresh on/off (click to switch the mode)
2. Stable running duration of the Router since network connection
3. Current working status of the Ethernet ports

   (LAN2, LAN4, and the WAN port are connected in this case)

4. A collection of the network diagnostic tools (refer to 3.7 for details)
5. Instant outbound traffic
6. The model, serial number, and management address of the router in use
7. System log information
8. Kernel log information
9. Number of clients connected to the Router via Wi-Fi

You will access Wi-Fi settings upon a click of the number.

10. Address information of clients connected to the Router via Ethernet

IPv4-Address	MAC-Address
172.18.1.224	16:0b:0e:4c:99:ac
172.18.1.126	ce:76:f9:f2:e7:e8

11. Details of the router connectivity

The illustrative image varies with the communication module on the Router.

12. Default route currently used by the Router
13. Traffic distribution of clients connected to the Router displayed by MAC addresses

Clicking on each MAC address in the table at the page bottom will get the detailed traffic information of the clients.

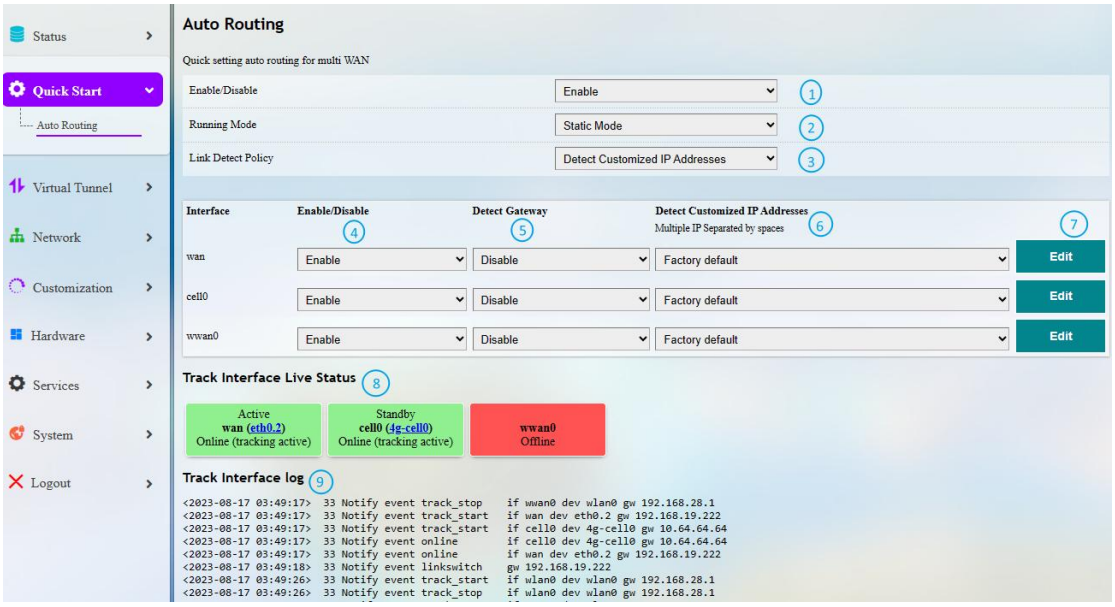
14. Traffic of application layer protocols

HTTPS, HTTP, and QUIC represent the top 3 protocols for data download and upload. HTTPS, HTTP and DNS represent the top 3 protocols for device connection.

3.3 Quick Start— Auto Routing

Automatic routing ensures that the Router maintains Internet access when multiple links are available. It features automatic link detection, automatic route switching, and recovery.

The default link detection and data forwarding are prioritized based on the following rule: Ethernet > Wi-Fi > LTE > others.



Description of the numbered areas

1. Enable/Disable route tracking
2. Mode of the automatic routing (refer to the details below)
3. Automatic link detection policy (refer to the details below)
4. Enable/Disable link detection for a specific network interface

   In the screenshot above, wan stands for Ethernet connection, cell0 for cellular connection, and wwan0 for Wi-Fi connection.
5. Enable/Disable gateway detection
6. Customized IP address detection (heartbeat or gateway address)
7. Edit the auto routing rule of a specific network interface (refer to the details below)
8. Link status
9. Link detection log and service running log

Mode of the automatic routing

Mode	Description
Static mode (Default)	1. The user-designated link priority takes precedence; 2. If the user does not designate the link priority, the default rule will apply.
Dynamic mode	1. The default rule governs the entire routing policy; 2. The user-designated link priority will be disabled. This is not recommended when special applications are installed on the Router that rely on the designated link priority.

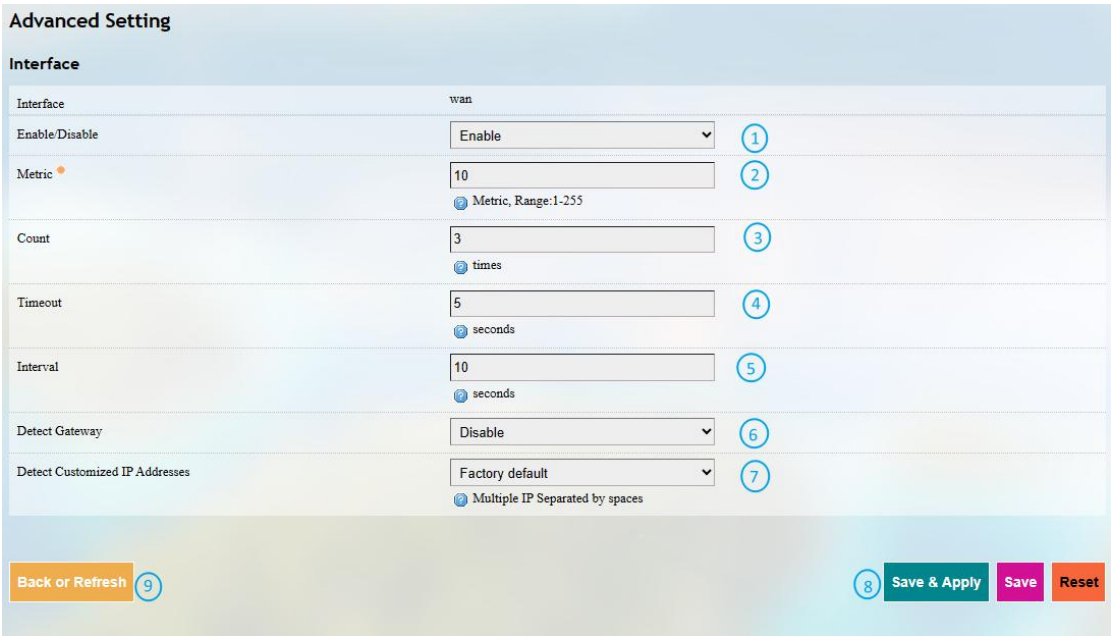
Automatic link detection policy

Policy	Description
Detect customized IP addresses (Default)	1. You can set IP addresses for a specific network interface. If these IP addresses have packets received and transmitted, the interface is active and set “Online”; 2. If the Router is located at a place without access to external network, please change the policy to “Detect gateway” or add some IP addresses that the Router can detect.
Detect gateway	This policy is to identify the IP address of the gateway on the current network. You are recommended not to apply this policy for P2P/PPP connection scenarios, in which circumstance, verifying the public network IP address (such as 8.8.8.8) is recommended.

Note:

1. Please choose an appropriate policy based on the device’s network position and the network access protocol used by the network interface.
2. If you have configured for both “Detect customized IP addresses” and “Detect gateway”, the gateway detection will take precedence.
3. If you have selected “Detect customized IP addresses” but have not provided any IP address, it will automatically switch to gateway detection.
4. Refer to the next page on editing the routing rules for more details.

Clicking on the **Edit** button behind an interface will direct you to the rule editing page as follows.



Description of the numbered areas

1. Enable/Disable the route tracking on this interface
2. Gateway metric (The smaller the number, the higher the priority)
3. The count of total messages sent in case of a detection timeout (3 by default)
4. The timeout for a single tracking (5s by default)
5. Tracking interval, defined as from the completion of one tracking to the initiation of the next tracking (10s by default)
6. Enable/disable gateway detection
7. Select the default IP addresses (‘factory default’) or customized IP addresses (‘custom’) for IP detection
8. **Save & Apply** the settings
9. Go back to the automatic routing page

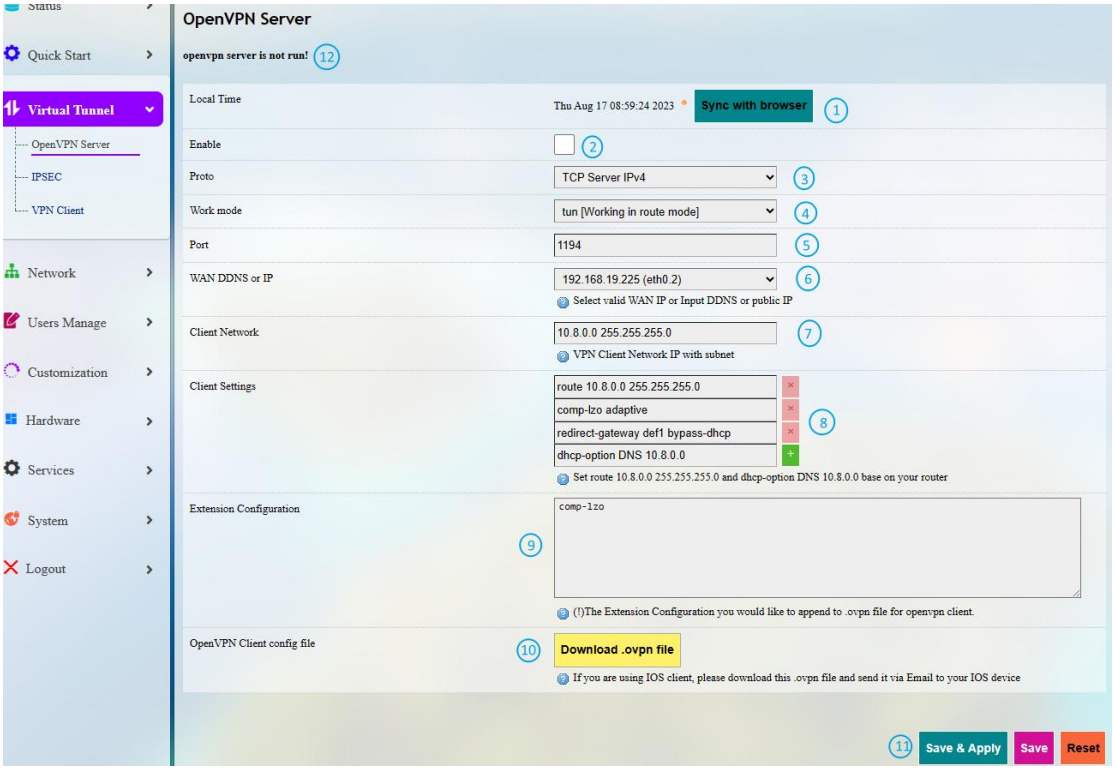
3.4 Virtual Tunnel

A virtual private network (VPN) lets you use the Internet to securely access your network remotely. The Router supports such VPN protocols as PPTP, L2TP, GRE, IPSec, and OpenVPN to ensure data confidentiality and undisturbedness.

You can configure the Router either as an OpenVPN server or an OpenVPN client based on needs.

3.4.1 OpenVPN Server

This page provides virtual private network based on SSL connection and transmission, which features simple and flexible configurations, better security, and no interference.



Follow the steps below to build an OpenVPN server:

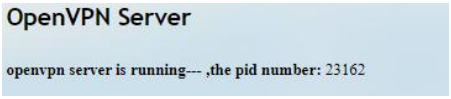
1. Synchronize the Router time with the browser (local) time;
2. Enable the server or not after the server is built;
3. Select a protocol (TCP by default);

TCP provides an ordered delivery of data from the user to server (and vice versa), whereas UDP is not dedicated to end-to-end communications, nor does it check the readiness of the receiver.

4. Select a working mode between **tap** and **tun** (tun by default);

> ***Tap*** *bridges two ethernet segments at different locations, so use* ***tap*** *if you need to connect to remote network (remote desktops, PLCs, controllers, etc.). If you only need network connection, then use* ***tun****.*

5. Set a port that the server is to monitor;
6. Choose the WAN port IP or DDNS or public IP that the server is to monitor;
7. Assign a virtual IP network for the clients;
8. The basic configurations sent to the clients (not applicable to the tap working mode);
9. The extension configurations sent to the clients;
10. Download the configuration file for client connection (not necessary for server setup);
11. **Save & Apply** the settings;
12. Status of the OpenVPN server after the setup.



Advanced Setting allows you to set the authentication method, certificate authentication options, and renew the system certificate.

Run Log displays the details after the server setup.

3.4.2 VPN Client

To connect the Router to a VPN server and use it as a client, navigate to **Virtual Tunnel > VPN Client** for specific settings.

Description of the numbered areas

1. Synchronize your VPN time with the browser (local) time
2. Select a WAN protocol for the virtual line (OPENVPN & PPTP available)
3. Click to switch to the protocol
4. Check or uncheck the box to enable/disable the protocol

Only when the protocol is enabled will subsequent options be displayed. The subsequent options correspond to the type of WAN protocol selected.

5. If you select OpenVPN as the WAN protocol, you'll have to continue with the configuration using a .ovpn file

If you select PPTP as the WAN protocol, you shall input the PPTP server IP, user name and password as indicated.

6. Select the .ovpn file from the local directory for configuration
7. Upload the file
8. Select to use a certificate or username & password for the authentication

The mode will update automatically, leave it as is.

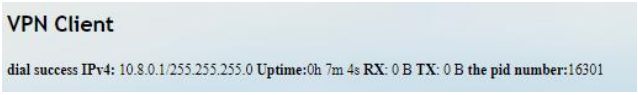
9. Set the MTU
10. Set the gateway metric (between 1 and 255)

The smaller the number, the higher the priority.

11. Disable/Enable heartbeat detection

*Select **custom** and enter the IP address for heartbeat detection to enable the mechanism.*

12. Enter a custom DNS server
13. **Save & Apply** the settings
14. Status of the VPN client after the setup



3.5 IPSec Connection

3.5.1 Prerequisites

- An R105 industrial router ('G1' for short)
- A supporting device (gateway/router) that runs on VantronOS and supports IPSec ('G2' for short)
- Certificates for the router and the supporting device:

1. Assume that the IP addresses of the G1 and G2 are as follows:

   G1— LAN IP: 172.18.2.1, WAN IP: 192.168.9.78

   G2— LAN IP: 172.18.3.1, WAN IP: 192.168.9.82

2. Assume the certificates of the two devices are as follows:

   G1—

   X509 root certificate: rootca.cert

   X509 certificate: 78.cert

   Private key: 78.priv.key

   Public key: 78.pub.key

   G2—

   X509 root certificate: rootca.cert

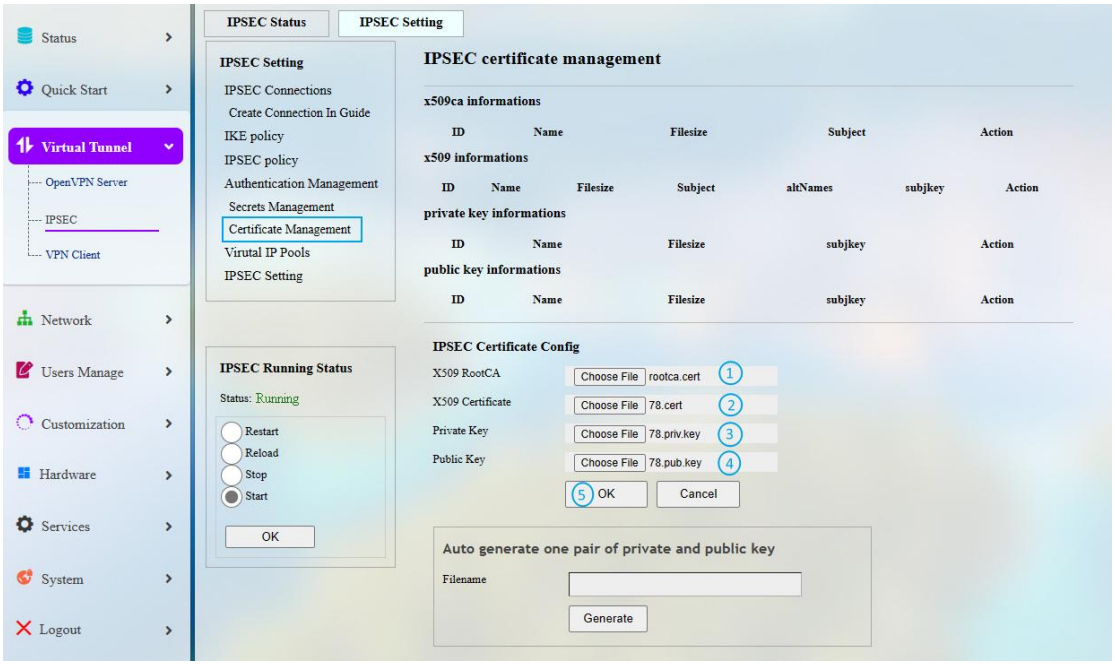
   X509 certificate: 82.cert

   Private key: 82.priv.key

Public key: 82.pub.key

3.5.2 Certificate Setup

- Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Certificate Management** to upload the certificates (take G1 as an example):

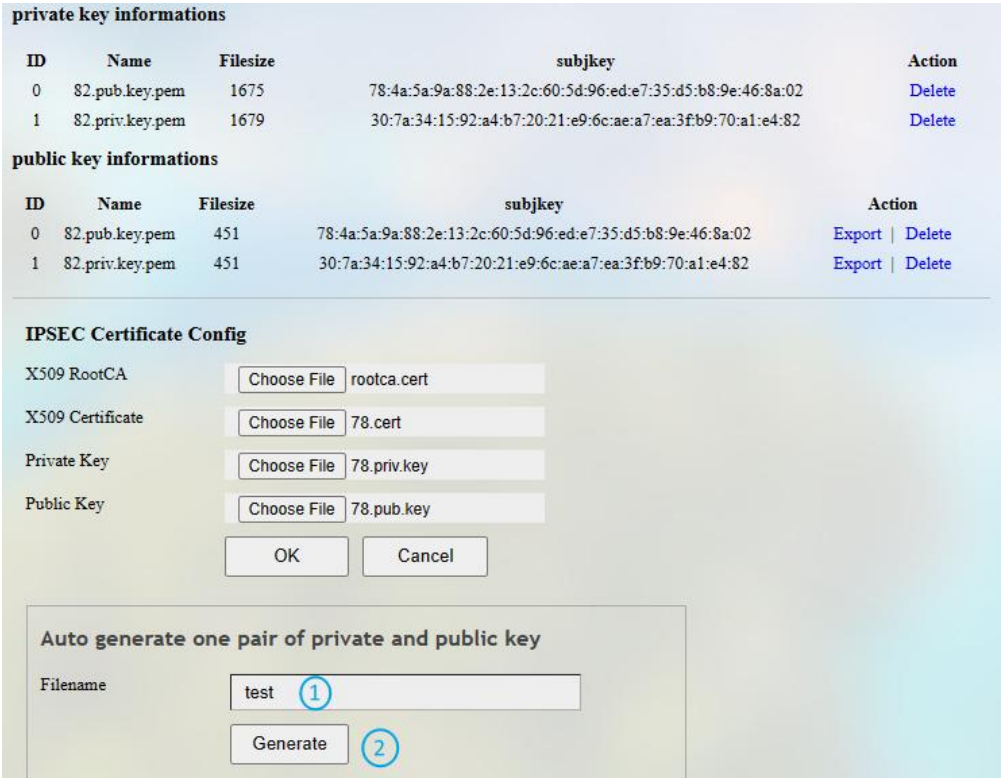


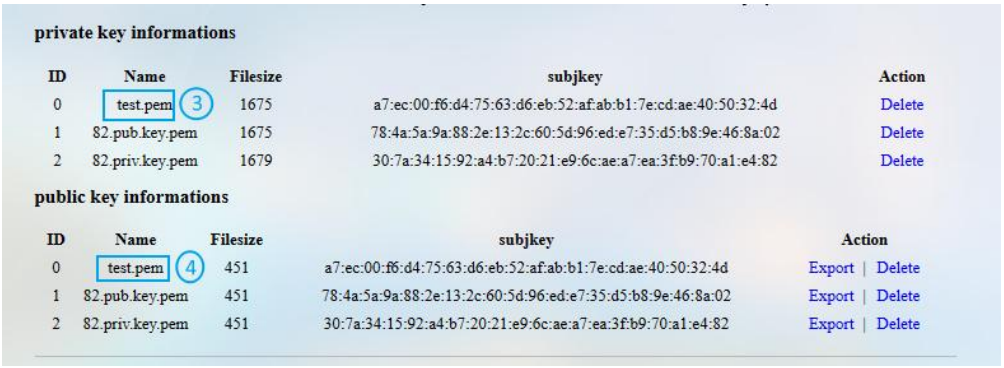
Follow the steps below to upload the certificates.

1. Select the X509 root certificate;
2. Select the X509 certificate;
3. Select the private key;
4. Select the public key;
5. Click **OK** to upload the certificates for G1.

The above screenshot only illustrates how to upload the certificates for G1. Please follow the same way to upload the certificates for G2.

You can use the tool located at the bottom of the page to generate a pair of private and public keys, which, however, can only be used as public key authentication.





Description of the numbered areas

1. Input a file name for the keys
2. Click **Generate** to generate the keys
3. Newly generated private key
4. Newly generated public key

3.5.3 Secret Setup

This configuration only applies when pre-shared key (PSK) is selected as the secret type.

- Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Secretes Management** to configure a local secret (take G1 as an example):

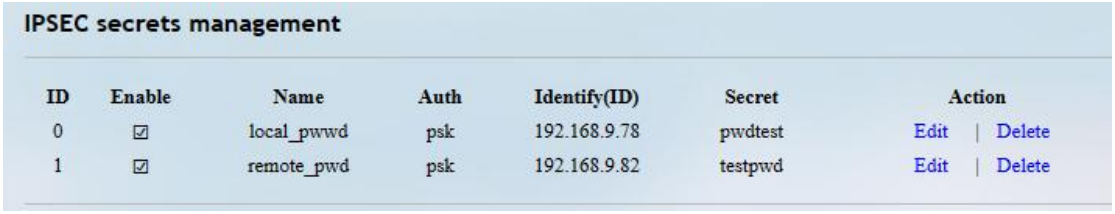
Follow the steps below to set a local secret**.**

1. Assign a name for the secrete;
2. Select **Enabled** from the dropdown list to enable the secret;
3. Select **PSK** as the secret type;
4. Input the PSK ID: 192.168.9.78 (WAN IP of G1);
5. Input a password;
6. Click **OK** to save the secret.

- Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Secretes Management** to configure a remote secret (take G1 as an example):

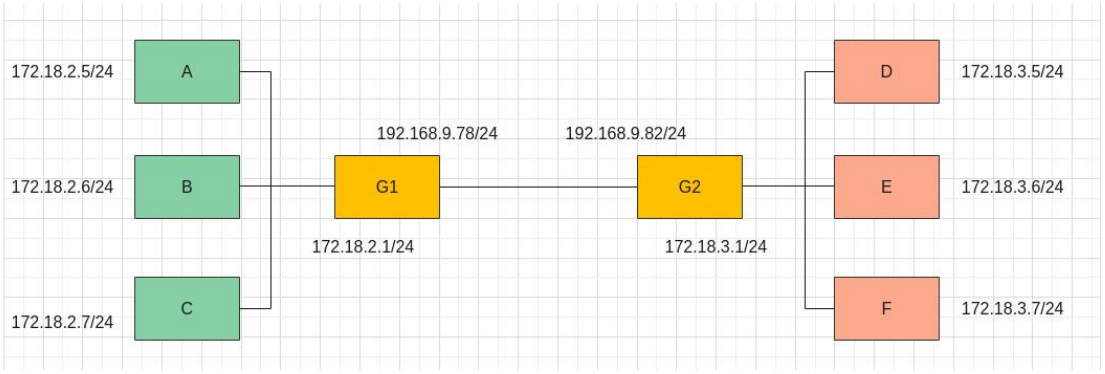
Follow the steps below to set a remote secret**.**

1. Assign a name for the secrete;
2. Select **Enabled** from the dropdown list to enable the secret;
3. Select **PSK** as the secret type;
4. Input the PSK ID: 192.168.9.82 (WAN IP of G2);
5. Input a password;
6. Click **OK** to save the secret.



The local secret of G1 acts as the remote secret of G2, and the remote secret of G1 acts as the local secret of G2.

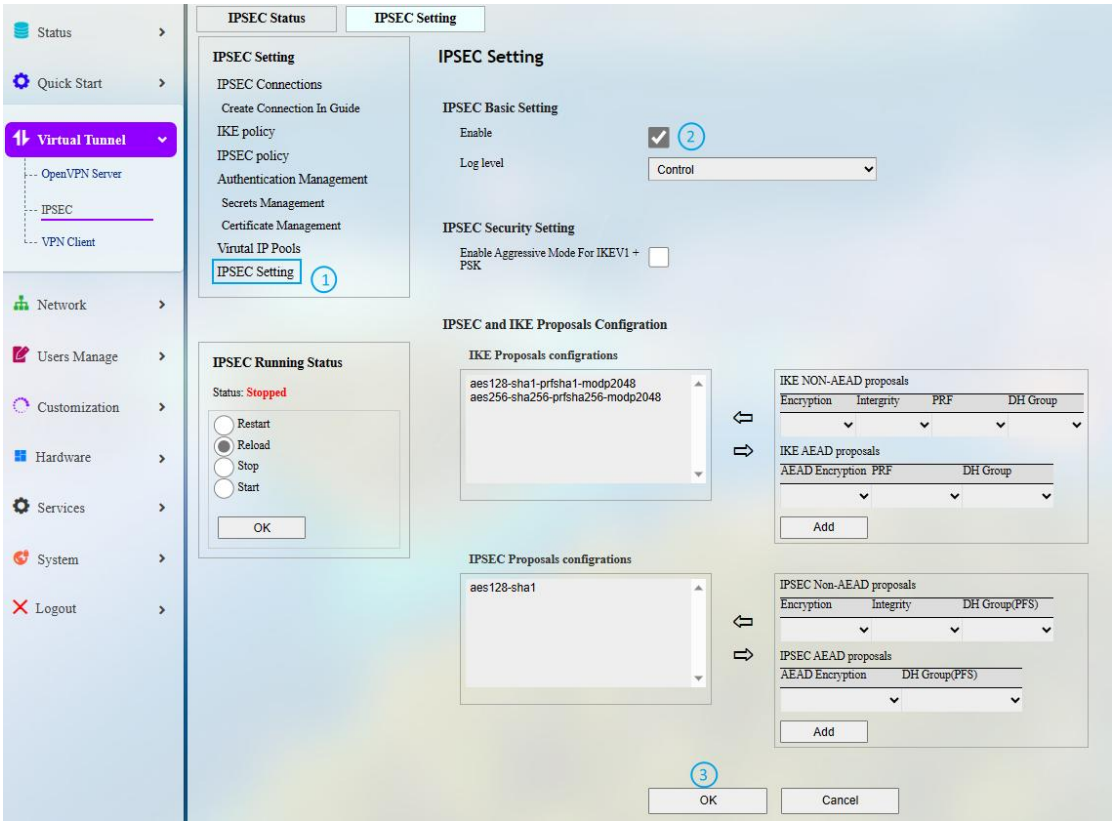
3.5.4 IPSec Connection Setup



Introduction to the above scenarios

- Scenario 1: Host-to-Host, G1 connects with G2 via IPSec, and subnets are not connected
- Scenario 2: Site-to-Site, G1 connects with G2 via IPSec, and subnets are connected
- Scenario 3: Remote access (Server), D connects to G1 via IPSec with access to subnets of G1
- Scenario 4: Remote access (Client), A connects to G2 via IPSec with access to subnets of G2

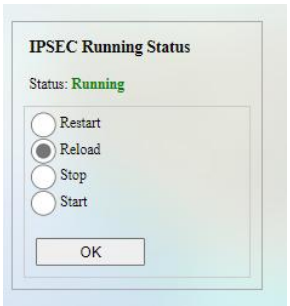
STEP 1: Enabling IPSec



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSEC Setting**
2. Enable IPSec settings
3. Click **OK** to save the setting

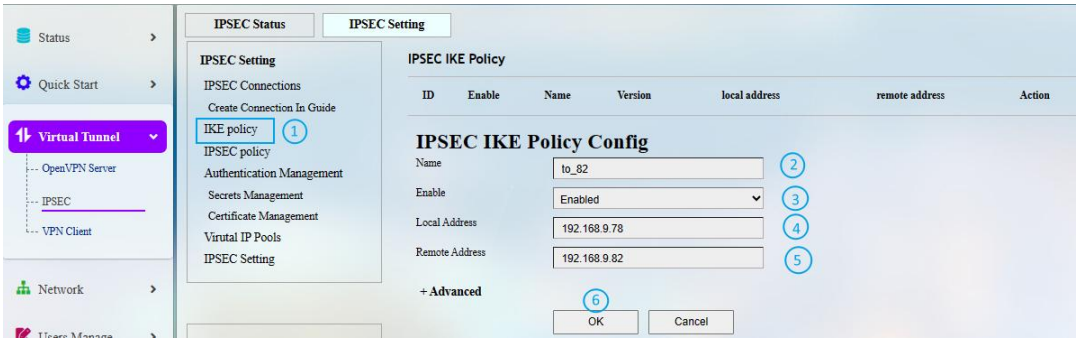
After the settings are loaded, the status of IPSec will change to ‘running’ as follows.



STEP 2: IKE policy configuration

Configurations for scenarios 1 and 2:

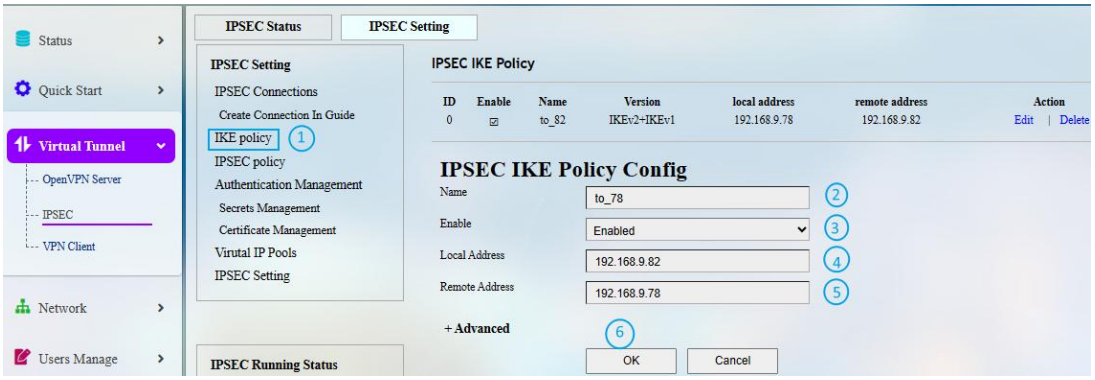
G1 setup



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IKE policy**
2. Assign a name to the policy
3. Select **Enabled** from the dropdown list to enable the policy
4. Input the local address: 192.168.9.78
5. Input the remote address: 192.168.9.82
6. Click **OK** to save the settings

G2 setup

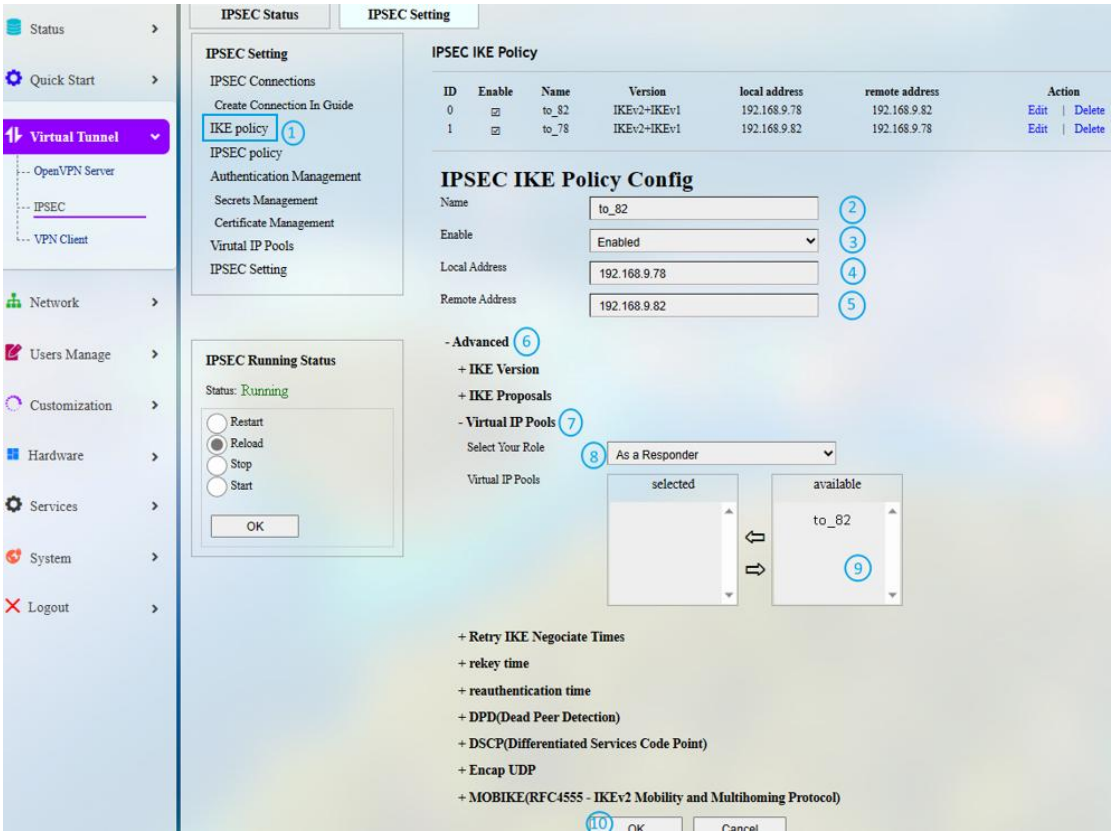


Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IKE policy**
2. Assign a name to the policy
3. Select **Enabled** from the dropdown list to enable the policy
4. Input the local address: 192.168.9.82
5. Input the remote address: 192.168.9.78
6. Click **OK** to save the settings

Configurations for scenario 3 (swapping the configurations of G1 and G2 will get you the configurations for scenario 4):

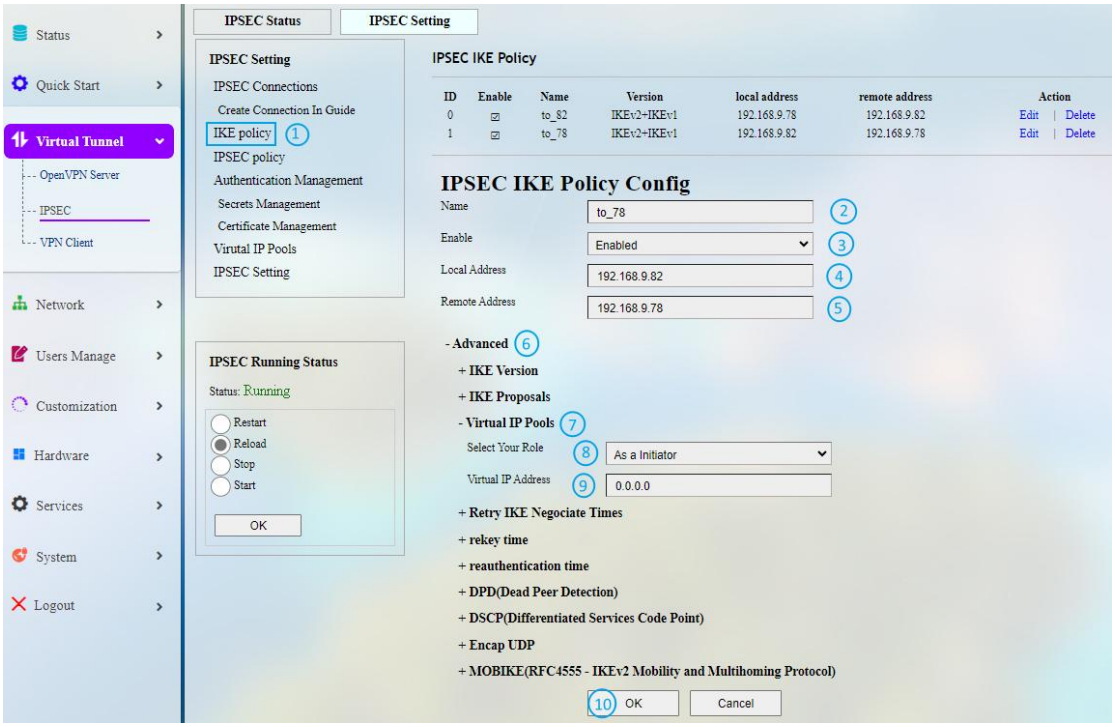
G1 setup



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IKE policy**
2. Assign a name to the policy (to_82)
3. Select **Enabled** from the dropdown list to enable the policy
4. Input the local address: 192.168.9.78
5. Input the remote address: 192.168.9.82
6. Click **Advanced** to access the advanced settings
7. Click **Virtual IP Pools**
8. Select 'Responder' as the role of G1
9. Double click the available 'to_82' IP to select it
10. Click **OK** to save the settings

G2 setup



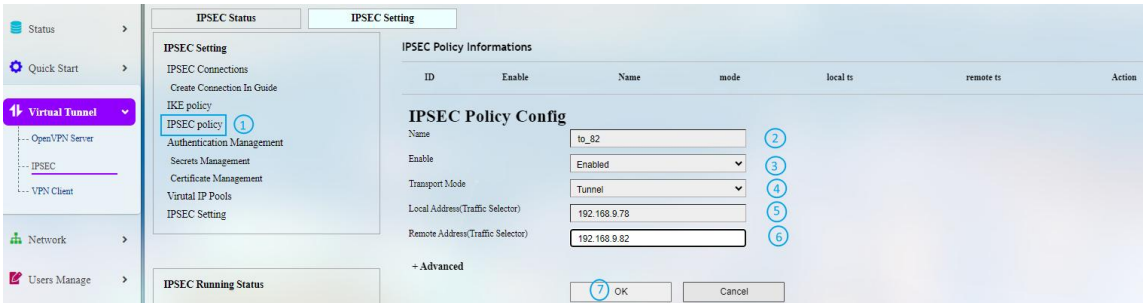
Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IKE policy**
2. Assign a name to the policy (to_78)
3. Select **Enabled** from the dropdown list to enable the policy
4. Input the local address: 192.168.9.82
5. Input the remote address: 192.168.9.78
6. Click **Advanced** to access the advanced settings
7. Click **Virtual IP Pools**
8. Select 'Initiator' as the role of G2
9. Input a virtual IP (0.0.0.0)
10. Click **OK** to save the settings

STEP 3: IPSec policy configuration

Configurations for scenario 1:

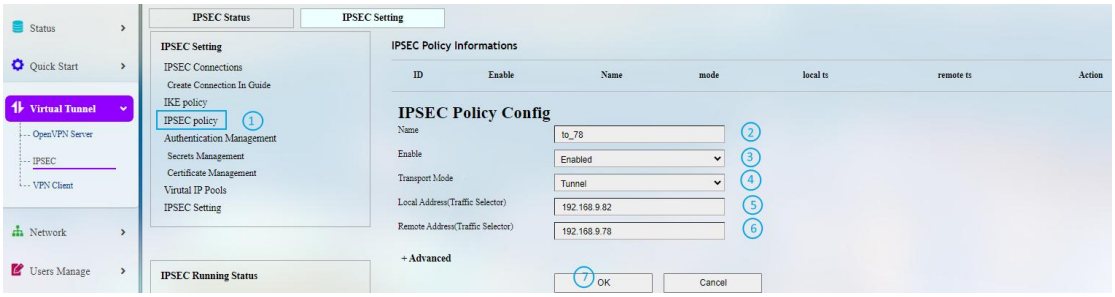
G1 setup



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSec policy**
2. Assign a name to the policy (to_82)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the local address: 192.168.9.78
6. Input the remote address: 192.168.9.82
7. Click **OK** to save the settings

G2 setup



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSec policy**
2. Assign a name to the policy (to_78)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the local address: 192.168.9.82
6. Input the remote address: 192.168.9.78
7. Click **OK** to save the settings

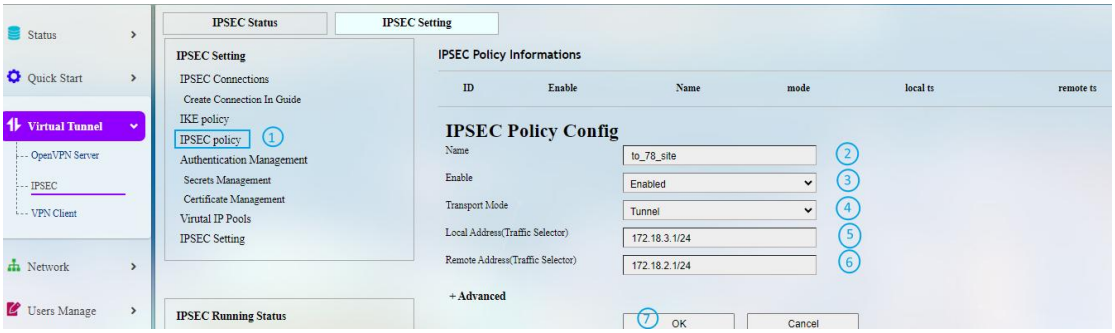
Configurations for scenario 2:

G1 setup

Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSec policy**
2. Assign a name to the policy (to_82_site)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the local address: 172.18.2.1/24 (LAN IP of G1)
6. Input the remote address: 172.18.3.1/24 (LAN IP of G2)
7. Click **OK** to save the settings

G2 setup



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSec policy**
2. Assign a name to the policy (to_78_site)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the local address: 172.18.3.1/24 (LAN IP of G2)
6. Input the remote address: 172.18.2.1/24 (LAN IP of G1)
7. Click **OK** to save the settings

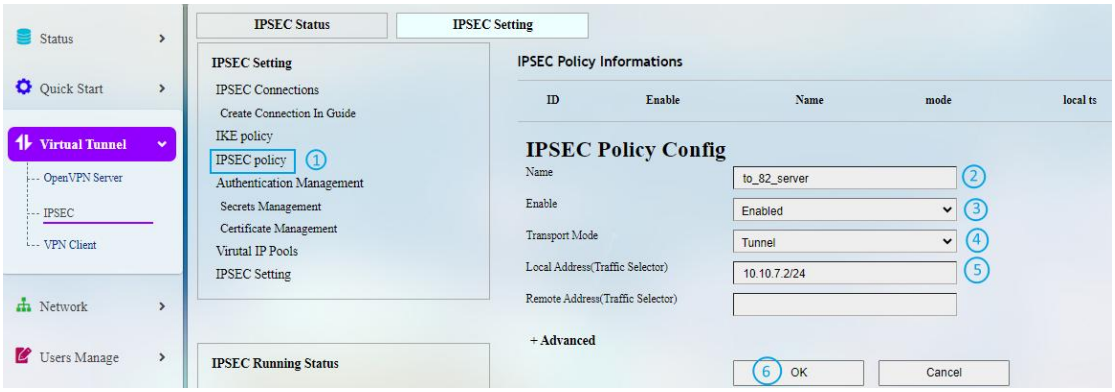
Configurations for scenario 3 (swapping the configurations of G1 and G2 will get you the configurations for scenario 4):

Virtual IP setup of G1

Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Virtual IP Pools**
2. Assign a name to the policy (to_82)
3. Select **Enabled** from the dropdown list to enable the policy
4. Input a virtual address: 10.10.7.0/24
5. Click **OK** to save the settings

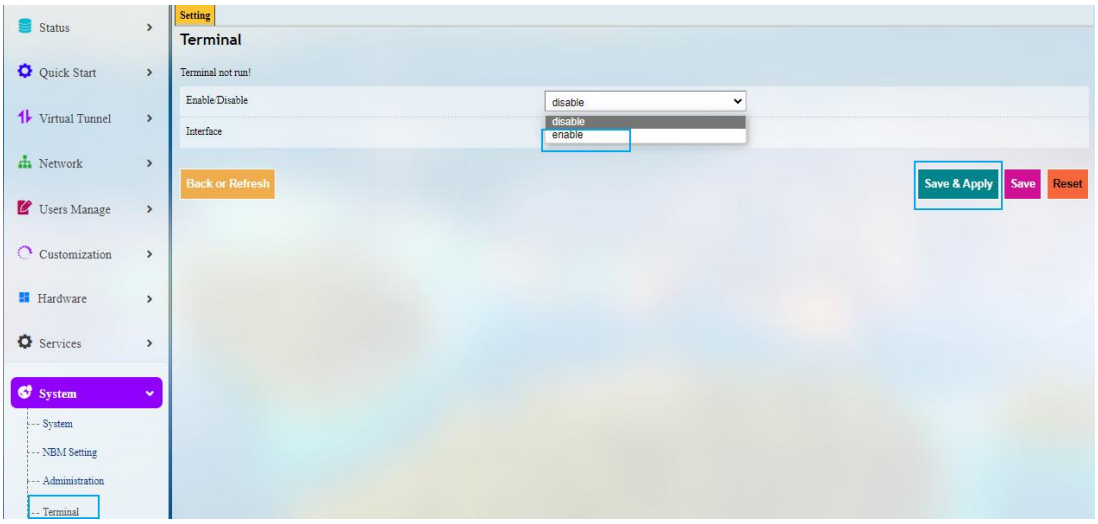
IPSec policy of G1



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSec policy**
2. Assign a name to the policy (to_82_server)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the local address: 10.10.7.0/24
6. Click **OK** to save the settings

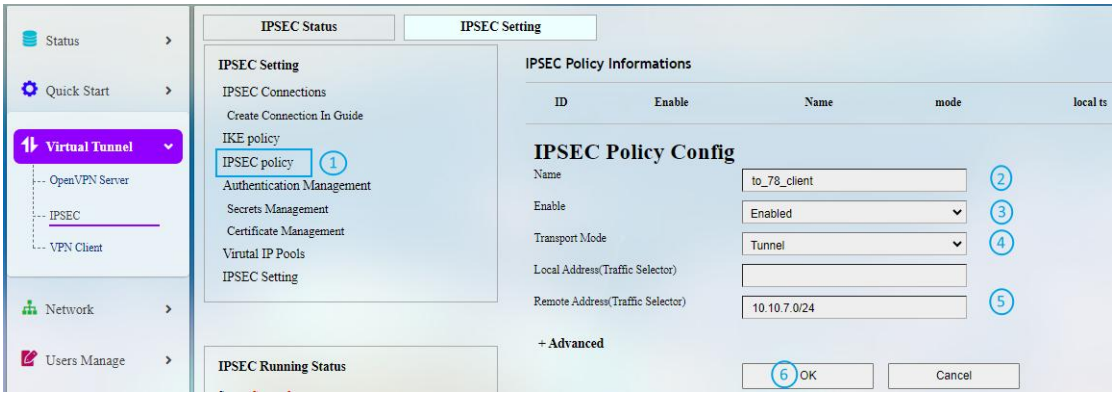
Navigate to **System > Terminal > Settings** to enable the terminal.



Log in with root account (default password: rootpassword), and input the following command to add the IP to G1.

```
ip address add 10.10.7.2/24 dev eth0
```

IPSec policy of G2



Description of the numbered areas

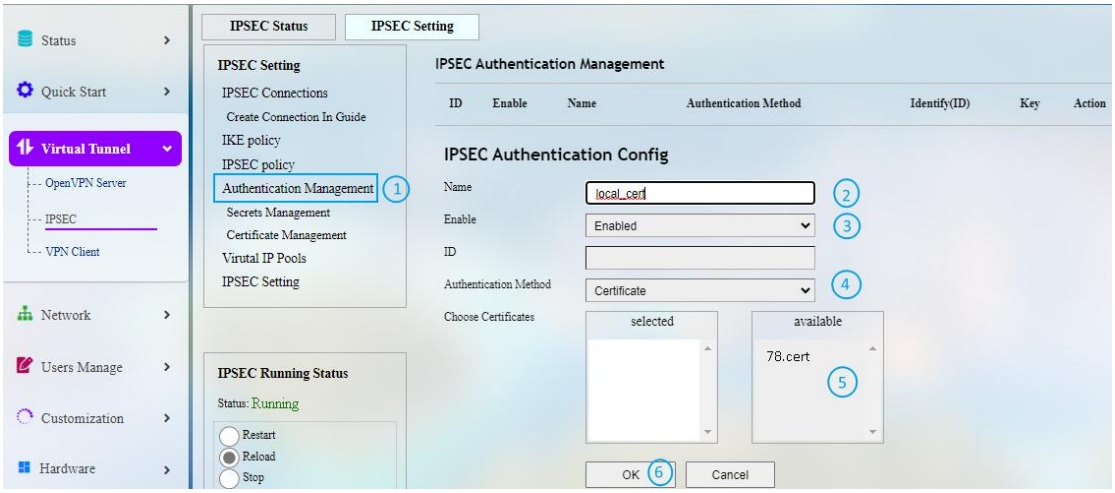
1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSEC policy**
2. Assign a name to the policy (to_78_client)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the remote address: 10.10.7.0/24
6. Click **OK** to save the settings

STEP 4: Authentication management

Three ways are available for the authentication: certificate, PSK, and public key.

Certificate authentication

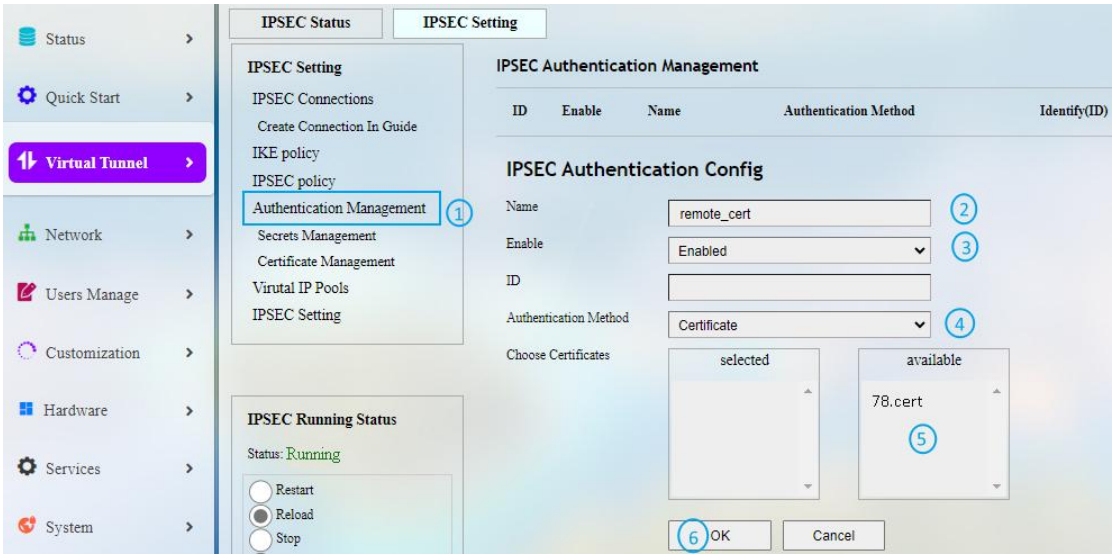
Configurations of G1 for local authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. **Certificate** is the default authentication method
5. Double click the available ’78.cert’ certificate to select it
6. Click **OK** to save the settings

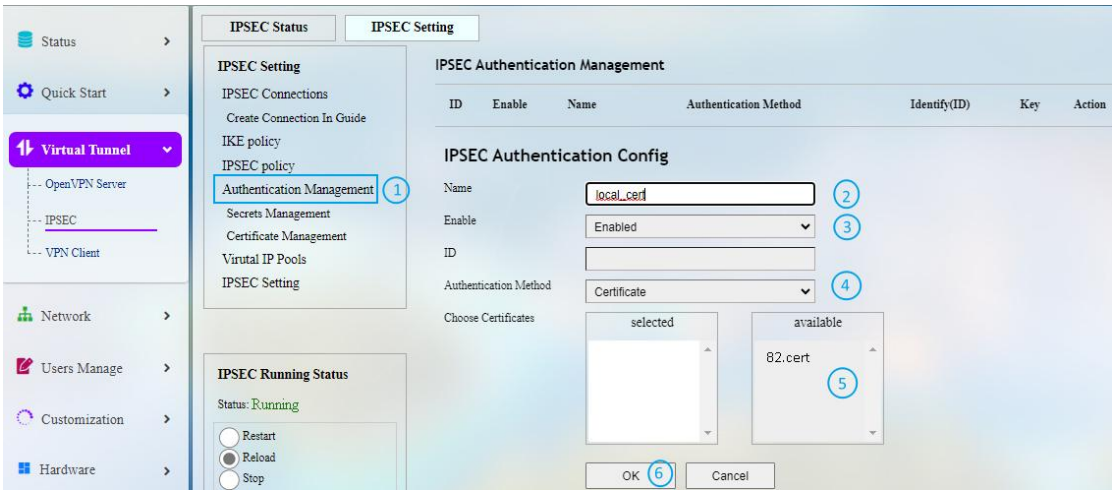
Configurations of G1 for remote authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. **Certificate** is the default authentication method
5. Double click the available '78.cert' certificate to select it
6. Click **OK** to save the settings

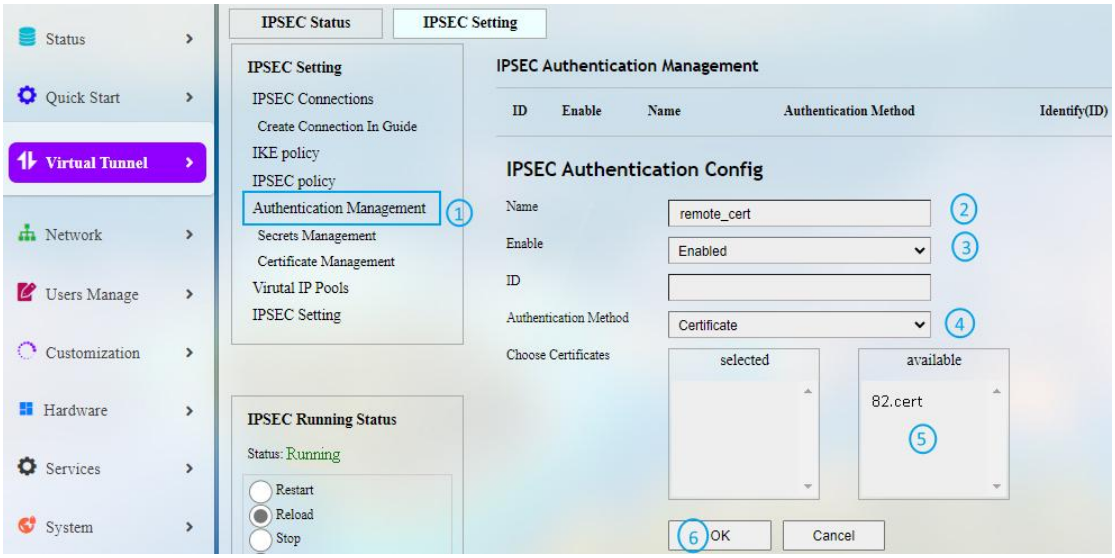
Configurations of G2 for local authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. **Certificate** is the default authentication method
5. Double click the available '82.cert' certificate to select it
6. Click **OK** to save the settings

Configurations of G2 for remote authentication

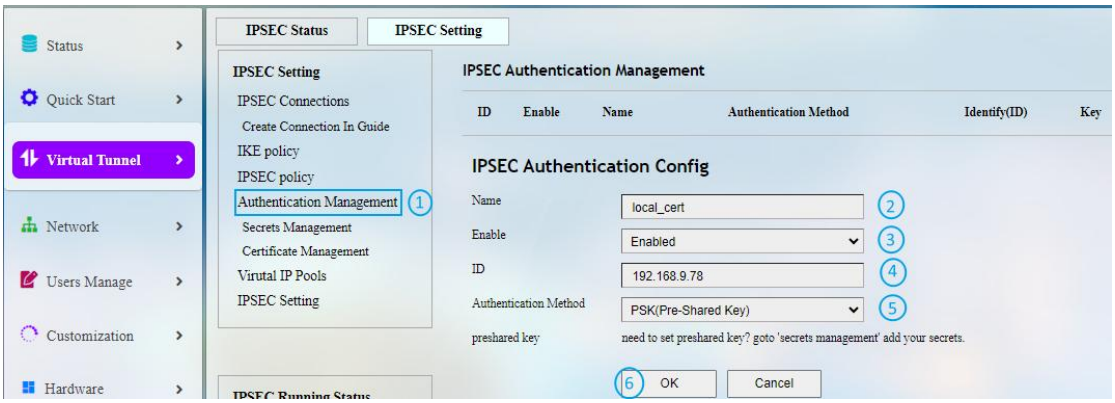


Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. **Certificate** is the default authentication method
5. Double click the available ’82.cert’ certificate to select it
6. Click **OK** to save the settings

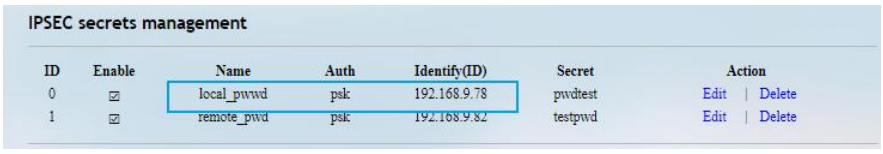
PSK authentication

Configurations of G1 for local authentication



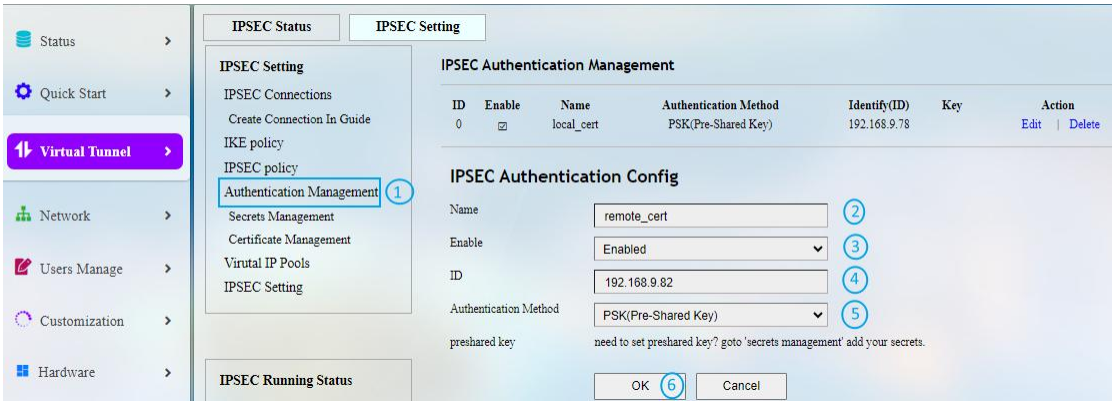
Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. Input the ID same as that set in **Secret Management** (192.168.9.78)



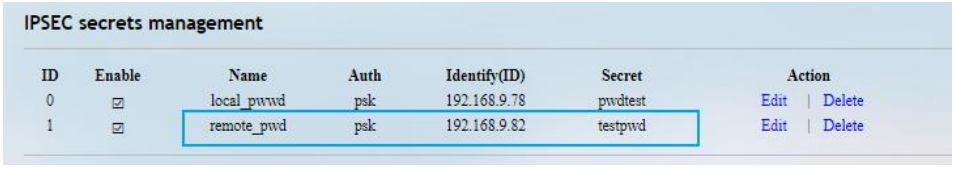
5. Select **PSK (Pre-shared key)** from the drop-down list as the authentication method
6. Click **OK** to save the settings

Configurations of G1 for remote authentication



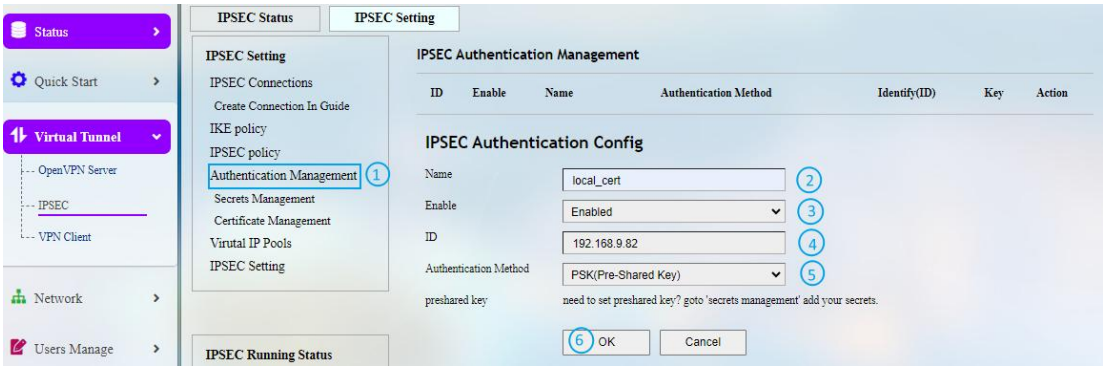
Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. Input the ID same as that set in **Secret Management** (192.168.9.82)



5. Select **PSK (Pre-shared key)** from the drop-down list as the authentication method
6. Click **OK** to save the settings

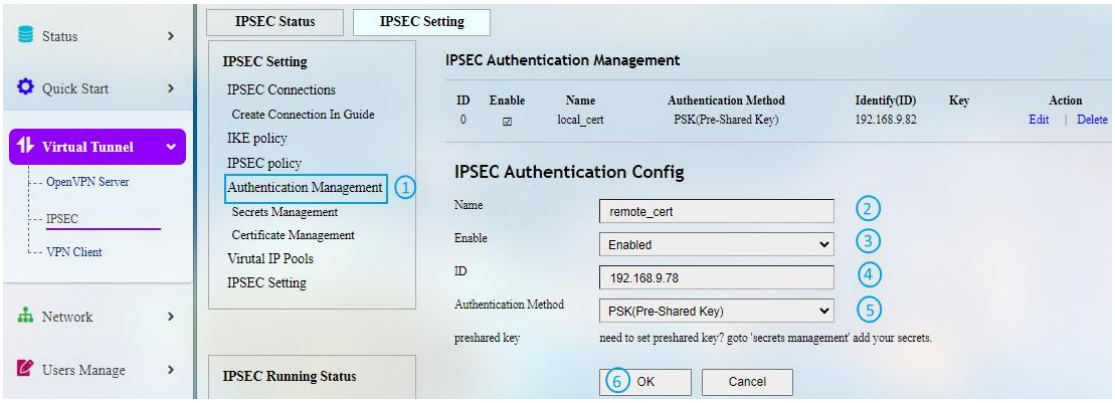
Configurations of G2 for local authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. Input the ID same as that set in **Secret Management** (192.168.9.82)
5. Select **PSK (Pre-shared key)** from the drop-down list as the authentication method
6. Click **OK** to save the settings

Configurations of G2 for remote authentication



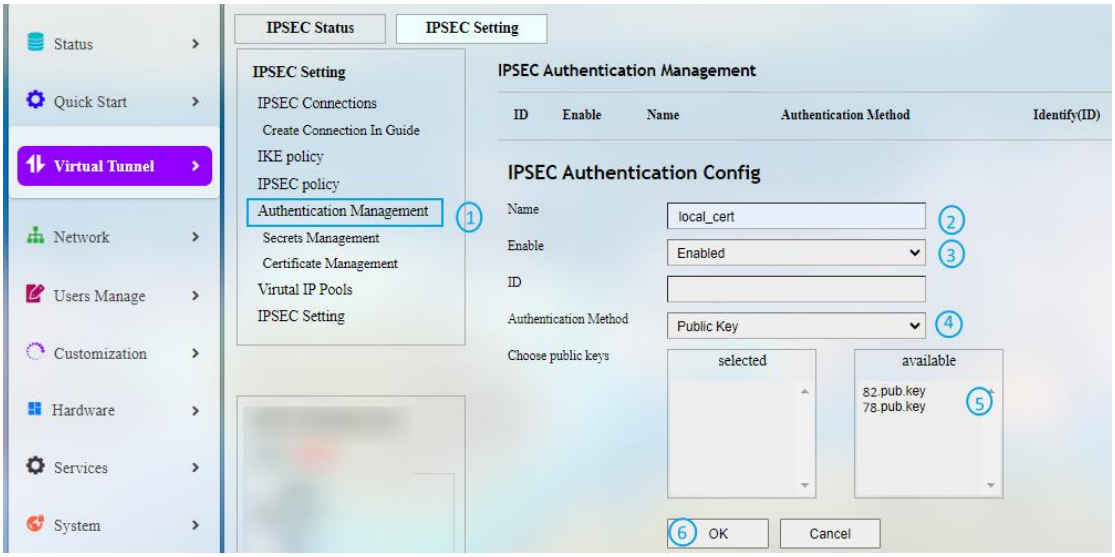
Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. Input the ID same as that set in **Secret Management** (192.168.9.78)
5. Select **PSK (Pre-shared key)** from the drop-down list as the authentication method
6. Click **OK** to save the settings

Public key authentication

This authentication requires to upload the public key of G1 (78.pub.key) to G2 and upload the public key of G2 (82.pub.key) to G1.

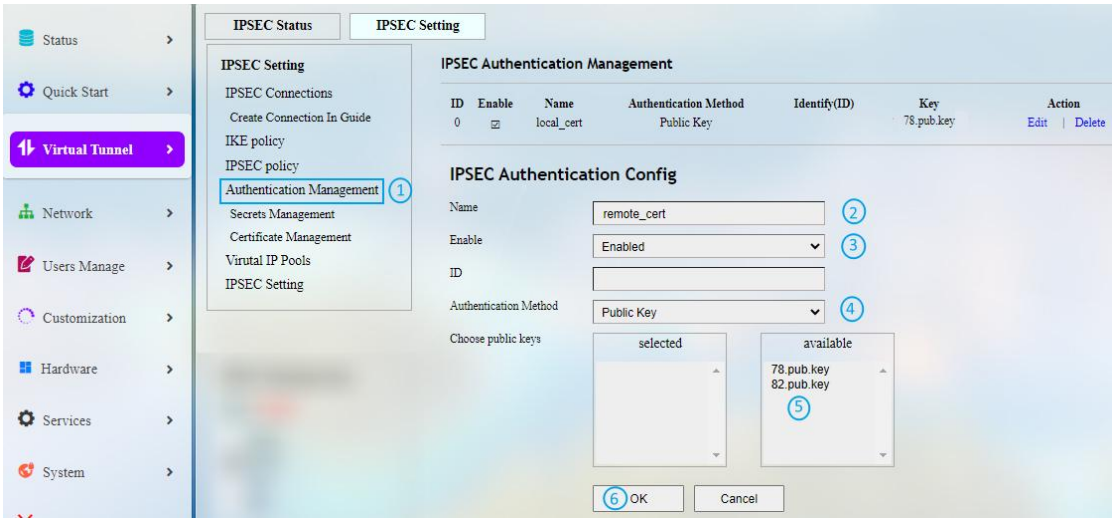
Configurations of G1 for local authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. Select **Public key** from the drop-down list as the authentication method
5. Double click to select '78.pub.key'
6. Click **OK** to save the settings

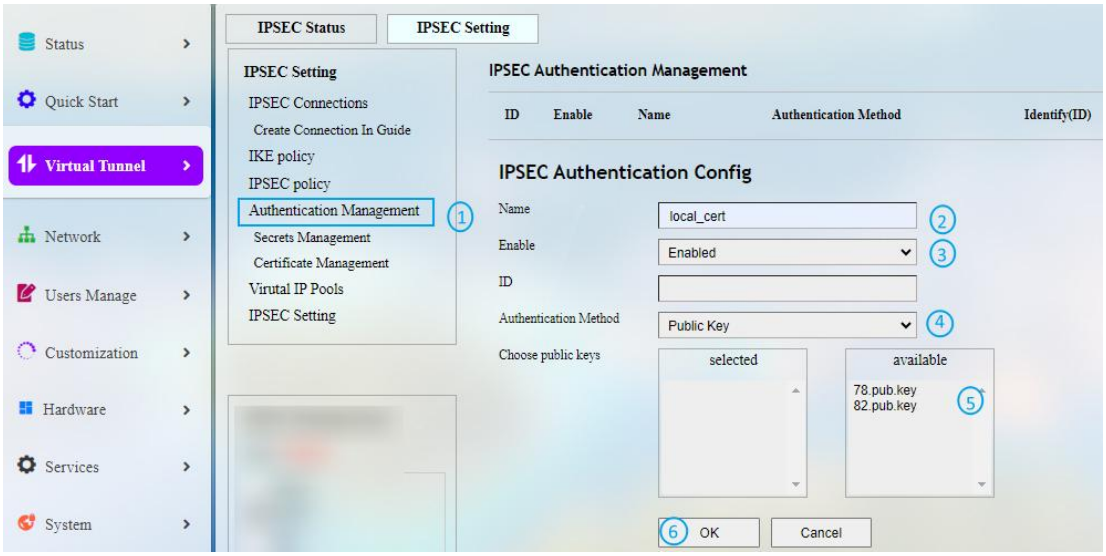
Configurations of G1 for remote authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. Select **Public key** from the drop-down list as the authentication method
5. Double click to select ’82.pub.key’
6. Click **OK** to save the settings

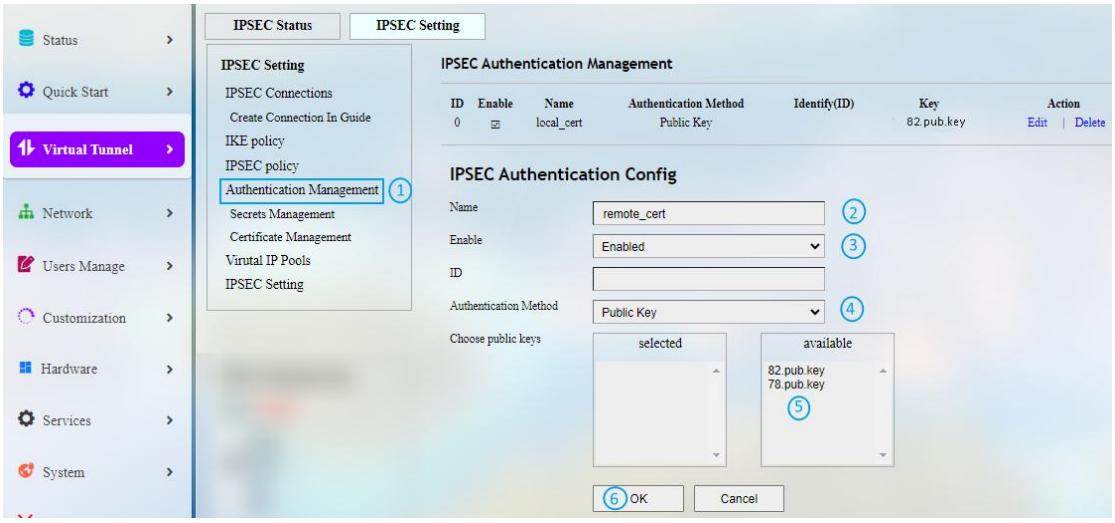
Configurations of G2 for local authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. Select **Public key** from the drop-down list as the authentication method
5. Double click to select ’82.pub.key’
6. Click **OK** to save the settings

Configurations of G2 for remote authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. Select **Public key** from the drop-down list as the authentication method
5. Double click to select ’78.pub.key’
6. Click **OK** to save the settings

STEP 5: Configurations for IPSec connection

G1 setup

Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSEC Connection**
2. Assign a name for the connection (to_82)
3. The certificate is **Enabled** by default
4. Select a previously created IKE policy ('to_82' in this case) from the drop-down list
5. Double click a previously created local authentication policy ('local_cert' in this case) to select the policy
6. Double click a previously created remote authentication policy ('remote_cert' in this case) to select the policy
7. Double click a previously created IPSec policy ('to_82' in this case) to select the policy
8. Click **OK** to save the settings

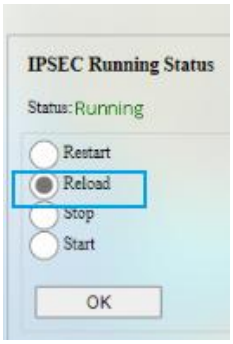
G2 setup

Description of the numbered areas

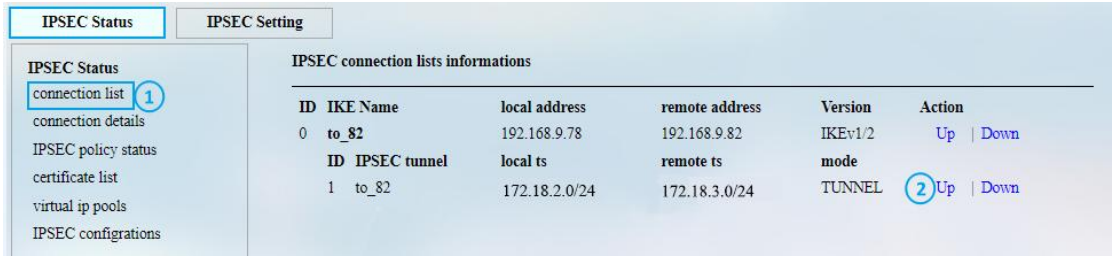
1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSEC Connection**
2. Assign a name for the connection (to_78)
3. The certificate is **Enabled** by default
4. Select a previously created IKE policy ('to_78' in this case) from the drop-down list
5. Double click a previously created local authentication policy ('local_cert' in this case) to select the policy
6. Double click a previously created remote authentication policy ('remote_cert' in this case) to select the policy
7. Double click a previously created IPSec policy ('to_78' in this case) to select the policy
8. Click **OK** to save the settings

STEP 6: Reloading the IPSec program

Click the radio button before **Reload** and then **OK** to reload the program.



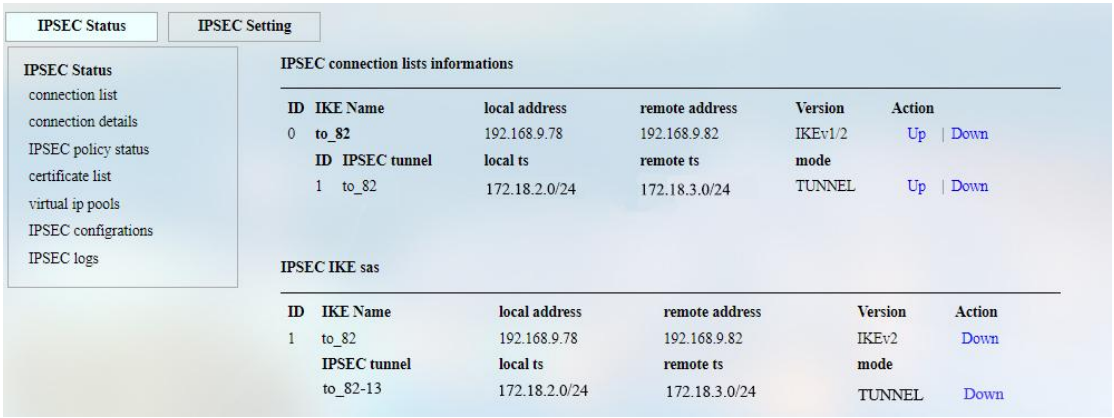
STEP 7: IPSec connection



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Status> Connection list**
2. Select the connection setting and click **Up**

When the connection is added to **IPSEC IKE SAS**, the connection is established successfully.



3.6 Network

Users can change the settings related to the available network interfaces in the **Network** page.

3.6.1 Interfaces

All the network interfaces currently available and configurable are displayed under **Network > Interfaces**.

Take the LAN port for example, the numbered areas are as follows:

1. Interface overview
2. Interface traffic details
3. Restart the interface manually
4. Edit the interface settings
5. Delete the interface (available only when you log in as a root user)
6. Instantaneous traffic of the interface
7. Add a new interface (available only when you log in as a root user)

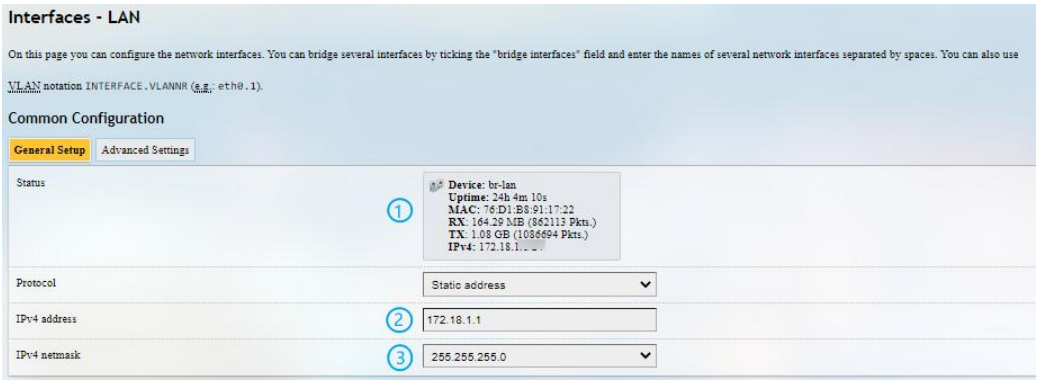
The interfaces may differ from what is shown above as certain interfaces are related to your prior settings and the communication modules available on the device.

The following section illustrates on how to edit the LAN port and WAN port settings of the Router.

3.6.1.1 LAN

- **Common Configurations**

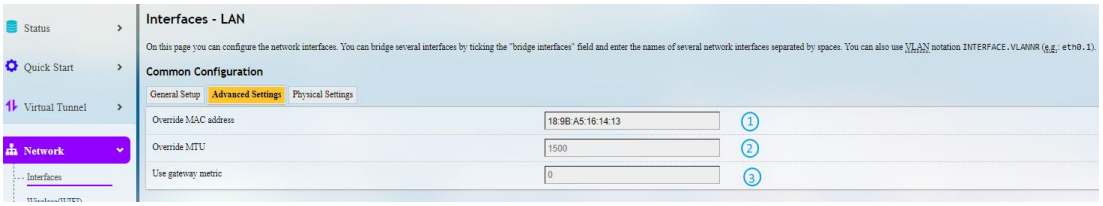
Clicking on the **Edit** button behind the **LAN** port will allow you to access the configurations of the LAN port, and **General Setup** is displayed by default.



Description of the numbered areas

1. Status of the interface
2. The IP address of the LAN port
3. The LAN port subnet mask

In the **Advanced Settings** next to the general setup:

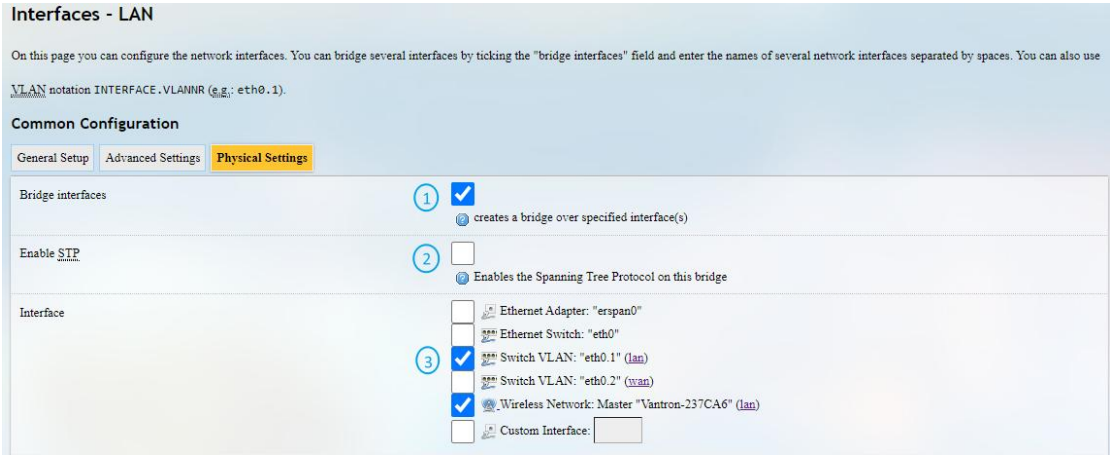


Description of the numbered areas

1. MAC address cloning
2. Set the MTU (keep the default setting)
3. Set a gateway metric (keep the default setting)

Be sure to save the settings before you exit the page.

There is a **Physical Settings** tab next to **Advanced settings** when you log in with the root account, allowing you to configure the LAN port for network bridge.



Description of the numbered areas

1. Enable the interface for network bridge
2. Enable STP protocol
3. Select the interfaces for bridge connection

Be sure to save the settings before you exit the page.

- **DHCP server**

In the **General Setup** page of **DHCP Server**, DHCP could be set up with more details:

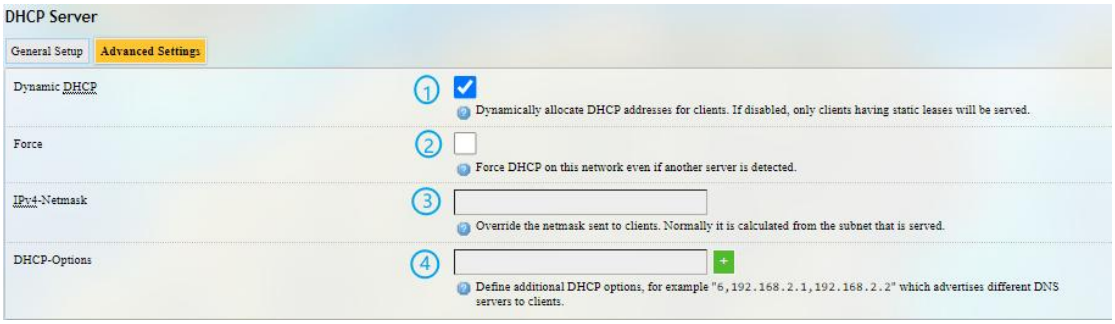
Description of the numbered areas

1. Disable the DHCP service

If disabled, the DHCP service will not be available to the client devices connected to the LAN port of the Router.

2. DHCP start address
3. Maximum number of leased addresses (up to 150)
4. Expiry time of leased addresses (min. 2m)

Advanced Settings of DHCP Server:



Description of the numbered areas

1. Enable allocation of DHCP addresses for client devices
2. Force enablement of DHCP service (to bypass other servers)
3. Override the netmask sent to clients

Normally it is based on the subnet that is served.

4. Add different DNS servers for client devices

*Be sure to save the settings before you exit the page. Clicking on **Back or Refresh** will get you back to the general information of the network interface.*

3.6.1.2 WAN

- **General DHCP settings**

Clicking on the **Edit** button behind the **WAN** port will allow you to access the configurations of the WAN port, and **General Setup** is displayed by default.

Description of the numbered areas

1. Status of the WAN port
2. Select a WAN protocol (DHCP client by default)
3. Input a hostname of the Router for requesting DHCP

Be sure to save the settings before you exit the page.

- **Advanced DHCP settings**

If you have selected DHCP client protocol, advanced settings are available after you have finished the setup as mention above.

Description of the numbered areas

1. Check the box to bring up the port upon device boot
2. Force link (once the box is checked, hotplug handlers will not be invoked after a link change)
3. Enable **Use default gateway**
4. Enable **Use DNS server advertised by peer**

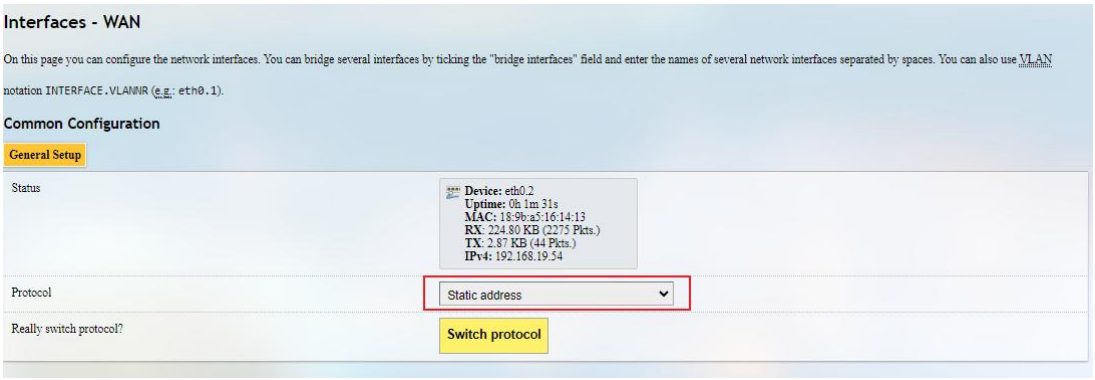
If this option is disabled, you will need to define a DNS server.

5. Set a gateway metric
6. MAC address cloning
7. Set the MTU

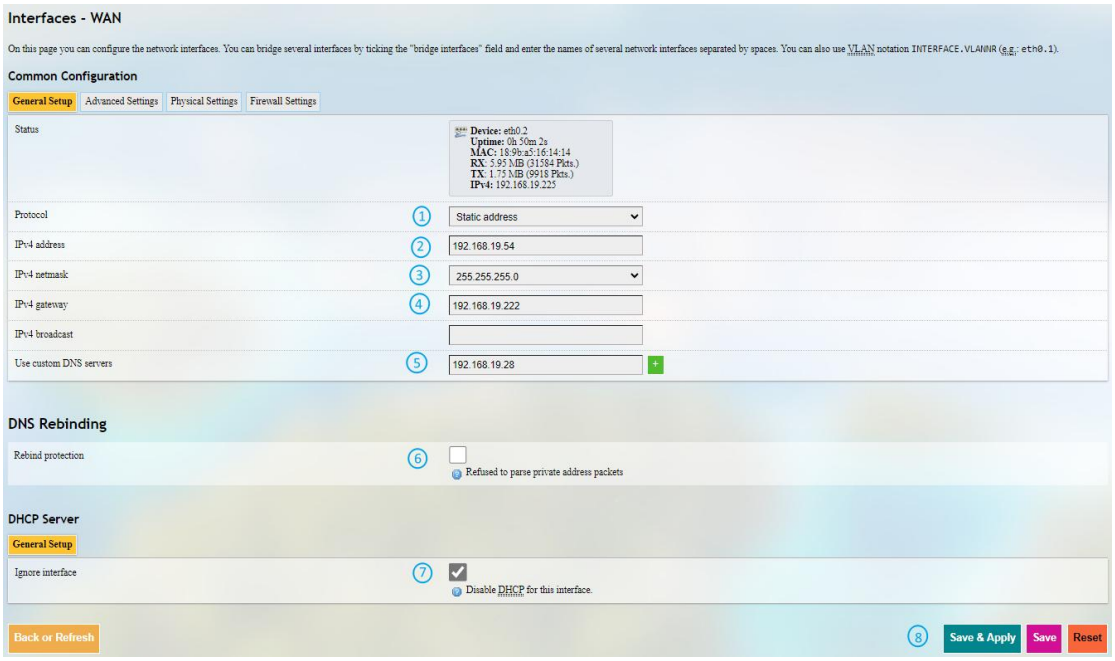
Be sure to save the settings before you exit the page.

- **General Static protocol settings**

To activate static address protocol, select **Static address** from the protocol drop-down list under **General Setup** of the WAN port and click **Switch protocol**.



Upon a click of **Switch protocol**, you'll need to input the IPv4 address, subnet mask, IPv4 gateway, and the IPv4 broadcast.



Description of the numbered areas

1. Current protocol
2. Input an IPv4 address
3. Input an IPv4 netmask
4. Input the IPv4 gateway
5. Set a custom DNS server (can be provided by the carrier or self-defined)
6. DNS re-binding protection (if enabled, parsing of private IP data will be refused)
7. Disable DHCP service (keep the default settings)

8. Save & apply the settings

Leave the field as is if not applicable.

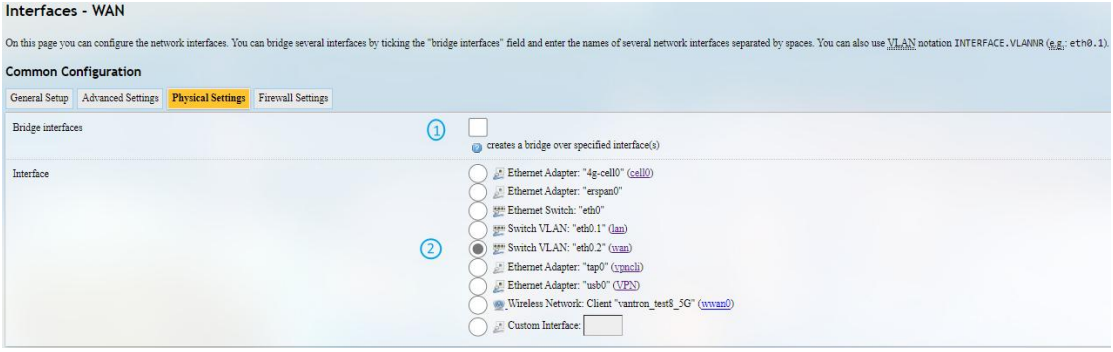
When static address protocol is selected, DHCP server will be automatically disabled.

The advanced settings are basically same as those for DHCP protocol.

Be sure to save the settings before you exit the page.

Other available WAN protocols include PPPoE, GRE tunnel over IPv4, and relay bridge. The settings are dependent on the specific protocols. Clicking on **Back or Refresh** allows you to return to interface settings.

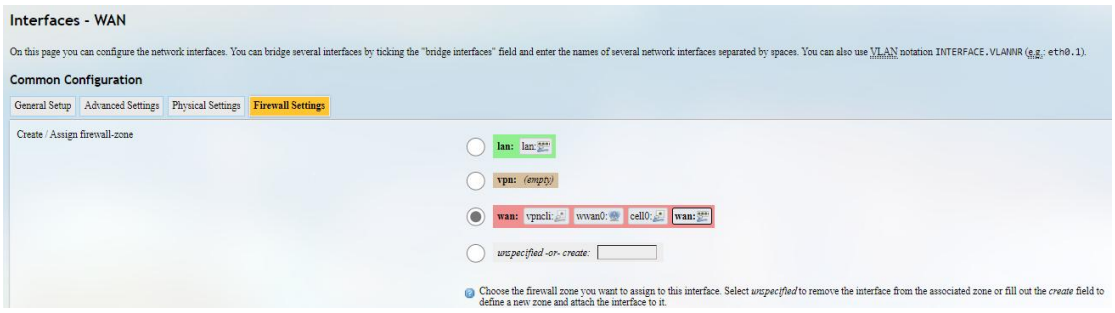
There is a **Physical Settings** tab next to **Advanced settings** when you log in with the root account, allowing you to configure the WAN port for network bridge.



Description of the numbered areas

1. Enable the interface for network bridge
2. Select the interfaces for bridge connection

There is a **Firewall Settings** tab next to the **Physical settings** tab when you log in with the root account, allowing you to create or designate a firewall zone.

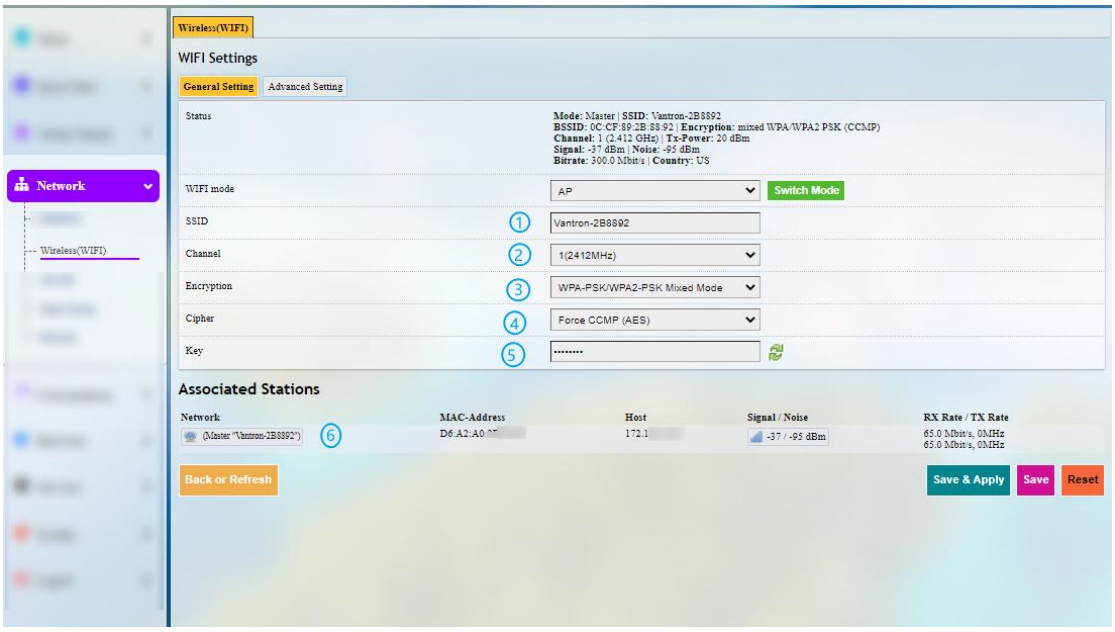


When 'unspecify or create' is selected, you can remove the interface from the associated firewall zone or create a new zone.

3.6.2 Wireless (WIFI)

You can switch between AP and client modes for wireless connection.

3.6.2.1 Wi-Fi – AP Mode (General settings)



Description of the numbered areas

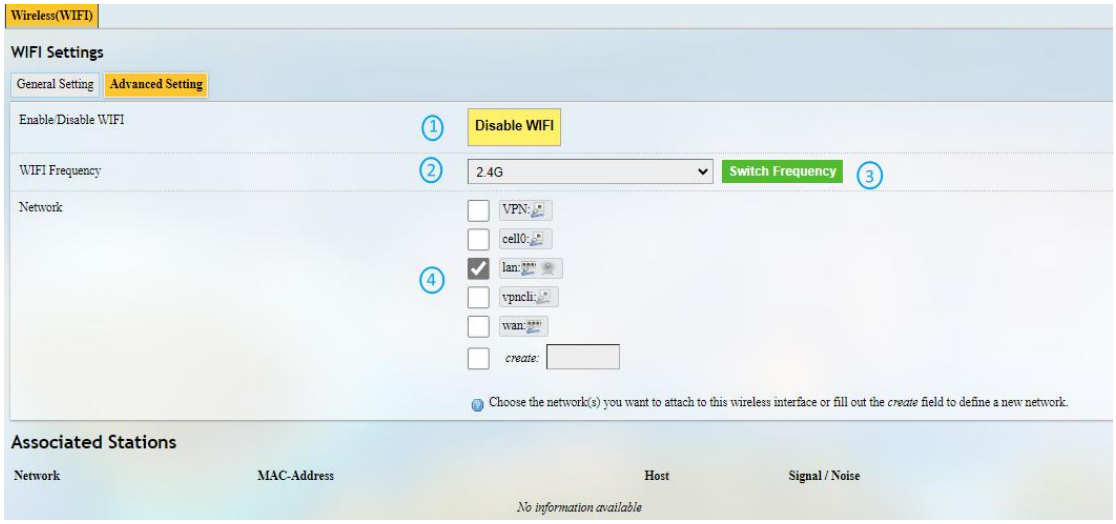
1. Set an SSID for the Router

The ID name shall not contain special characters including $, `, \.

2. Select a Wi-Fi channel
3. Select an encryption method (the following options vary with the encryption method)
4. Select an encryption algorithm
5. Assign a Wi-Fi password (no less than 8 characters)
6. List of currently connected devices

Be sure to save the settings before you exit the page.

3.6.2.2 Wi-Fi – AP Mode (Advanced setting)



Description of the numbered areas

1. Turn on/off Wi-Fi
2. Select a Wi-Fi frequency (determined by hardware)
3. Click to switch the frequency
4. The network interfaces to which Wi-Fi belongs

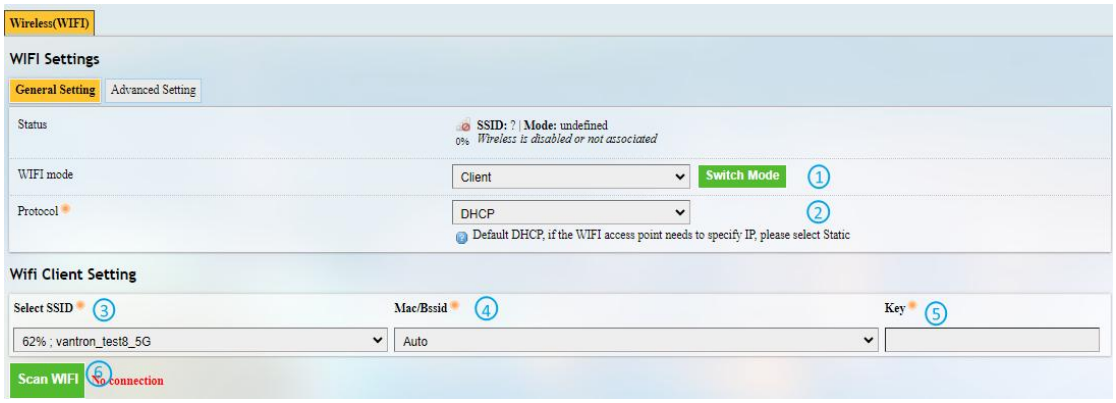
As modification of field 2 will have impact on the Wi-Fi signal, the web interface will return to the general settings page upon a click of the switch button.

Be sure to save the settings before you exit the page.

3.6.2.3 Wi-Fi – Client Mode

When the Router is set as a client on a wireless network, the page below allows you to make changes to the network settings.

*A wwan0 port will be added (as shown in the **Interface** page) when the Wi-Fi client mode is enabled.*

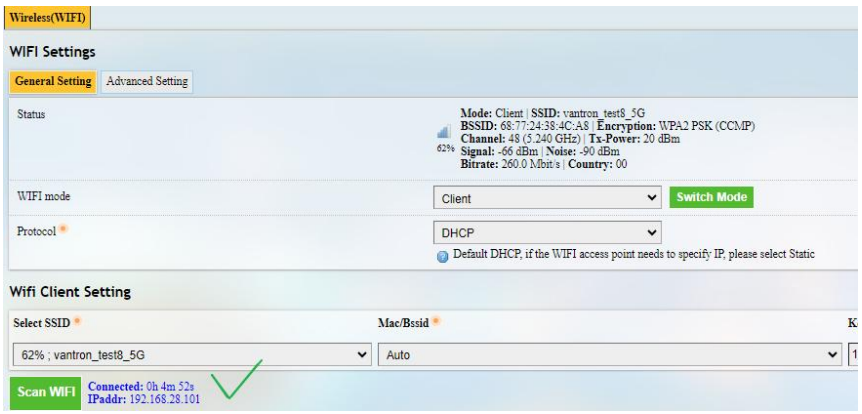


Description of the numbered areas

1. Switch to **Client mode**
2. Select DHCP protocol to automatically get an IP or Static protocol to specify an IP for the Router
3. Select a wireless network for internet access
4. Select the MAC address of the access point or leave it to 'Auto' if not sure
5. Input the password of the access point
6. Click **Scan WIFI** to refresh the Wi-Fi list if the target SSID is not identified

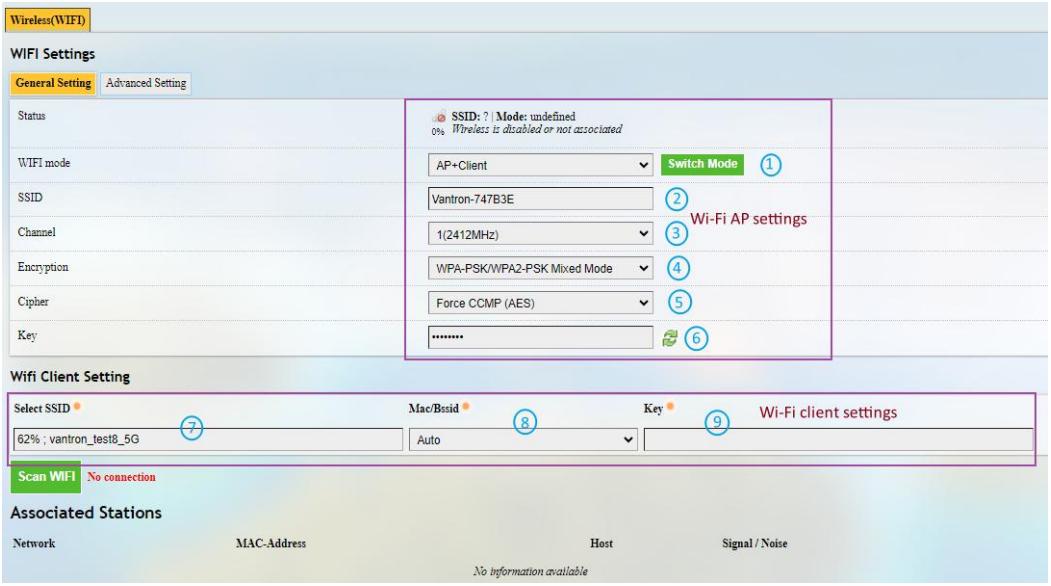
Be sure to save the settings before you exit the page.

When the Router is successfully connected as a client, there will be the network information next to the **Scan WIFI** button.



3.6.2.4 Wi-Fi – AP + Client Mode

This mode enables you to use the Router as an AP to allow client devices to join after it connects a Wi-Fi AP as a client.



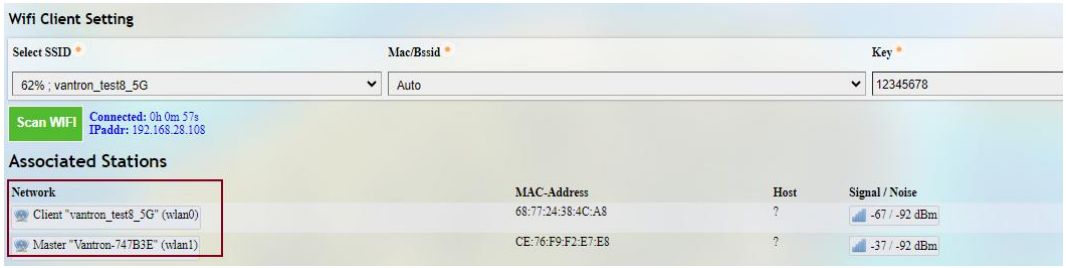
Description of the numbered areas

1. Switch to **AP + Client mode**
2. Set an SSID for the Router
3. Select a Wi-Fi channel
4. Select an encryption method (the following options vary with the encryption method)
5. Select an encryption algorithm
6. Assign a Wi-Fi password (no less than 8 characters)
7. Select a wireless network for internet access
8. Select the MAC address of the access point or leave it to 'Auto' if not sure
9. Input the password of the Wi-Fi

*Click **Scan WIFI** to refresh the Wi-Fi list if the target SSID is not identified.*

Be sure to save the settings before you exit the page.

Status of the connectivity is as follows when the settings take effect.



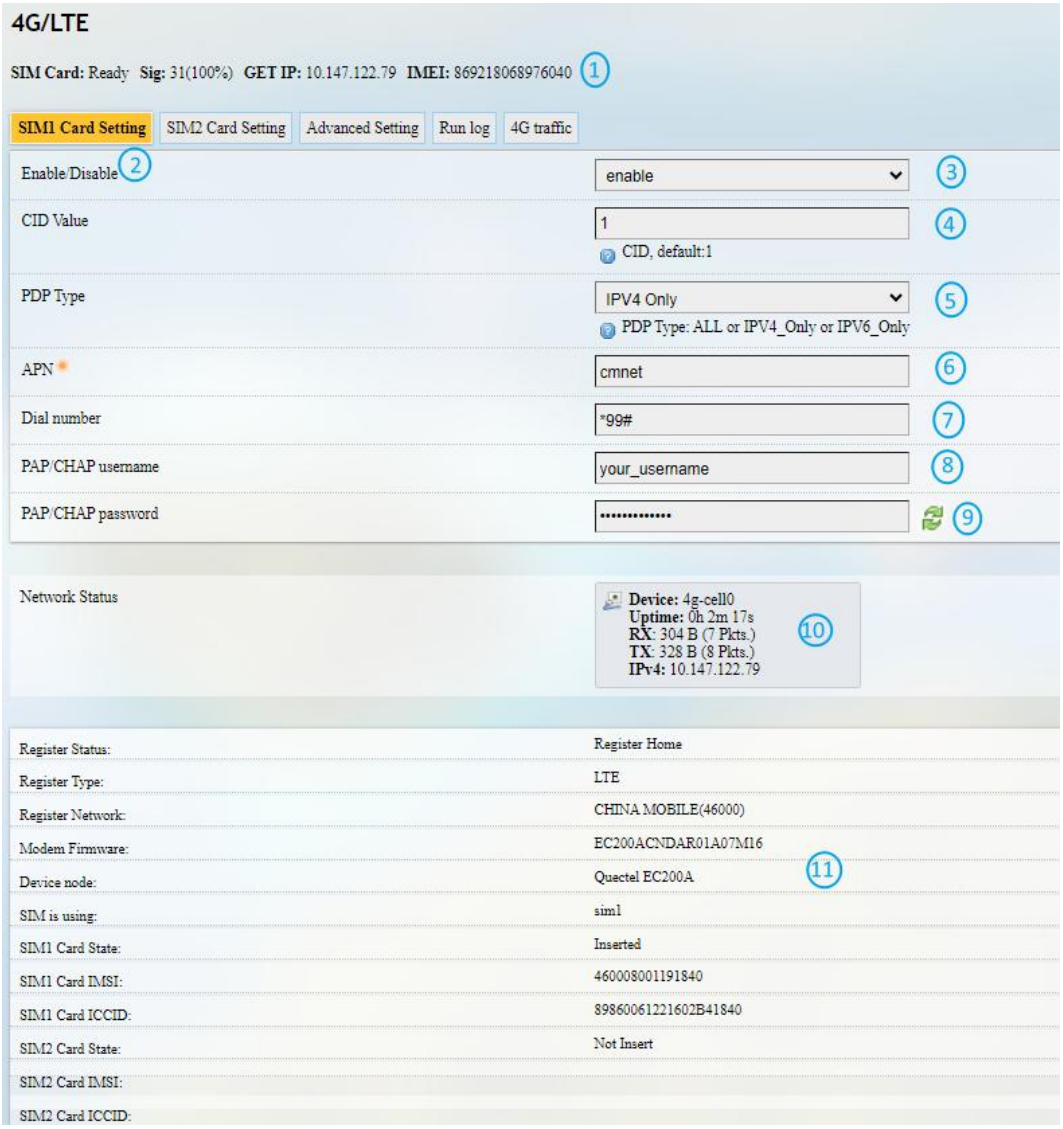
3.6.3 4G/LTE

Before you configure for 4G/LTE, be sure to install the activated SIM card and the LET antennas following the steps set out in 2.1.

Confirm with your sales executive whether the 4G module is AT&T or Verizon pre-certified. If so, when you apply for SIM cards from the carriers,

- provide Verizon with the pre-certified module name **VT-MOB-CELL-mPCIe**.
- provide AT&T with the pre-certified module name **VT-MOB-MPCIE-4G**.

After installation, the 4G signal indicators on the Router will light up to indicate the signal strength. Navigate to **Network > 4G/LTE** for more settings.



Description of the numbered areas

1. Connection status information (including SIM card status, signal strength, IP, and IMEI)
2. Set up SIM card 1/2
3. Enable/Disable the SIM card
4. Input the CID value
5. Select a PDP type
6. Input the APN provided by the carrier
7. Input ***99***1#** for SIM cards from AT&T and ***99***3#** for SIM cards from Verizon
8. Enter the username provided by the carrier for PAP/CHAP authentication
9. Enter the password provided by the carrier for PAP/CHAP authentication
10. Current network interface status
11. Detailed information of the SIM cards

Leave the field as is if not applicable or if you are not sure.

PAP/CHAP username and password are to be specified only if your carrier has setup APN with user name and password.

*If you have inserted a SIM card into SIM slot 2, you can click the **SIM2 Card Setting** tab for more settings.*

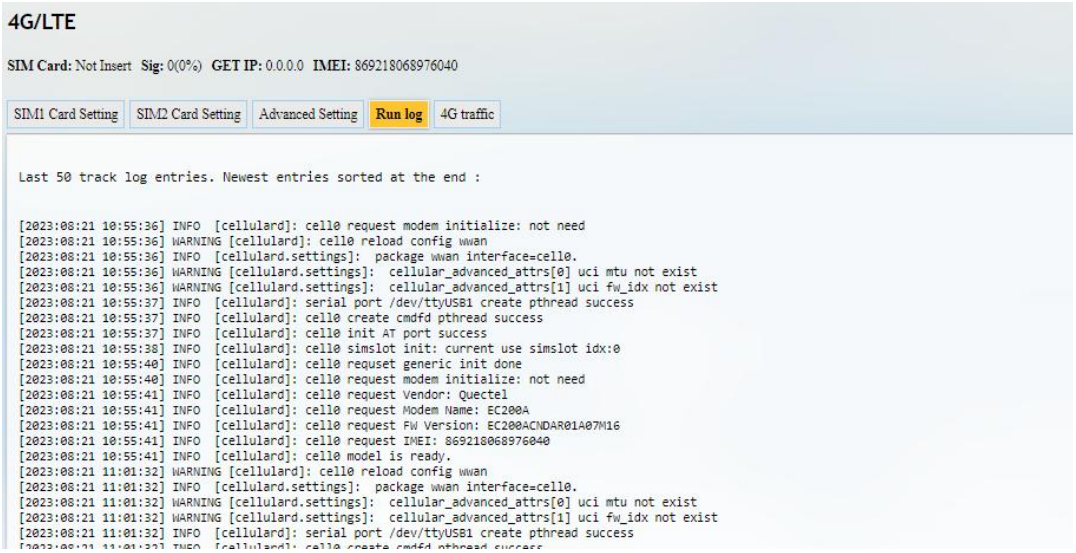
In the **Advanced Setting** page, you can further configure the cellular network.

Description of the numbered areas

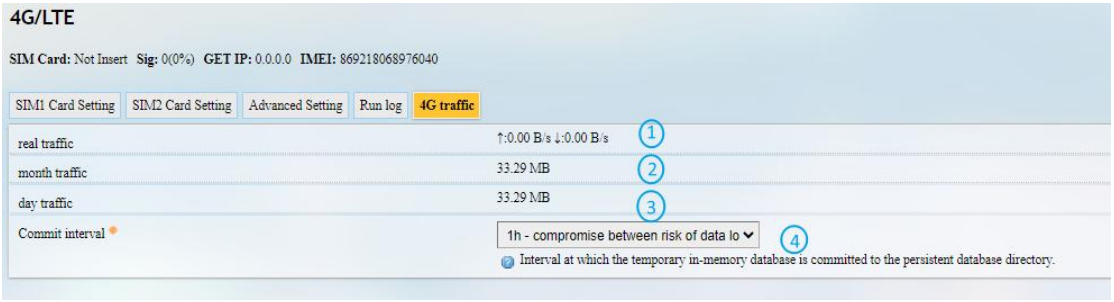
1. Click to restart the 4G module
2. Time interval for automatic restart of the 4G module when it is offline
3. Time interval for auto refresh of the cellular information

Be sure to save the settings before you exit the page.

The **Run Log** tab next to the **Advanced Setting** tab displays the last 50 log entries of the module.



Under the **4G traffic** tab, traffic information measured in real time or on the monthly and daily basis is available. You can also set the interval for submitting the temporary in-memory database to the persistent database directory.



Description of the numbered areas

1. Real-time traffic
2. Data used in the current month
3. Data used in the day
4. Time interval for submitting the temporary database to the persistent database

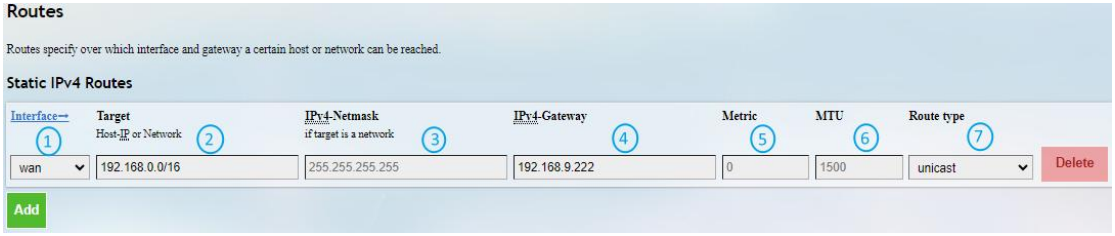
3.6.4 Static Routes

This is an advanced function allowing you to specify interface rules for route access.

Example:

Requirement: When the Router has both 4G and WAN network interfaces, the internal network (192.168.0.0 - 192.168.255.254) is accessed via the WAN port by the internal server. Other data access is realized via the 4G interface.

Click **Add** to set a new static route.



Description of the numbered areas

1. Select an interface to configure the route
2. Input the IP address of the host
3. Input the subnet mask (255.255.255.255 by default)
4. Input the address of IPv4 gateway
5. Gateway metric (The smaller the number, the higher the priority)
6. Set the MTU
7. Select a route type (refer to the details next page)

Be sure to save the settings before you exit the page.

Description of the route type:

Type	Description
Unicast	The route entry describes real paths to the destinations covered by the route prefix.
Local	The destinations are assigned to this host. The packets are looped back and delivered locally.
Broadcast	The destinations are broadcast addresses. The packets are sent as link broadcasts.
Multicast	IP datagrams are sent to a group of interested receivers in a single transmission. It is not present in normal routing tables.
Unreachable	The destinations are unreachable. Packets are discarded and the ICMP message of host unreachable is generated. The local senders will receive an EHOSTUNREACH error.
Prohibit	The destinations are unreachable. Packets are discarded and the ICMP message of communication administratively prohibited is generated. The local senders will receive an EACCES error.
Blackhole	The destinations are unreachable. Packets are discarded silently. The local senders will receive an EINVAL error.
Anycast	The destinations are any cast addresses assigned to this host. They are mainly equivalent to local with one difference that such addresses are invalid when used as the source address of any packet.

3.6.5 Firewall

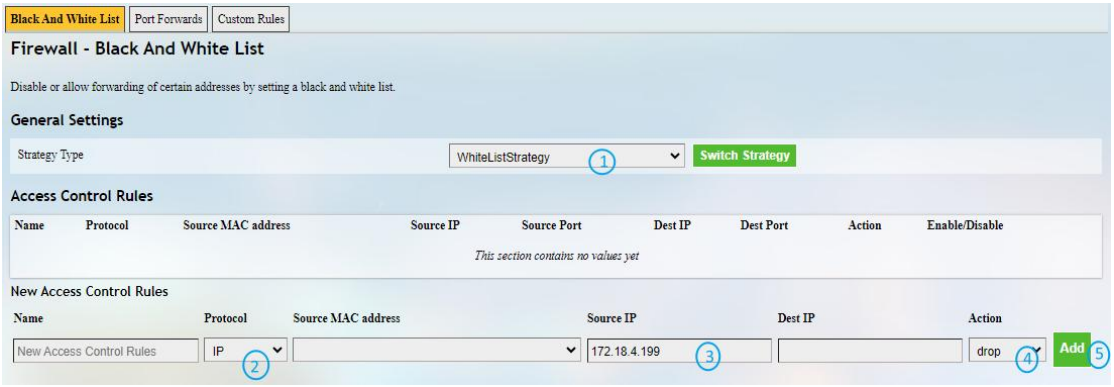
- **Black List and White List**

The black and white list feature allows you to enable/disable the forwarding of specific addresses.

White list policy: All addresses but those added to the **Access Control Rules** have the access

Black list policy: All addresses but those released to the **Access Control Rules** are blocked

Scenario 1: To block the internet access of 172.18.4.199

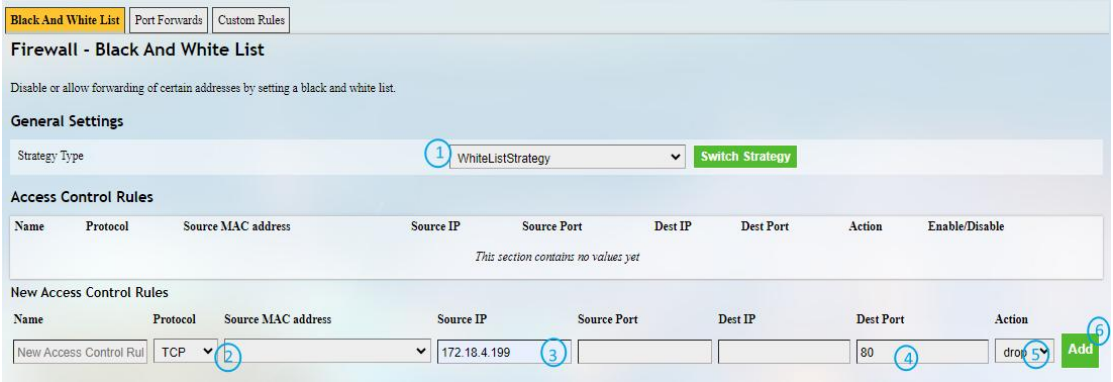


Description of the numbered areas

1. Select the white list strategy and click the button behind to switch to the strategy
2. Select the IP protocol
3. Input the source IP
4. Select ‘drop’ as the action for the target address
5. Click **Add** to add the address to the access control list

Be sure to save the settings before you exit the page.

Scenario 2: To block the TCP communication between 172.18.4.199 and the external network via port 80

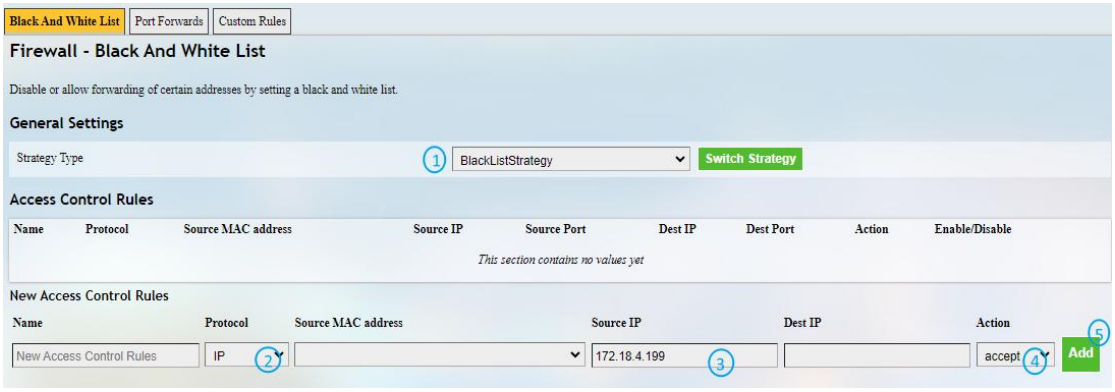


Description of the numbered areas

1. Select the white list strategy and click the button behind to switch to the strategy
2. Select the TCP protocol
3. Input the source IP
4. Input the destination port
5. Select 'drop' as the action for the target IP and port
6. Click **Add** to add the IP and port to the access control list

Be sure to save the settings before you exit the page.

Scenario 3: To release 172.18.4.199 for internet access

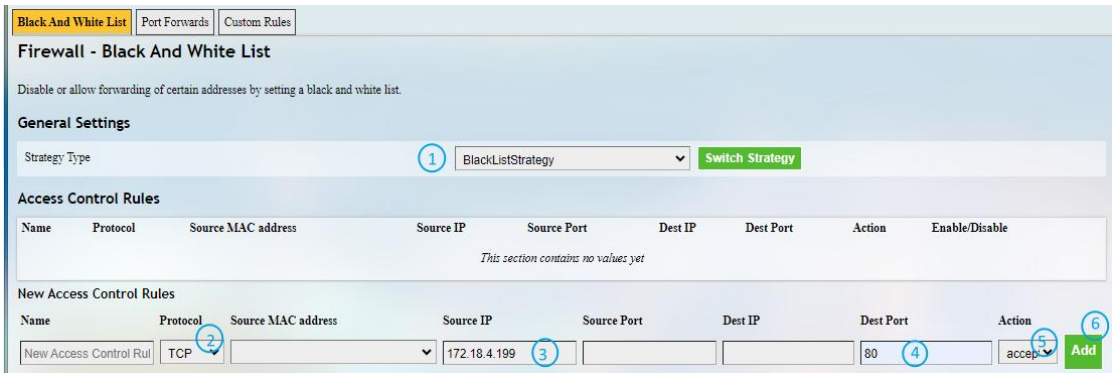


Description of the numbered areas

1. Select the black list strategy and click the button behind to switch to the strategy
2. Select the IP protocol
3. Input the source IP
4. Select 'accept' as the action for the target IP
5. Click **Add** to release the IP from the access control list

Be sure to save the settings before you exit the page.

Scenario 4: To allow the TCP communication between 172.18.4.199 and the external network via port 80



Description of the numbered areas

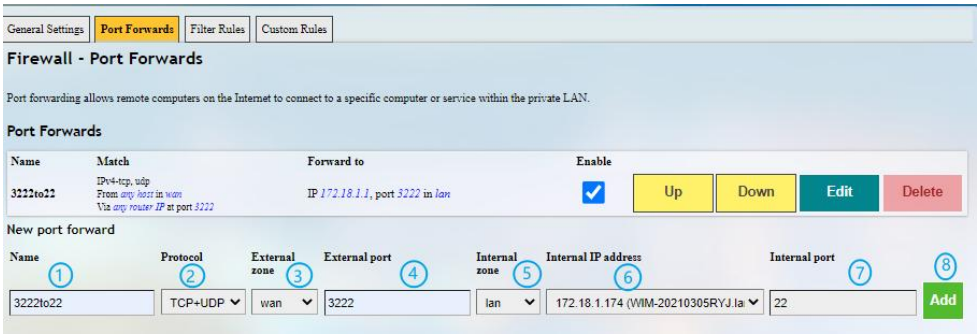
1. Select the black list strategy and click the button behind to switch to the strategy
2. Select the TCP protocol
3. Input the source IP
4. Input the destination port
5. Select 'accept' as the action for the target IP and port
6. Click **Add** to release the IP and port from the access control list

Be sure to save the settings before you exit the page.

- **Port Forwards**

The forwarding controls the traffic between zones and may enable MSS clamping for specific directions. Only one direction is covered by a forwarding rule. To allow bidirectional traffic flows between two zones, two forwarding setups are required with the dest ports reversed.

Example of port forwarding (To forward port 3222 of the WAN port to port 22 of the LAN host 172.18.1.174):

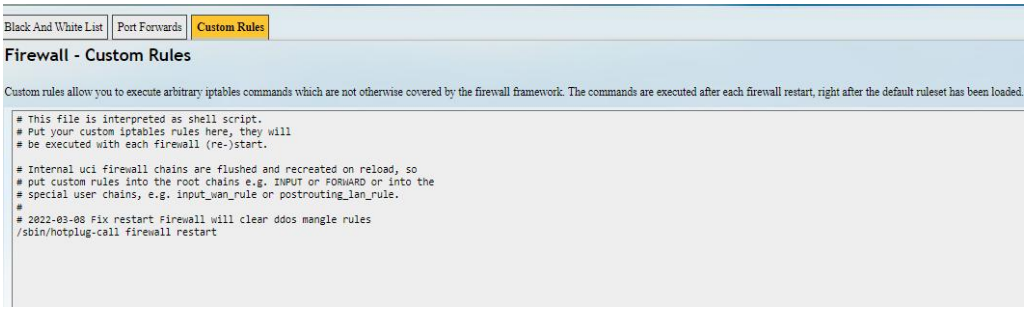


Description of the numbered areas

1. Rule name
2. Protocol (TCP/UDP/TCP + UDP are supported)
3. External zone: WAN
4. External port: 3222
5. Internal zone: LAN
6. LAN host: 172.18.1.174
7. Port number of the target host in the internal zone: 22
8. Add the rule (mandatory)

- **Custom Rules**

Custom rules allow you to execute arbitrary **iptables** commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default rule settings have been loaded.



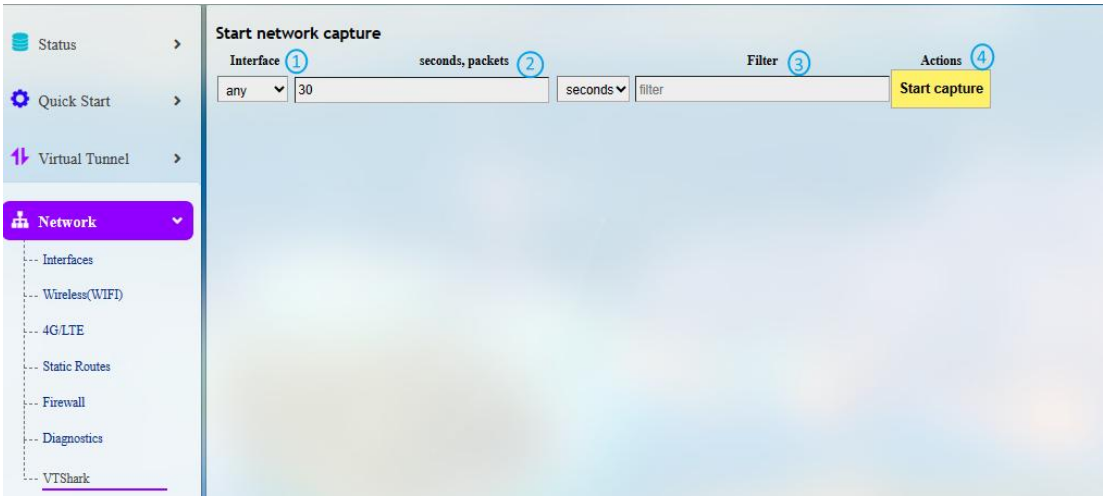
3.7 Diagnostics

Tools available in **Diagnostics** are explained below:

Tool	Description
Ping	To test the connectivity and measure the response time between the router and external IP addresses on the internet
Traceroute	To access information about the path that network traffic follows, including the number of hops and the response time of each hop
Nslookup	To query the Domain Name System (DNS) to obtain information about domain names, IP addresses, and DNS records

3.8 VTShark

The **VTShark** feature provides a flexible way to follow up and verify network issues. You can use wireshark to open and check the packets captured.



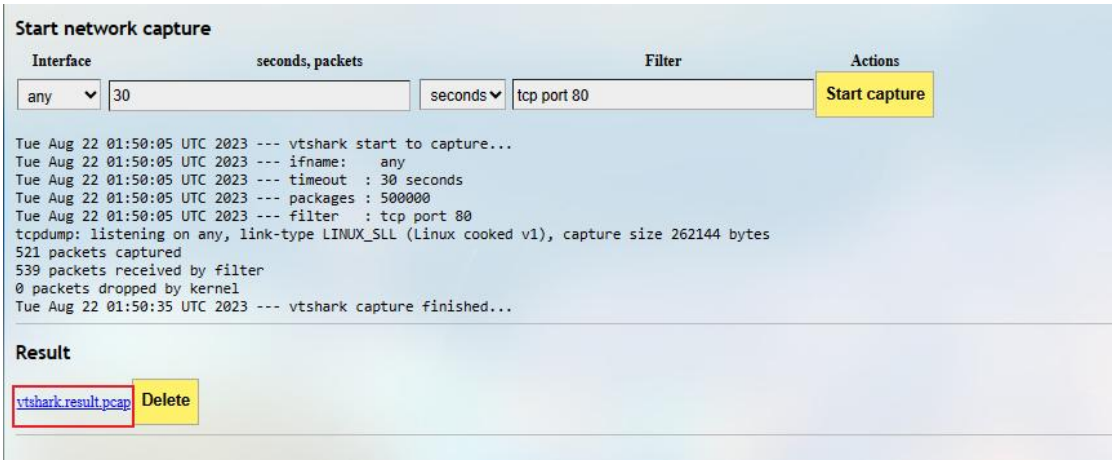
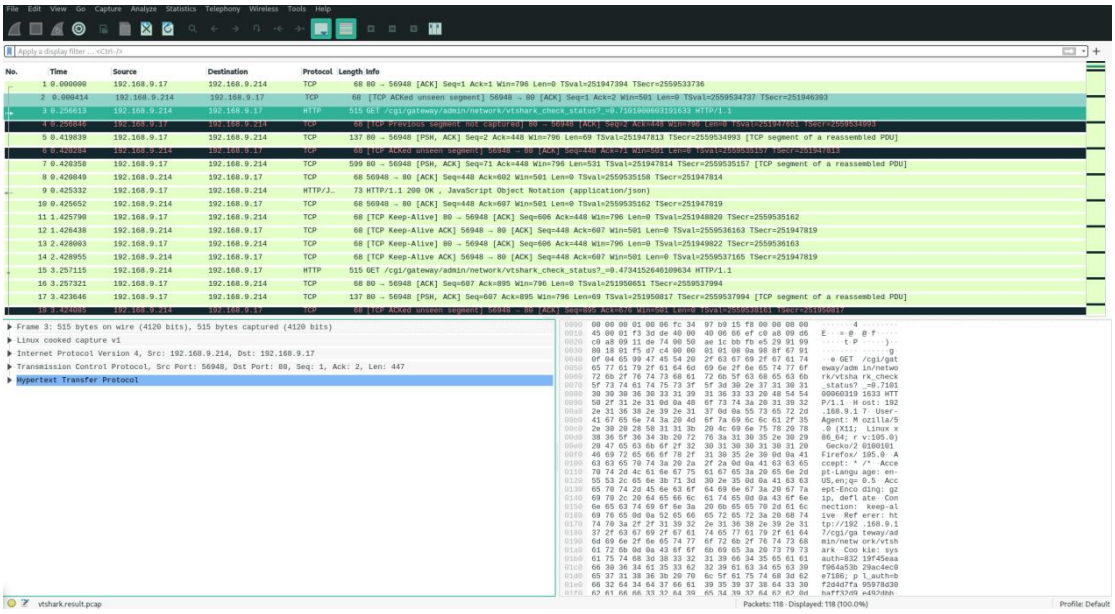
Description of the numbered areas

1. The interface from which the packets are captured (all interfaces are selected by default)
2. The measurement by which the data packets are captured (by seconds or by packet counts as explained below)
3. The filter for capturing the designated packets (more details are available at https://www.tcpdump.org/manpages/pcap-filter.7.html for advanced filtering)
4. Start the data capturing

Packets capturing by seconds and by packet counts:

Measurement	Description
Seconds	To specify a time duration for data capturing. For instance, you can input '10/20/30…' for the data capturing, which indicates that the capture will stop in 10/20/30 seconds.
	The system supports up to 500,000 packets for the time-based data capturing. The capture stops after reaching this limit, even if it has not reached the preset time duration.
Packets	To specify the count of packets for data capturing. For instance, you can input '100/200/500…' for the data capturing, which indicates that the capture will stop when 100/200/500 packets have been captured.
	The system supports up to 10 minutes (600 seconds) for the packet-based data capturing. The capture stops after reaching this limit, even if it has not reached the preset packet counts.

In the following scenario, the capture targets at all interfaces for the http packets from 'tcp port 80' for 30 seconds.



Clicking the result will download it to the local directory and you can open it with wireshark.