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	 Deleted Firewall zone related description as per design change; Added blacklist and whitelist description to the Firewall section. 	Apr. 4, 2023
V1.2	V200R003	 Modified Overview menu description; Deleted Quick Start for networking; Modified Auto routing description; Updated 4G/LTE description; Added Diagnostic description; Added IPSec setup description. 	Jul. 11, 2023
V1.3	V200R003	 Updated Product appearance diagram; Updated Ethernet port status indicator description; 	Dec. 5, 2023

Table of Contents

Forewo	ord	1
СНАРТИ	ER 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
CHAPT	ER 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
CHAPT	ER 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	
3.10 Customization	87
3.10.1 Custom Program	
3.10.2 IPK Installer	88
3.10.3 Manufacturer Info Customization	89
3.10.4 DMP Agent	90
3.11 Hardware	
3.11.1 Ser2TCP	91
3.11.2 Ser2net Environment Setup and Verification	91
3.11.3 Protocol comparison	97
3.12 Services	
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	
SSH Access	104
3.13.4 Terminal	106
3.13.5 Mount Points	107
3.13.6 Backup/Flash Firmware	
3.13.7 Reboot	112
3.14 Logout	
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 <u>www.vantrontech.com</u>.

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.

\triangle	Caution for latent damage to system or harm to personnel
Ì	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.
- \triangle 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
- A 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		
	Console	1 x Console for local configuration		
	Serial port	1 x RS485, isolated 1 x RS232, isolated		
I/Os	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		
	Dimensions	150mm x 115mm x 35mm		
	Enclosure	Metal		
	Installation	DIN rail mounting, panel mounting, wa	all mounting	
wechanical	IP rating	IP30		
	Drop test	6 ft. drop test		
	Cooling mode	Fanless		
Power	Input	9-36V DC, over-current protection, rev	verse polarity protection	
	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		
Software	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		
	Firewall	Supported (Stateful)		
Socurity	Access control	MAC address, IP address		
Security	Data security	PPTP, L2TP, GRE, IPSec, OpenVPN		
	Wi-Fi security	64/128-bit WEP, TKIP, WPA, WPA2, W	PA3, AES, WPS	
Favingereret	Temperature	Operating: -20°C~+60°C	Storage: -40°C~+70°C	
Condition	Humidity	Storage: RH 5%~95% (non-condensing)	
condition	Certification	FCC, IC, PTCRB, AT & T, Verizon, T-Mot	bile	

8

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 $0 \sim 2$ seconds will restart the Router.
- 2. A long press of the button for 3 ~ 6 seconds will factory reset the Router.
- 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



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	Туре	Description
1	RX		tyS1 COM1	I	RS232 receive signal
2	тх	/dev/ttyS1		0	RS232 transmit signal
3	232. GND			NC	RS232 isolated ground
4	485. GND			NC	RS485 isolated ground
5	А	/dev/ttyS2	52 COM2	I/O	RS485 A signal
6	В			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

14

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;



- 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: <u>http://172.18.1.1/)</u>.



- 2. For SSH login, use the LAN port IP address (default: <u>http://172.18.1.1/)</u>.
 - ° 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 <u>3.13.3</u> 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**.

System		
Here you can configure the basic aspects of your device like its hostname of	or the timezone.	
System Properties		
General Settings Logging Language and Style		
Language	auto	~
Design	XOS2	•

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 <u>3.10.4 DMP Agent</u> 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 <u>3.7</u> 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
- *b* 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.

Status	>	Auto Routing							
		Quick setting auto rou	ting for multi WAN						
🗘 Quick Start	~	Enable/Disable			Enable	~			
Auto Routing	_	Running Mode			Static Mode	~	(2)		
		Link Detect Policy			Detect Customize	d IP Addresses 🗸 🗸	3		
1 Virtual Tunnel	>								
A Network	>	Interface	Enable/Disable	Detect Gateway		Detect Customized IP Add Multiple IP Separated by space	s 6		7
		wan	Enable	✓ Disable	~	Factory default		v	Edit
Customization	>	cell0	Enable	✓ Disable	~	Factory default		~	Edit
Hardware	>	wwan0	Enable	✓ Disable	v	Factory default		~	Edit
O Services	>	Track Interface	Live Status 8						
😍 System	>	Active wan (<u>eth0.2</u> Online (tracking a) Standby cell0 (<u>4g-cell0</u>) cctive) Online (tracking active)	wwar Offlir	10 ne				
× Logout	>	Track Interface	log (9)						
		<pre><2023-08-17 03:4 <2023-08-17 03:4 <2023-08-17 03:4 <2023-08-17 03:4 <2023-08-17 03:4 <2023-08-17 03:4 <2023-08-17 03:4 <2023-08-17 03:4 <2023-08-17 03:4</pre>	9:17> 33 Notify event track 9:17> 33 Notify event track 9:17> 33 Notify event track 9:17> 33 Notify event online 9:17> 33 Notify event online 9:18> 33 Notify event linksw 9:26> 33 Notify event track	stop if wwar start if wan start if cell if cell if wan itch gw 192. start if wlar stop if wlar	0 dev wlan0 gw 19 dev eth0.2 gw 192 10 dev 4g-cell0 gw 10 dev 4g-cell0 gw dev eth0.2 gw 192 .168.19.222 10 dev wlan0 gw 19 n0 dev wlan0 gw 19	02.168.28.1 2.168.19.222 10.64.64.64 10.64.64.64 2.168.19.222 02.168.28.1 02.168.28.1			

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)	 The user-designated link priority takes precedence; If the user does not designate the link priority, the default rule will apply. 			
Dynamic mode	 The default rule governs the entire routing policy; 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)	 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"; 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.

Advanced Setting		
Interface		
Interface	wan	
Enable/Disable	Enable	 ✓ (1)
Metric *	10 Metric, Range:1-255	2
Count	3 @ times	3
Timeout	5 seconds	4
Interval	10 seconds	5
Detect Gateway	Disable	▲ 6
Detect Customized IP Addresses	Factory default Multiple IP Separated by spaces	· 🤊
Back or Refresh		8 Save & Apply Save Reset

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.

Status	'	OpenVPN Server		
Quick Start	>	openvpn server is not run! 12		
11 Virtual Tunnel	~	Local Time	1	Thu Aug 17 08:59:24 2023 • Sync with browser
OpenVPN Server	_	Enable	[
IPSEC		Proto	[TCP Server IPv4 3
VPN Client		Work mode	[tun [Working in route mode]
		Port	[1194 5
h Network	>	WAN DDNS or IP	[192.168.19.225 (eth0.2)
🕜 Users Manage	>	Client Network	[10.8.0.0 255.255.255.0 7
O Customization	>	Client Settings	[route 10 8 0 0 255 255 255 0
Hardware	>			comp-izo adaptive × 8 redirect-gateway def1 bypass-dhcp × 8
Services	>			dhcp-option DNS 10.8.0.0 * Set route 10.8.0.0 255.255.255.0 and dhcp-option DNS 10.8.0.0 base on your router
🚭 System	>	Extension Configuration		comp-lzo
🗙 Logout	>		(9)	
			L	(!)The Extension Configuration you would like to append to .ovpn file for openvpn client.
		OpenVPN Client config file	10	Download .ovpn file
				(1) Save & Apply Save Reset

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.

OpenVPN Server openvpn server is running----,the pid number: 23162

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.

Status	•	VPN Client					
		dial success IPv4: 10.8.0.1/255.255.255.0 Uptime:0h 2m 49s	RX: 0 B TX: 0 B the pid number:1	16301 (14)			
Quick Start	>						
1 Virtual Tunnel	~	Devices	Client	Provider	Server	Internet	
OpenVPN Server		Z D O		6.0			
VPN Client							
1 Martin				~	_		
INCLINETWORK	,	General Setting Run log					
🖉 Users Manage	>	Local Time		Mon Aug 28 05:59:19 2	2023 * Sync with browser	1	
Customization	>	WAN Protocol ·	2	openvpn	✓ Switcl	h Protocol 3	
		Enabled	4				
Hardware	>	Configuration Type	(5)	Use .ovpn file	~		
O Services	>	Upload .ovpn file	6	Choose local file:	Choose File No file chosen	Upload 7	
😴 System	>	Authentificate Mode	8	Use Certification	~		
		NTT	0	Opdate automatica	uty, please don't change it manually.		
× Logout	>	Marc	3	1300			
		De la companya de la comp					
		Peer intranet detection	(II)	disable Support multi IP, E	► E.g: 10.8.0.1 10.8.0.3		
		Use custom DNS servers	(12)		+		
		Back or Refresh					(13) Save & Apply Save Reset

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

VPN Client

dial success IPv4: 10.8.0.1/255.255.255.0 Uptime:0h 7m 4s RX: 0 B TX: 0 B the pid number:16301

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):

Status	,	IPSEC Status IPSEC	Setting					
- ouros		IPSEC Setting	IPSEC certificate	e manageme	nt			
Quick Start	>	IPSEC Connections Create Connection In Guide	x509ca informations					
🛿 Virtual Tunnel	~	IKE policy	ID Nan	ie	Filesize	Subject		Action
OpenVPN Server		Authentication Management	ID Name	Filesize	Subject	altNames	subjkey	Action
IPSEC		Secrets Management	private key informatio	ns				
VPN Client		Virutal IP Pools	ID Nan	ie	Filesize	subjkey		Action
	_	IPSEC Setting	public key information	s	Filerize	mbikar		Action
Network	>				TIRSIE	subjicy		
		menen	IPSEC Certificate Co	onfig	-			
Users Manage	>	IPSEC Running Status	X509 RootCA	Choose File	rootca.cert (1)			
Customization	>	Restort	X509 Certificate	Choose File	78.cert (2)			
		Reload	Public Key	Choose File	78.priv.key 3			
Hardware	>	Stop		бок	Cancel			
Services	>							
		UK	Auto generate o	ne pair of pri	vate and public k	ey		
5 System	>		Filename					
×				Generate				

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.

riva	te key informat	ions				
ID	Name	Filesize	subjkey	Action		
0	82.pub.key.pem	1675	78:4a:5a:9a:88:2e:13:2c:60:5d:96:ed:e7:35:d5:b8:9e:46:8a:02	2 Delete		
1	82.priv.key.pem	1679	30:7a:34:15:92:a4:b7:20:21:e9:6c:ae:a7:ea:3f:b9:70:a1:e4:82	Delete		
ıbli	c key informati	ons				
D	Name	Filesize	subjkey	Action		
0	82.pub.key.pem	451 75	8:4a:5a:9a:88:2e:13:2c:60:5d:96:ed:e7:35:d5:b8:9e:46:8a:02	Export Delete		
1	82.priv.key.pem	451 3	0:7a:34:15:92:a4:b7:20:21:e9:6c:ae:a7:ea:3f:b9:70:a1:e4:82	Export Delete		
IPS	EC Certificate	Config				
X50	9 RootCA	Choose File	e rootca.cert			
\$50	9 Certificate	Choose File	9 78.cert			
Priv	ate Key	Choose File	78.priv.key			
ubl	lic Key	Choose File	78.pub.key			
		OK	Cancel			
A Fi	uto generate lename ivate key informa	test 1 Generate	rivate and public key			
т	D Name	Filesize	subikey	Action		
(0 test.pem	3 1675	a7:ec:00:f6:d4:75:63:d6:eb:52:af:ab:b1:7e:cd:ae:40:50:32:4d	Delete		
	1 82.pub.key.pen	n 1675	78:4a:5a:9a:88:2e:13:2c:60:5d:96:ed:e7:35:d5:b8:9e:46:8a:02	Delete		
1	2 82.priv.key.pen	n 1679	30:7a:34:15:92:a4:b7:20:21:e9:6c:ae:a7:ea:3f:b9:70:a1:e4:82	Delete		
pu	blic key informa	tions				
I	D Name	Filesize	subjkey	Action		
() test.pem	451 a	17:ec:00:f6:d4:75:63:d6:eb:52:af:ab:b1:7e:cd:ae:40:50:32:4d	Export Delete		
1	82.pub.key.pem	451 7	8:4a:5a:9a:88:2e:13:2c:60:5d:96:ed:e7:35:d5:b8:9e:46:8a:02	Export Delete		

30:7a:34:15:92:a4:b7:20:21:e9:6c:ae:a7:ea:3f:b9:70:a1:e4:82

Description of the numbered areas

2 82.priv.key.pem 451

- 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

Export | Delete

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):

Status	,	IPSEC Status IPSEC	Setting				
- Status		IPSEC Setting	IPSEC secrets ma	inagement			
Quick Start	>	IPSEC Connections Create Connection In Guide	ID Enable	Name Auth	Identify(ID)	Secret Act	tion
1 Virtual Tunnel	~	IKE policy IPSEC policy	IPSEC Sec	crets Config			
OpenVPN Server	_	Authentication Management	Name	local_pwd			
IPSEC	_	Secrets Management Certificate Management	Enable	Enabled	~ (2)		
VPN Client		Virutal IP Pools	Secret Type	PSK(Pre-Shared Key)	~ (3)		
		IPSEC Setting	PSK ID []	192.168.9.78	(4)		
h Network	>		Secret	pwdtest	5		
11 Isers Manage	,	IPSEC Running Status		6 OK Cancel			

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):

Status	>	IPSEC Status IPSE	C Setting						
		IPSEC Setting	IPSEC s	secrets ma	nagement				
Quick Start	>	IPSEC Connections Create Connection In Guide	ID 0	Enable	Name local_pwwd	Auth psk	Identify(ID) 192.168.9.78	Secret pwdtest	Action Edit Delete
1 Virtual Tunnel	×	IPSEC policy	IPS	EC Sec	rote Cont	fia			
· OpenVPN Server		Authentication Management Secrets Management	Name	LC SR	remote_pv	vd		1	
VEN Client		Certificate Management	Enable		Enabled		~	2	
VPN Chem		IPSEC Setting	Secret T	Гуре	PSK(Pre-S	Shared Key)	~	3	
h Network	>		PSK ID Secret	0	192.168.9. testpwd	82		(4) (5)	
🖉 Users Manage	>	IPSEC Running Status			бок	Ca	ncel		

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.

IPSEC	secrets m	anagement				
ID	Enable	Name	Auth	Identify(ID)	Secret	Action
0	Ø	local_pwwd	psk	192.168.9.78	pwdtest	Edit Delete
1		remote_pwd	psk	192.168.9.82	testpwd	Edit Delete

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

Ctatus >	IPSEC Status IPSI	EC Setting		
Jiaius /	IPSEC Setting	IPSEC Setting		
Quick Start >	IPSEC Connections Create Connection In Guide	IPSEC Basic Setting		
1 Virtual Tunnel	IKE policy IPSEC policy	Enable 2 Log level Control		~
IPSEC	Authentication Management Secrets Management			
VPN Client	Virutal IP Pools IPSEC Setting 1	IPSEC Security Setting Enable Aggressive Mode For IKEV1 + PSK		
h Network >		IPSEC and IKE Proposals Configration		
🙋 Users Manage 🔷 🕨	IPSEC Running Status	IKE Proposals configrations		
C Customization >	Status: Stopped	aes128-sha1-prfsha1-modp2048 aes256-sha256-prfsha256-modp2048	Û	IKE NON-AEAD proposals Encryption Intergrity PRF DH Group
Hardware >	Reload Stop Start	· · · · · · · · · · · · · · · · · · ·	⇒	IKE AEAD proposals AEAD Encryption PRF DH Group
Services >	ОК			Add
🔮 System 🔹		IPSEC Proposals configrations		
× Logout >		aes128-sha1	Ų Ĥ	PSEC Non-AEAD proposals Encryption Integrity DH Group(PFS) PSEC AEAD proposals AEAD Encryption DH Group(PFS)
) DK	Add Cancel

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.

Status: 1	Running	
~		
Re	start	
Re	load	
St	p	
Sta	urt	
\smile		
-	OK	

STEP 2: IKE policy configuration

Configurations for scenarios 1 and 2:

G1 setup

Status	>	IPSEC Status IPSEC	C Setting				
		IPSEC Setting	IPSEC IKE Policy				
Quick Start	>	IPSEC Connections Create Connection In Guide	ID Enable	Name Version	local address	remote address	Action
1 Virtual Tunnel	*	IKE policy 1 IPSEC policy	IPSEC IKE	Policy Config			
OpenVPN Server		Authentication Management	Fushle	to_82			
IPSEC	-	Certificate Management	Local Address	Enabled 192.168.9.78	✓ (3)④		
	_	IPSEC Setting	Remote Address	192.168.9.82	5		
A Network	>		+ Advanced	6 OK Car	ncel		

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

Status	IPSEC Status IPSE	C Setting				
	IPSEC Setting	IPSEC IKE Policy				
Quick Start	IPSEC Connections Create Connection In Guide	ID Enable Nam 0 ☑ to_8	Version IKEv2+IKEv1	local address 192.168.9.78	remote address 192.168.9.82	Action Edit Delete
Virtual Tunnel OpenVPN Server	IPSEC policy Authentication Management	IPSEC IKE	Policy Config		0	
IPSEC	Secrets Management Certificate Management	Enable	to_78 Enabled	~	3	
···· vriv chem	Virutal IP Pools IPSEC Setting	Local Address Remote Address	192.168.9.82 192.168.9.78		(4) (5)	
A Network >		+ Advanced	6		Ŭ	
Users Manage >	IPSEC Running Status		ОК	Cancel		

- 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									
		PSEC Status	IPSEC Setting						
Status	IPS	EC Setting	IPSE	C IKE Poli	cy				
 Quick Start Virtual Tunnel 	> IPS Cro	EC Connections eate Connection In Gu	de 0	Enable Ø	Name to_82 to_78	Version IKEv2+IKEv1 IKEv2+IKEv1	local address 192.168.9.78 192.168.9.82	remote address 192.168.9.82 192.168.9.78	Action Edit Delete Edit Delete
OpenVPN Server	IPS Aut	EC policy thentication Manager	ient TF	SECI	KE P	licy Config			
IPSEC	- Sei	crets Management rtificate Management	Nar	ne	KL I	to_82		2	
U VPN Client	Vin	utal IP Pools	Ena	ble		Enabled	~	3	
	IPS	EC Setting	Loc	al Address		192.168.9.78		4	
the Network	>		Ren	note Address		192.168.9.82		(5)	
 Users Manage Customization Hardware Services System Logout 	PPSI Statu O	EC Running Status ar Running Restat Reload Stop Start OK		+ IKE Vers + IKE Prop - Virtual IP Select Your Virtual IP P	ion posals Pools Role cools	8 As a Responder selected	to,	silable 9	
A Program				+ Retry IK + rekey tim + reauthen + DPD(Dea + DSCP(Di + Encap UI + MOBIKE	E Negociat tication tin of Peer Det fferentiate DP E(RFC4555	e Times ection) d Services Code Point) - IKEx2 Mobility and	Multihoming Protoco	a)	

- 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

Status	,	IPSEC Status IPSE	CC Setting					
- Status		IPSEC Setting	IPSEC IKE Poli	cy				
Quick Start	>	IPSEC Connections Create Connection In Guide	ID Enable	Name to 82	Version IKEv2+IKEv1	local address 192.168.9.78	remote address 192.168.9.82	Action Edit Delete
1 Virtual Tunnel	~	IKE policy 1 IPSEC policy	1 🖉	to_78	IKEv2+IKEv1	192.168.9.82	192.168.9.78	Edit Delete
OpenVPN Server		Authentication Management	IPSEC I	KE Po	olicy Config			
IPSEC	_	Secrets Management	Name		to_78]/	2	
VPN Client		Virutal IP Pools	Enable		Enabled	*	3	
		IPSEC Setting	Local Address		192.168.9.82		4	
h Network	>		Remote Address		192.168.9.78		5	
🕑 Users Manage	,	IPSEC Running Status	- Advanced (+ IKE Vers	6) ion				
O Customization	>	Status: Running	+ IKE Prop - Virtual IP	osals				
Hardware	>	Reload Stop	Select Your	Role	8 As a Initiator	~]	
O Services	>	OK	+ Retry IKI	E Negociat	9 0.0.0.0 Times			
🚭 System	>		+ rekey tim + reauthent	e ication tin	16			
× Logout	>		+ DPD(Dea + DSCP(Di	d Peer Det fferentiate	ection) d Services Code Point)			
			+ Encap UI	OP				
			+ MOBIKE	(RFC4555	- IKEv2 Mobility and	Multihoming Protoco	1)	
					(10) ок	Cancel		

- 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

Status >	IPSEC Status	IPSEC Setting					
- otato	IPSEC Setting	IPSEC Policy Informa	tions				
Quick Start	IPSEC Connections Create Connection In Guide	ID I	nable Name	mode	local ts	remote ts	Action
1) Virtual Tunnel 🗸 🗸	IKE policy IPSEC policy	IPSEC Policy	Config				
OpenVPN Server	Authentication Management	Name	to_82	2			
IPSEC VPN Client	Secrets Management Certificate Management Virutal IP Pools	Enable Transport Mode	Enabled Tunnel	✓ ③✓ ④			
	IPSEC Setting	Local Address(Traffic Sele	tor) 192.168.9.78	5			
h Network		Remote Address(Traffic Se	lector) 192.168.9.82	6			
🕑 Users Manage 🔹 🔸	IPSEC Running Status	+ Advanced	7 ок	Cancel			

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

Status	IPSEC Status	IPSEC Setting					
Quick Start	IPSEC Setting IPSEC Connections	IPSEC Policy Informat ID E	tions Name	mode	local ts	remote ts	Action
Virtual Tunnel OpenVPN Server	IKE policy IPSEC policy Authentication Management	IPSEC Policy Name	7 Config				
IPSEC	Secrets Management Certificate Management Virutal IP Pools	Enable Transport Mode	Enabled	• 3 • 4			
A Network	IPSEC Setting	Local Address(Traffic Selec Remote Address(Traffic Sel	tor) 192.168.9.82 ector) 192.168.9.78	6)		
🕑 Users Manage 🔹 🕨	IPSEC Running Status	+ Advanced	Ок	Cancel			

- 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

Status	>	IPSEC Status	IPSEC Setting					
		IPSEC Setting	IPSEC Polic	y Informations				
Quick Start	>	IPSEC Connections Create Connection In Guide	ID	Enable	Name	mode	local ts	remote ts
11 Virtual Tunnel	*	IKE policy IPSEC policy	IPSEC	Policy Config				
OpenVPN Server		Authentication Management	Name		to_82_site	(2)		
IPSEC		Secrets Management	Enable		Enabled	~ 3)	
VPN Client		Certificate Management Virutal IP Pools	Transport Mo	de	Tunnel	~ (4)		
		IPSEC Setting	Local Address	(Traffic Selector)	172.18.2.1/24	(5)	
h Network	>		Remote Addre	ess(Traffic Selector)	172.18.3.1/24	6)	
🕑 Users Manage	>	IPSEC Running Status	+ Advance	đ	7 ок	Cancel		

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

Status >	IPSEC Status	IPSEC Setting					
	IPSEC Setting	IPSEC Poli	cy Informations				
Quick Start	IPSEC Connections Create Connection In Guide	ID	Enable	Name	mode	local ts	remote ts
1 Virtual Tunnel 🔹	IKE policy IPSEC policy	IPSEC	C Policy Config)			
OpenVPN Server	Authentication Management	Name		to_78_site	(2)		
IPSEC	Secrets Management	Enable		Enabled	v (3))	
VPN Client	Certificate Management Virutal IP Pools	Transport M	ode	Tunnel	~ (4))	
	IPSEC Setting	Local Addre	ss(Traffic Selector)	172.18.3.1/24	5)	
th Network		Remote Add	ress(Traffic Selector)	172.18.2.1/24	6)	
🖉 Users Manage 🔹 🔸	IPSEC Running Status	+ Advanc	ed	Ок	Cancel		

- 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

Statue	,	IPSEC Status IP	SEC Setting			
- Status		IPSEC Setting	IPSEC virtu	al ip address pools		
Ouick Start	>	IPSEC Connections Create Connection In Guide	ID	Enable	Name	Address
1 Virtual Tunnel	~	IKE policy	Virtua	l IP Address Po	ool config	
OpenVPN Server		Authentication Management	Name	to_82	Ū	2
IPSEC		Secrets Management	Enable	Enabled		✓ 3
VPN Client		Certificate Management Virutal IP Pools 1	Address	10.10.7.0/2	24	4
		IPSEC Setting		5 ок	Cancel	

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

Status	,	IPSEC Status	IPSEC Setting				
		IPSEC Setting	IPSEC Polic	y Informations			
Quick Start	>	IPSEC Connections Create Connection In Guide	ID	Enable	Name	mode	local ts
1 Virtual Tunnel	~	IKE policy IPSEC policy	IPSEC	C Policy Config			
OpenVPN Server		Authentication Management	Name		to_82_server	(2)	
IPSEC	_	Secrets Management	Enable		Enabled	v (3)	
VPN Client		Certificate Management Virutal IP Pools	Transport Mo	de	Tunnel	~ (4)	
-		IPSEC Setting	Local Addres	s(Traffic Selector)	10.10.7.2/24	5	
h Network	>		Remote Addr	ess(Traffic Selector)			
The stress of the second			+ Advance	d			
users Manage		IPSEC Running Status			бок	Cancel	

- 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

		Setting		
Status Status	,	Terminal		
Ouick Start	>	Terminal not run!		
4		Enable/Disable	disable 🗸	
Virtual Tunnel	,	Interface	disable enable	
network	>			
Licere Manage		Back or Refresh		Save & Apply Save Ret
Sers Manage	,			
Customization	>			
Hardware	>			
Services	>			
System	~			
System				
NBM Setting				
Administration				
Terminal				

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

Status	,	IPSEC Status	IPSEC Setting				
		IPSEC Setting	IPSEC Polic	y Informations			
Quick Start	>	IPSEC Connections Create Connection In Guide	ID	Enable	Name	mode	local ts
1 Virtual Tunnel	~	IKE policy IPSEC policy	IPSEC	Policy Config	ļ		
OpenVPN Server		Authentication Management	Name		to_78_client	(2)	
IPSEC		Secrets Management	Enable		Enabled	~ (3)	
VPN Client	_	Certificate Management Virutal IP Pools	Transport Mov	le	Tunnel	~ (4)	
		IPSEC Setting	Local Address	(Traffic Selector)			
h Network	>		Remote Addre	ess(Traffic Selector)	10.10.7.0/24	5	
-			+ Advance	d			
🖉 Users Manage	,	IPSEC Running Status			бок	Cancel]

- 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

Status	,	IPSEC Status IPSEC	C Setting
		IPSEC Setting	IPSEC Authentication Management
Quick Start	>	IPSEC Connections Create Connection In Guide	ID Enable Name Authentication Method Identify(ID) Key Action
1 Virtual Tunnel		IKE policy IPSEC policy	IPSEC Authentication Config
OpenVPN Server		Authentication Management 1	Name local_cert (2)
IPSEC		Secrets Management	Enable Enabled
		Certificate Management	
VPN Chent		Virutal IP Pools	
	_	IPSEC Setting	Authentication Method Certificate
h Network	>		Choose Certificates selected available
			A 79 port
🖉 Users Manage	>	IPSEC Running Status	70.0ert
O Customization	>	Status: Running	
Hardware	>	Reload Stop	OK 6 Cancel

- 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

Status	,	IPSEC Status	IPSEC Se	etting			
		IPSEC Setting		IPSEC Authentication	n Management		
Ouick Start	>	IPSEC Connections Create Connection In G	iuide	ID Enable	Name Authenti	cation Method	Identify(ID)
11 Virtual Tunnel	•	IKE policy IPSEC policy		IPSEC Authentic	ation Config		
		Authentication Manage	ement 1	Name	remote_cert	2	
h Network	`	Secrets Management Certificate Managemen	t	Enable	Enabled	v (3)	
🖉 Users Manage	>	Virutal IP Pools		ID			
		IPSEC Setting		Authentication Method	Certificate	~ (4)	
O Customization	>			Choose Certificates	selected	available	
Hardware	>	IPSEC Running Statu	s		*	78.cert	
Services	>	Status: Running					
System	>	Reload Stop			(6) ОК Саг	ncel	

Configurations of G1 for remote authentication

- 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

Status	,	IPSEC Status IPSI	EC Setting							
		IPSEC Setting	IPSEC A	uthentication	Management					
O Quick Start	>	IPSEC Connections Create Connection In Guide	ID	Enable N	ame	Authenticat	tion Method	Identify(ID)	Key Act	tion
1 Virtual Tunnel	~	IKE policy IPSEC policy	IPSEC	Authentica	ation Config					
OpenVPN Server		Authentication Management	1) Name		local_cert					
IPSEC	_	Secrets Management	Enable		Enabled		~ (3)			
VPN Client		Certificate Management Virutal IP Pools	ID							
		IPSEC Setting	Authenti	cation Method	Certificate		~ (4)			
h Network	>		Choose	Certificates	selected	1	available			
Users Manage	>	IPSEC Running Status				*	82.cert 5			
O Customization	>	Status: Running				*	,			
Hardware	>	Reload			ок 6	Cance	el			

- 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

Status	,	IPSEC Status	IPSEC S	etting			
		IPSEC Setting		IPSEC Authenticatio	n Management		
Quick Start	>	IPSEC Connections Create Connection In G	iuide	ID Enable	Name Authenti	ication Method	Identify(ID)
1 Virtual Tunnel	•	IKE policy IPSEC policy		IPSEC Authentic	ation Config		
		Authentication Manage	ement 1	Name	remote_cert	2	
h Network	`	Secrets Management Certificate Managemen	t	Enable	Enabled	~ (3)	
🖉 Users Manage	>	Virutal IP Pools		ID			
		IPSEC Setting		Authentication Method	Certificate	~ (4)	
O Customization	>			Choose Certificates	selected	available	
Hardware	>	IPSEC Running Statu	s		*	82.cert	
Services	>	Status: Running				0	
😴 System	>	Reload Stop			(6) ОК Са	ncel	

Configurations of G2 for remote authentication

- 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

Status	,	IPSEC Status IPSEC	Setting		
-		IPSEC Setting	IPSEC Authenticatio	on Management	
Quick Start	>	IPSEC Connections Create Connection In Guide	ID Enable	Name Authentication Method	Identify(ID) Key
1 Virtual Tunnel	•	IKE policy IPSEC policy	IPSEC Authenti	cation Config	
A Network	>	Authentication Management Secrets Management Certificate Management	Name Enable	Iocal_cert Enabled	2 3
🕼 Users Manage	>	Virutal IP Pools IPSEC Setting	ID Authentication Method	192.168.9.78	(4) (5)
C Customization	>		preshared key	need to set preshared key? goto 'secrets managemen'	add your secrets.
Hardware	>	IPSEC Running Status		6 OK Cancel	

- 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)

SEC	secrets ma	nagement				
ID	Enable	Name	Auth	Identify(ID)	Secret	Action
0		local_pwwd	psk	192.168.9.78	pwdtest	Edit Delete
1	R	remote pwd	psk	192.168.9.82	testowd	Edit Delete

- 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

Status	,	IPSEC Status IPSEC	Setting			
- Status		IPSEC Setting	IPSEC Authentication	n Management		
O Quick Start	>	IPSEC Connections Create Connection In Guide	ID Enable Nat	me Authentication Method	Identify(ID) Key	Action
11 Virtual Tunnel	•	IKE policy IPSEC policy	IPSEC Authentic	cation Config		Lui Duit
th Network	>	Authentication Management 1 Secrets Management Certificate Management	Name	remote_cert	2	
🕻 Users Manage	>	Virutal IP Pools IPSEC Setting	ID	Enabled 192.168.9.82	 ✓ (3) ✓ (4) 	
Customization	>		Authentication Method preshared key	PSK(Pre-Shared Key) need to set preshared key? goto 'secrets manage	▼ 5 gement' add your secrets.	
Hardware	>	IPSEC Running Status		OK 6 Cancel		

- 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)

EC	secrets ma	nagement				
D	Enable	Name	Auth	Identify(ID)	Secret	Action
0		local_pwwd	psk	192.168.9.78	pwdtest	Edit Delete
1		remote pwd	psk	192.168.9.82	testpwd	Edit Delete

- 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

Status	•	IPSEC Status	IPSEC S	ietting						
Onick Start	,	IPSEC Setting		IPSEC Authenticatio	n Management					
- Quick Start		Create Connection In (Guide	ID Enable	Name	Authentication Me	thod	Identify(ID)	Key	Action
1 Virtual Tunnel	Ľ	IKE policy IPSEC policy		IPSEC Authentic	ation Config					
OpenVPN Server		Authentication Manag	gement 1	Name	local_cert		2			
IPSEC	_	Secrets Management		Enable	Enabled		v (3)			
VPN Client		Virutal IP Pools		ID	192.168.9.82		(4)			
	_	IPSEC Setting		Authentication Method	PSK(Pre-Shared	d Key)	▼ 5			
h Network	>	-		preshared key	need to set preshare	ed key? goto 'secrets m	anagement' add your se	ecrets.		
🕑 Users Manage	>	IPSEC Running State	us		6 ок	Cancel				

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

Status	,	IPSEC Status	IPSEC S	etting		
		IPSEC Setting		IPSEC Authenticatio	n Management	
Quick Start	>	IPSEC Connections Create Connection In Gui	de	ID Enable Na 0 ☑ local	ne Authentication Method _cert PSK(Pre-Shared Key)	Identify(ID) Key Action 192.168.9.82 Edit Delete
11 Virtual Tunnel	~	IKE policy				
OpenVPN Server		Authentication Managen	nent (1)	IPSEC Authentic	ation Config	
IPSEC		Secrets Management		Name	remote_cert	
VPN Client		Certificate Management Virutal IP Pools		Enable	Enabled	✓ ③
		IPSEC Setting		ID	192.168.9.78	
th Network	>			Authentication Method	PSK(Pre-Shared Key)	 ✓ (5)
				preshared key	need to set preshared key? goto 'secrets manag	ement' add your secrets.
Users Manage	>	IPSEC Running Status			6 OK Cancel	

- 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

Status	,	IPSEC Status	IPSEC Se	etting			
		IPSEC Setting		IPSEC Authentication	on Management		
Quick Start	>	IPSEC Connections Create Connection In G	Juide	ID Enable	Name Authent	cation Method	Identify(ID)
1 Virtual Tunnel	>	IKE policy IPSEC policy		IPSEC Authenti	cation Config		
		Authentication Manag	ement (1)	Name	local_cert	0	
r Network	>	Secrets Management Certificate Managemen	ıt	Enable	Enabled	▼ 3	
🖉 Users Manage	>	Virutal IP Pools		ID			
		IPSEC Setting		Authentication Method	Public Key	~ (4)	
O Customization	>			Choose public keys	selected	available	
Hardware	,				*	82.pub.key 78.pub.key 5	
O Services	>					-	
🔮 System	>				6 ок Са	ncel	

- 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

Status	,	IPSEC Status IPSEC	C Setting	
- Callor		IPSEC Setting	IPSEC Authentication Management	
Quick Start	>	IPSEC Connections	ID Enable Name Authentication Method Identify(ID) Key	Action
1 Virtual Tunnel	>	Create Connection In Guide IKE policy IPSEC policy	0	Edit Delete
h Network	>	Authentication Management	Name remote_cert 2	
🕑 Users Manage	>	Virutal IP Pools IPSEC Setting	Enabled (3)	
Customization	>		Authentication Method Public Key Choose public keys selected available	
Hardware	>	Concession in the local division of the loca	78 pub.key 82 pub.key	
Services	>			
🔮 System	>		©OK Cancel	

- 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

Status	>	IPSEC Status IPSEC S	Setting			
Quick Start	>	IPSEC Setting IPSEC Connections Create Connection In Guide	IPSEC Authentication	n Management	ation Method	Identify(ID)
1 Virtual Tunnel	>	IKE policy IPSEC policy	IPSEC Authentic	ation Config		
A Network	>	Authentication Management Secrets Management Certificate Management	Name Enable	local_cert Enabled	2 • 3	
🕑 Users Manage	>	Virutal IP Pools IPSEC Setting	ID Authentication Method	Public Key	✓ ④	
O Customization	>		Choose public keys	selected	available	
Hardware	>				82.pub.key 5	
© Services	>					
😴 System	>			6 OK Can	cel	

- 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

Status	,	IPSEC Status IPSEC	Setting
- Otatus		IPSEC Setting	IPSEC Authentication Management
Quick Start	>	IPSEC Connections	ID Enable Name Authentication Method Identify(ID) Key Action
1 Virtual Tunnel	•	Create Connection In Guide IKE policy IPSEC policy	0 🖂 local_cert Public Key 82. pub.key Edit Delete
A Network	>	Authentication Management 1 Secrets Management	Name remote_cert (2)
Users Manage	>	Virutal IP Pools IPSEC Setting	Enable California Cali
Customization	>		Authentication Method Public Key (4)
Hardware	,		selected available available block selected block s
O Services	>		
🔮 System	>		GOK Cancel

- 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

G1	setup	
~	Jerah	

Status	>	IPSEC Status IPSEC	Setting					
		IPSEC Setting	IPSEC Connections					
Quick Start	>	IPSEC Connections 1 Create Connection In Guide	ID Enable Name	IKE Policy Local Authe	entication	Remote Authentication	IPSEC Policy	Action
11 Virtual Tunnel	~	IKE policy IPSEC policy	IPSEC Conn	ection Config		~		
OpenVPN Server		Authentication Management	Name	to_82		(2)		
IPSEC		Secrets Management	Enable	Enabled	~	3		
- HOLC	-	Certificate Management	IKE Policy			ã		
L VPN Client		Virutal IP Pools	ind i oncy	to_82	~	4		
		IPSEC Setting	Local Authentication	selected	availa	ble		
h Network	>			*	local_cert remote_cert	() [^]		
Users Manage	,	IPSEC Running Status		•		.		
O Customization	>	Restart	Remote Authentication	selected	availa	ble		
Hardware	>	Reload Stop Start			remote_cert	6		
O Services	>	ок		-		-		
🔮 System	>		IPSEC Policy	selected	availa to_82	ble		
× Logout	>							
				*		Ŧ		
				ОК 🚷 Са	ncel			

- 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

Status	,	IPSEC Status IPSEC	C Setting					
		IPSEC Setting	IPSEC Connections					
Ouick Start	>	IPSEC Connections 1 Create Connection In Guide	ID Enable Name	IKE Policy Local Auther	ntication	Remote Authentication	IPSEC Policy	Action
1 Virtual Tunnel	~	IKE policy IPSEC policy	IPSEC Conn Name	ection Config		2		
		Secrets Management	Enable			3		
IPSEC	- 1	Certificate Management	WE Deline	Enabled				
L VPN Client		Virutal IP Pools	IKE Policy	to_78	~	(4)		
		IPSEC Setting	Local Authentication	selected	availat	ole		
h Network	>			-	local_cert remote_cert	5		
Users Manage	>	IPSEC Running Status				*		
Customization	>	Restart	Remote Authentication	selected	availat	ole		
Hardware	>	Reload Stop Start			remote_cert	6		
O Services	>	ОК		•		•		
😍 System	>		IPSEC Policy	selected	to_78	ole		
× Logout	>							
				· · · · · · · · · · · · · · · · · · ·		*		
				OK 🛞 Can	ncel			

- 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

I SEC Status	20 Secting				
IPSEC Status	IPSEC connection lists	informations			
connection list	ID IKE Name	local address	remote address	Version	Action
connection details	0 to_82	192.168.9.78	192.168.9.82	IKEv1/2	Up Down
IPSEC policy status	ID IPSEC tunnel	local ts	remote ts	mode	
certificate list virtual ip pools	1 to_82	172.18.2.0/24	172.18.3.0/24	TUNNEL	2Up Down
IPSEC configrations					

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.

IPSEC Status	IPSEC Setting						
IPSEC Status	IPSI	C connection lists info	rmations				
connection list connection details IPSEC policy status certificate list	ID 0	IKE Name to_82 ID IPSEC tunnel	local address 192.168.9.78 local ts	remote address 192.168.9.82 remote ts	Version IKEv1/2 mode	Action Up	Down
virtual ip pools IPSEC configrations		1 to_82	172.18.2.0/24	172.18.3.0/24	TUNNEL	Up	Down
IPSEC logs	IPSI	C IKE sas					
	ID	IKE Name	local address	remote address	Ve	rsion	Action
	1	to_82 IPSEC tunnel	192.168.9.78 local ts	192.168.9.82 remote ts	IK. mo	Ev2 ode	Down
		to_82-13	172.18.2.0/24	172.18.3.0/24	т	JNNEL	Down

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**.

Overview 1			
VPN	VPN server	Uptime: 0h. 26m: 47a MAC-Address: 02:0C:29::A3:9B:6D RX: 5.53 KB (178 Pits.)	Restart Edit
aub0		TX: 41.68 KB (326 Pkti) IPv4: 192.168.43.100/24	
LAN	LAN	Uptime: 0h 26m 55s MAC-Address: 189B:A5:16:14:13 DX: 1.26.108 (2016): Blen. 1	Restart Edit
an (ter) tr-lan		TX: 2.52 http://doi.org/10.1011/001111/00111111111111111111111	(6
CELL0	4G	Uptime: 0h 1m 52s MAC-Address: 60:00:00:00:00 DVX 5:01 # 20 # 20 # 20	Restart Edit
4g-cell0		TX 328 (Phts) TX 328 (Phts) IPv4: 10.104.205.108/32	
VPNCLI	VPN client	RX: 0 B (0 Plets.)	Restart Edit
<u>}≉</u> tap0		TX: 0 B (0 Picts.)	
WAN	WAN	Uptime: 0h 26m 52a MAC-Address: 18:9B-A5:16:14:14	Restart Edit
eth0.2		RK 300 (ab (1)346 FRB.) TK 931.7 KB (537 FRB.) IPv4: 192.168.19.225/24	
WWAN0	Wi-Fi client	Uptime: 0h 26m 42s MAC-Address: B8513:32:74:7B:3E PV: 06.52D (200 Ptm.)	Restart Edit
Client "vantrop test\$ 5	50°	TX: 30.25 KB (422 Plta) IPv4: 192.168.28.101/24	4

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.

Interfaces - LAN	
On this page you can configure the network interfaces. You can bridge several i	sterfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use
<u>VLAN</u> notation INTERFACE.VLANNR (e.g. eth0.1).	
Common Configuration	
General Setup Advanced Settings	
Status	(1) Device: br-lan Uptime: 24h 4m 10s MAC: 7:4D:183:9:117:22 RX: 164.29 MB (652113 Pkts.) TX: 105 GB (106694 Pkts.) IPv4: 172.18.1
Protocol	Static address
IPv4 address	2 172.18.1.1
IPv4 netmask	3 255 255 255.0 🗸

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:

Status	>	Interfaces - LAN					
		On this page you can configure the network interfaces. You can bridge several interfaces by toking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use <u>VLAN</u> notation INTERFACE VLANIN (e.g., etho. 1).					
Quick Start	>	Common Configuration					
11 Virtual Tunnel >	General Setup Advanced Settings Physical Settings						
	Override MAC address	18:9B:A5:16:14:13					
A Network	*	Override MTU	1500	2			
Interfaces	_	Use gateway metric	0	3			
Wireless (UTED)							

- 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.

Interfaces - LAN	
On this page you can configure the network interfaces. You can bridge several interfa	ces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use
VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).	
Common Configuration	
General Setup Advanced Settings Physical Settings	
Bridge interfaces	Creates a bridge over specified interface(s)
Enable <u>STP</u>	 Enables the Spanning Tree Protocol on this bridge
Interface	Ethernet Adapter: "erspan0" Ethernet Switch: "eth0" String Switch VLAN: "eth0.1" (lan) String Switch VLAN: "eth0.2" (van) V Wireless Network: Master "Vantron-237CA6" (lan) Custom Interface:

- 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:

DHCP Server	
General Setup Advanced Settings	
Ignore interface	Disable <u>DHCP</u> for this interface.
Start	 100 Lowest leased address as offset from the network address.
Limit	 150 Maximum number of leased addresses.
Lease time	 12h ② Expiry time of leased addresses, minimum is 2 minutes (2m).

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:

DHCP Server	
General Setup Advanced Settings	
Dynamic <u>DHCP</u>	 Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.
Force	Force DHCP on this network even if another server is detected.
IPv4-Netmask	Override the netmask sent to clients. Normally it is calculated from the subnet that is served.
DHCP-Options	 Define additional DHCP options, for example "6, 192.168.2.1, 192.168.2.2" which advertises different DNS servers to clients.

- 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.

Interfaces - WAN	
On this page you can configure the network interfaces. You can bridg	several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use
VIAN notation INTERFACE.VLANNR (e.g. eth0.1).	
Common Configuration	
General Setup Advanced Settings	
Starus	(1)
Protocol	DHCP client V
Hostname to send when requesting DHCP	3 VantronOS-B4A7

- 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.

On this page you can configure the network interfaces. You can bridge several interfaces by tic	ting the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use <u>VILAN</u> notation INTERFACE.VL4WIR (<u>e.g.</u> ; etr0.1).
Common Configuration	
General Setup Advanced Settings Physical Settings Firewall Settings	
Bring up on boot	 Image: A set of the set of the
Force link	 Image: Set instrace properties regardless of the link currier (If set, currier sense events do not invoke hotphag handlets).
Use default gateway	 If unchecked, no default route is configured
Use DNS servers advertised by peer	 If unchecked, the advertised DNS server addresses are ignored
Use gateway metric	5 10
Override MAC address	6 18:9B:A5:16:14:14
Override MTU	7 1500
Back or Refresh	Save & Apply Save Reset

- 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**.

Interfaces - WAN	
On this page you can configure the network interfaces. You can bridge several interfaces by t	ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use <u>VLAN</u>
notation INTERFACE.VLANNR (e.g.: eth0.1).	
Common Configuration	
General Setup	
Status	Device: eth0.2 Uptime: 0.1 im 31.8 Uptime: 0.8 im 31.8 Uptime: Uptime: Uptime: Uptime: Uptime: Uptime: Uptime: Uptime: Uptime: Uptime:
Protocol	Static address
Really switch protocol?	Switch protocol

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

Interfaces - WAN	
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge	interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VI.AN notation INTERFACE. VLANNR (e.g., eth0.1).
Common Configuration	
General Setup Advanced Settings Physical Settings Firewall Settings	
Status	201 Derice: etb0.2 Uptime: 0h 50m 3a Derice: 201 MAC: 1890-263:164:14 RX: 5593.MB (31584-Pfm.) TX: 1753.MB (9818-Pfm.) IPvet: 192.168.19.225
Protocol	Static address
IPv4 address	192.168.19.54
IPv4 netmask 3	255.255.255.0
IPv4 gateway (4)	192.168.19.222
IPv4 broadcast	
Use custom DNS servers 5	192.168.19.28
DNS Rebinding	
Rebind protection 6	Perfused to parse private address packets
DHCP Server General Setup	
Ignore interface	Duable DHCP for this interface.
Back or Refresh	8 Save & Apply Save Reset

- 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.

Interfaces - WAN	
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge	interfaces" field and enter the names of several network interfaces separated by spaces. You can also use <u>VLAN</u> notation INTERFACE. VLANNR (e.g., eth0.1).
Common Configuration	
General Setup Advanced Settings Physical Settings Firewall Settings	
Bridge interfaces	creates a bridge over specified interface(s)
Interface	Image: State Adapter: "4g-cell0" (cell0) Image: State Adapter: "4g-cell0" (CER) Image: State Adapter: Tage Ad

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.

Interfaces - WAN	
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interface	" field and enter the names of several network interfaces separated by spaces. You can also use <u>VLAN</u> notation INTERFACE, VLANNR (e,g.; eth0, 1).
Common Configuration	
General Setup Advanced Settings Physical Settings Firewall Settings	
Create / Assign firewall-zone	Inn: Inn:200
0	vpa: (emp())
۲	wan: vpncli: 🧾 wwan0: 🛬 cell0: 🛃 wan: 🗯
0	unapocified-or-create:
() Cî de	cose the firewall zone you want to assign to this interface. Select usepscifted to remove the interface from the associated zone or fill out the create field to ine a new zone and attach the interface to it.

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)

-	Wireless(WIFI)				
	WIFI Settings				
 manufact manufact 	General Setting Advanced Setting				
Course 1	Status		Mode: Master SSID: Vantron-2B8892 BSSID: 0C:CF:89:2B:88:92 Encryption: m Channel: 1 (2.412 GHz) Tx-Power: 20 dBs Signal: -37 dBm Noise: -95 dBm Bitrate: 300.0 Mbits Country: US	nimed WPA/WPA2 PSK (CCMP)	
📩 Network 🗸 🗸	WIFI mode		AP	Switch Mode	
-	SSID	1	Vantron-2B8892		
Wireless(WIFI)	Channel	2	1(2412MHz)	~	
	Encryption	3	WPA-PSK/WPA2-PSK Mixed Mode	~	
	Cipher	4	Force CCMP (AES)	~	
	Key	5		a	
	Associated Stations				
	Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
•	(Master "Vantron-2B8892") 6	D6:A2:A0 **	172.1	al -37 / -95 dBm	65.0 Mbit/s, 0MHz 65.0 Mbit/s, 0MHz
	Back or Refresh				Save & Apply Save Reset

- 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)

Wireless(WIFI)			
WIFI Settings			
General Setting Advanced Sett	ting		
Enable Disable WIFI		1	Disable WIFI
WIFI Frequency		2	2.4G Switch Frequency 3
Network		4	VPN: cell0: inn: pmch: pmch: wan : create: create: @ Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.
Associated Stations			
Network	MAC-Address		Host Signal / Noise
			No information available

- 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.

Wireless(WIFI)			
WIFI Settings			
General Setting Advanced Setting			
Status	SSID: ? Mode: undefined 0% Wireless is disabled or not a	sociated	
WIFI mode	Client	Switch Mode	1
Protocol ·	DHCP	~	2
	Default DHCP, if the WIFI ad	cess point needs to specify IP, please	select Static
Wifi Client Setting			
Select SSID * 3	Mac/Bssid 🍍 🕢		Key 🔹 🕤
62% ; vantron_test8_5G 🗸	Auto		~
Scan WIFI			

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.

Wireless(WIFI)			
WIFI Settings			
General Setting Advanced Setting			
Status	Mode: Client SSID BSSID: 68:77:24:38 Channel: 48 (5.240) 62% Signal: -66 dBm N Bitrate: 260.0 Mbit/	0: vantron_test8_5G :4C:A8 Encryption: WPA2 PSF GHz) Tx-Power: 20 dBm ioise: -90 dBm is Country: 00	(CCMP)
WIFI mode	Client	✓ Switcl	h Mode
Protocol *	DHCP	~	
	Default DHCP, if the V	WIFI access point needs to specify	r IP, please select Static
Wifi Client Setting			
Select SSID *	Mac/Bssid 🍍		
62% ; vantron_test8_5G	Auto		*
62% ; vantron_test8_5G	Auto		

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.

Wireless(WIFI)			
WIFI Settings			
General Setting Advanced	Setting		
Status		SSID: ? Mode: undefined 0% Wireless is disabled or not associated	
WIFI mode		AP+Client	Switch Mode
SSID		Vantron-747B3E	2
Channel		1(2412MHz)	 ✓ ③ Wi-Fi AP settings
Encryption		WPA-PSK/WPA2-PSK Mixed Mode	• 4
Cipher		Force CCMP (AES)	 ✓ (5)
Key			2 6 6 C
Wifi Client Setting			
Select SSID *	0	Mac/Bssid	Key Wi-Fi client settings
62% ; vantron_test8_5G	Ø	Auto	
Scan WIFI No connectio	n		
Associated Station	15		
Network	MAC-Address	Host	Signal / Noise
		No information available	

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.

Wifi Client Setting				
Select SSID *	Mac/Bssid *			Key •
62% ; vantron_test8_5G	✓ Auto		✔ 12345678	
Scan WIFI Connected: 0h 0m 57s IPaddr: 192.168.28.108				
Associated Stations				
Network		MAC-Address	Host	Signal / Noise
@ Client "vantron_test8_5G" (wlan0)		68:77:24:38:4C:A8	?	📶 -67 / -92 dBm
👷 Master "Vantron-747B3E" (wlan1)		CE:76:F9:F2:E7:E8	?	ali -37 / -92 dBm

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.

G/LIE M Card: Ready Sig	g: 31(100%) GET IP	: 10.147.122.79 IM	EI: 869218	068976040	Ð	
IMI Card Setting	SIM2 Card Setting	Advanced Setting	Run log	4G traffic		
Enable/Disable					enable 🗸	3
CID Value					1	(4)
					[2] CID, default:1	0
PDP Type					IPV4 Only	6
					PDP Type: ALL or IPV4_Only or IPV6_Only	9
APN 🧧					cmnet	6
Dial number					*99#	$\overline{0}$
PAP/CHAP username					your_usemame	8
PAP/CHAP password						20
					Uptime: Öh 2m 17s RX: 304 B (7 Picts.) TX: 328 B (8 Picts.) IPv4: 10.147.122.79	
Register Status:					Register Home	
Register Type:					LTE	
Register Network:					CHINA MOBILE(46000)	
Mo <mark>d</mark> em Firmware:					EC200ACNDAR01A07M16	
Device node:					Quectel EC200A	
SIM is using:					siml	
SIM1 Card State:					Inserted	
SIM1 Card IMSI:					460008001191840	
SIM1 Card ICCID:					89860061221602B41840	
SIM2 Card State:					Not Insert	
SIM2 Card IMSI:						
SIM2 Card ICCID:						

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
- \triangleright 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.

4G/LTE							
SIM Card: Not Inser	t Sig: 0(0%) GET I	P: 0.0.0.0 IMEI: 869	218068976	5040			
SIM1 Card Setting	SIM2 Card Setting	Advanced Setting	Run log	4G traffic			
Restart Module					Re-power	1	
Redial Interval					600	2	
Cellular Info Fresh Interval						3	

- 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.

4G/LTE

SIM Card: Not Inser	t Sig: 0(0%) GET I	P: 0.0.0.0 IMEI: 86	921806897	j040					
SIM1 Card Setting	SIM2 Card Setting	Advanced Setting	Run log	4G traffic					
Last 50 track	log entries. New	est entries sort	ed at the	end :					
[2023:08:21 10:	55:36] INFO [cell	ulard]: cell0 req	uest mode	n initial:	ze: not nee	d			
[2023:08:21 10: [2023:08:21 10: [2023:08:21 10:	55:36] WARNING [Ce 55:36] INFO [Cell 55:36] WARNING [Ce	llulard]: cell0 r ulard.settings]: llulard.settings]	eload con package : cellul	ig wwan wan inter ar advance	face=cell0.	uci mtu not	t exist		
[2023:08:21 10: [2023:08:21 10:	55:36] WARNING [ce 55:37] INFO [cell	llulard.settings] ulard]: serial po	: cellul rt /dev/t	ar_advance SyUSB1 cre	d_attrs[1] ate pthread	uci fw_idx success	not exist		
[2023:08:21 10: [2023:08:21 10: [2023:08:21 10:	5:37] INFO [Cell 55:37] INFO [Cell 55:38] INFO [Cell	ulard]: cell0 cre ulard]: cell0 ini ulard]: cell0 sim	t AT port slot init	success current	uccess use simslot	idx:0			
[2023:08:21 10: [2023:08:21 10: [2023:08:21 10:	55:40] INFO [cell 55:40] INFO [cell	ulard]: cell0 req ulard]: cell0 req ulard]: cell0 req	uset gene uest mode	ic init o initiali	one ze: not nee	d			
[2023:08:21 10: [2023:08:21 10: [2023:08:21 10:	55:41] INFO [cell 55:41] INFO [cell 55:41] INFO [cell	ulard]: cell0 red ulard]: cell0 red ulard]: cell0 red	uest Mode uest FW V	n Name: EC ersion: EC	200A 200ACNDAR01	A07M16			
[2023:08:21 10: [2023:08:21 10: [2023:08:21 10:	55:41] INFO [cell 55:41] INFO [cell 81:32] WARNING [ce	ulard]: cell0 req ulard]: cell0 mod llulard]: cell0 r	uest IMEI el is rea eload con	86921806 ly. fig wwan	8976040				
[2023:08:21 11:0 [2023:08:21 11:0	1:32] INFO [cell 1:32] WARNING [ce	ulard.settings]: llulard.settings]	package cellul	wan inter ar_advance	<pre>face=cell0. d_attrs[0]</pre>	uci mtu not	t exist		
[2023:08:21 11:0 [2023:08:21 11:0 [2023:08:21 11:0	01:32] WARNING [Ce 01:32] INFO [Cell	ulard]: serial po ulard]: serial po	: cellul ort /dev/t	yUSB1 cre	d_attrs[1] ate pthread	uci +w_idx success	not exist		

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.

IG/LTE					
IM Card: Not Inser	t Sig: 0(0%) GET I	P: 0.0.0.0 IMEI: 86	592180689	76040	
SIM1 Card Setting	SIM2 Card Setting	Advanced Setting	Run log	4G traffic	
real traffic					1:0.00 B/s 1:0.00 B/s (1)
month traffic					33.29 MB (2)
day traffic					33.29 MB
Commit interval 🍨					1h - compromise between risk of data lo 🗸 🕢
					Interval at which the temporary in-memory database is committed to the persistent database directory.

- 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.

Routes						
Routes specify over which interface and gateway a o	certain host or network can be reached.					
Static IPv4 Routes						
Interface→ Target 1 Host-P or Network 2	IPv4-Netmask if target is a network 3	IPv4-Gateway	Metric 5	MTU 6	Route type	
wan 🗸 192.168.0.0/16	255.255.255.255	192.168.9.222	0	1500	unicast	✓ Delete
Add						

- 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:

Туре	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

Black And White List Port Forwards Custom Rules			
Firewall - Black And White List			
Disable or allow forwarding of certain addresses by setting a black and white list.			
General Settings			
Strategy Type	WhiteListStrategy 1	Switch Strategy	
Access Control Rules			
Name Protocol Source MAC address	Source IP Source Port	Dest IP Dest Port	Action Enable/Disable
	This section contains no values yet		
New Access Control Rules			
Name Protocol Source MAC address	Source IP	Dest II	P Action
New Access Control Rules	✔ 172.18.4	199 (3)	drop (4) Add 5

- 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

Black And White List Port Forwards Custom Rules					
Firewall - Black And White List					
Disable or allow forwarding of certain addresses by setting a black and white list.					
General Settings					
Strategy Type	1 WhiteListStrate	ay 🗸	Switch Strategy		
Access Control Rules					
Name Protocol Source MAC address	Source IP Sou	rce Port Dest IP	Dest Port	Action	Enable/Disable
	This section c	ontains no values yet			
New Access Control Rules					
Name Protocol Source MAC address	Source IP	Source Port	Dest IP	Dest Port	Action
New Access Control Rul	▼ 172.18.4.199	3		80 (4)	droi S Add

- 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

Black And White List Port Forwards Custom Rules			
Firewall - Black And White List			
Disable or allow forwarding of certain addresses by setting a black and white list.			
General Settings			
Strategy Type	BlackListStrategy	Switch Strategy	
Access Control Rules			
Name Protocol Source MAC address	Source IP Source Port	Dest IP Dest Port	Action Enable/Disable
	This section contains no	values yet	
New Access Control Rules			
Name Protocol Source MAC address		Source IP De	st IP Action
New Access Control Rules IP	•	172.18.4.199	accept Add

- 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

Black And White List Port Forwards Custom Rules					
Firewall - Black And White List					
Disable or allow forwarding of certain addresses by setting a black and white list.					
General Settings					
Strategy Type	1 BlackListStrategy	~	Switch Strategy		
Access Control Rules					
Name Protocol Source MAC address	Source IP Source	e Port Dest IP	Dest Port	Action	Enable/Disable
	This section con	ains no values yet			
New Access Control Rules					
Name Protocol Source MAC address	Source IP	Source Port	Dest IP	Dest Port	Action 6
New Access Control Rul TCP	✓ 172.18.4.199 (3)			80 (4	accept Add

- 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):

General Settin	ngs Port Forwards Filter Ru	es Custom Rules			
-irewall	- Port Forwards				
ort forwardir	as allows remote computers on the	Internet to connect to a specific computer or service u	within the private LAN.		
			•		
Port Forw	ards				
Name	Match	Forward to	Enable		
3222to22	IPv4-tcp, udp From any host in wan Via any router IP at port 3222	IP 172.18.1.1, port 3222 in lan	Image: Contract of the second seco	Jp Down	Edit Delete
	amurand				
New port f	orwaru				
New port fo	Protocol	External External port In	nternal IP address	Inter	rnal port
New port fo Name	Protocol	External External port 4	one 5 Internal IP address	Inter	raal port

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.

Status	>	Start network captur	e seconds, packets (2)		Filter 3	Actions 4
Quick Start	>	any 🗸 30		seconds ✓ filter		Start capture
1 Virtual Tunnel	>					
n Network	~					
Interfaces Wireless(WIFI)						
4G/LTE						
Static Routes						
Firewall						
Diagnostics						
VTShark						

- 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

rackets 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.
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.

File Ed	lit View Go (Capture Analyze Statist	lics Telephony Wireless Q, ← → ∩ ↔	Tools Help		
Apply	a display filter	«Ctrl-/>				-+
No.	Time	Source	Destination	Protocol	Length Info	_
-	1 0.000000	192.168.9.17	192.168.9.214	TCP	68 80 - 56948 [ACK] Seq=1 Ack=1 Win=796 Len=0 TSval=251947394 TSecr=2559533736	
	2 0.000414	192.168.9.214	192.168.9.17	TCP	68 [TCP ACKed unseen segment] 56948 - 89 [ACK] Seq=1 Ack=2 Win=501 Len=9 TSval=2559534737 TSecr=251946393	_
÷						
	4-0.256846	192-168.9.17	192.168.9.214	TCP	68 [TCP Previous segment not captured] 80 - 56948 [ACK] Sequ2 Ack#448 Win#798 Len#0 T5val#251947651 T5ecr#2559534893	
	5 0.419839	192.168.9.17	192.168.9.214	TCP	137 80 - 56948 [PSH, ACK] Seq=2 Ack=448 Win=796 Len=69 TSval=251947813 TSecr=2559534993 [TCP segment of a reassembled PDU]	
	6 8.428284	192.108.9.214	192.168.9.17	TCP	be [10] ALKed undern Beginnt [boyad - se [ALK] begraad Ack-/1 Win-Sbi Lenev 15VA1250505515/ 15ec7-25194/813	
	7 0.420358	102.108.9.17	192.100.9.214	TCP	pay bu - powe (pon, ALK) pogeri ALKe-448 MIN-190 LEN-31, 1948-2219-414 (bet=20093031) (ity segment or a reassembled PDU) 68 EGNA - 00 (ALV) Sandda Autorion (itorian) (and a real-31 (itorian)) (itorian) (itorian) (itorian) (itorian)	
	0.0.425222	102 168 0 17	102 168 0 214	HTTP/1	ve source = de [noc] seguente nocketus ministri Leiner (stal=coundation = coundation) 73 uttrict 1 200 (Nr. DausGerict Dhinch Dhatainn (staling)(staling)	
-	10 0.425652	192 168 9 214	192 168 9 17	TCP	to mini-ziz zoo ok , ownaki zp ovjetc motalizon (applization jenn) Ra Rođak _ Ro IAKK Samada AckeRN Mini-Rol Innes Toxal=25005515/2 Tierr=251047810	_
	11 1.425799	192,168,9,17	192,168,9,214	TCP	58 TTCP Keen-Ally 80 - 56948 (ACK) Sect-566 Ack=448 Win=706 Len=0 TSval=251948820 TSecr=2559535162	
	12 1.426438	192, 168, 9, 214	192.168.9.17	TCP	68 TTCP Keen-Alive ACK1 56948 - 80 FACK1 Sen-448 Ack-567 Win-501 Len=0 TSval=2559536163 TSecr=251947819	_
	13 2,428003	192,168,9,17	192,168,9,214	TCP	68 (TCP Keep-Alive) 89 - 56948 (ACK) Sep-509 Ack=448 Win=796 Len=0 Tsval=251949822 TSecr=2559536163	
	14 2.428955	192.168.9.214	192.168.9.17	TCP	66 [TCP Keep-Alive ACK] 56948 - 80 [ACK] Seg=448 Ack=607 Win=501 Len=0 TSval=2559537165 TSecr=251947819	_
	15 3.257115	192.168.9.214	192.168.9.17	HTTP	515 GET /cgi/gateway/admin/network/vtshark_check_status?_=0.4734152646109634 HTTP/1.1	
	16 3.257321	192.168.9.17	192.168.9.214	TCP	68 80 - 56948 [ACK] Seq=507 Ack=895 Win=796 Len=0 TSval=251950651 TSecr=2559537994	_
	17 3.423646	192.168.9.17	192.168.9.214	TCP	137 80 - 56948 [PSH, ACK] Seq=607 Ack=895 Min=796 Len=69 TSval=251950817 TSecr=2559537994 [TCP segment of a reassembled PDU]	
	18 3.424085	192.168.9.214	192:168:9:17	TOP	88 [TCP ACKed unseen segment] 50048 80 [ACK] Seq=895 Ack=076 Win=501 Len+0 T\$val=2550538[10] TSecr=251050817	
▶ Frame	e 3: 515 bytes	on wire (4120 bits)	, 515 bytes captured	(4120 bits)	0000 00 00 00 01 00 06 fc 34 07 b9 15 f6 00 00 08 00 4	
-Linux	x cooked captu	ire vi			0010 45 00 01 73 33 d 64 00 40 00 60 67 60 88 09 d6 E = e.e.g. g. r 0020 61 86 09 11 de 74 00 55 as 1 c bb r be 52 99 19 9 r r).	
▶ Inter	rnet Protocol	Version 4, Src: 192.	168.9.214, Dst: 192.1	68.9.17	9030 89 18 81 15 d7 c6 90 00 91 91 98 9a 98 8f 67 91	
▶ Trani	smission Contr	ol Protocol, Src Por	t: 56948, Dst Port: 8	0, Seq: 1, A	ck: 2, Len: 447 0050 65 77 61 79 2f 61 64 6d 69 6e 2f 6e 65 74 77 6f eway/adm in/netwo	
Hyper	rtext Transfer	Protocol			0050 72 6b 27 76 74 73 86 61 72 6b 5f 63 68 65 63 6b rk/vtsha rk_check	
					0000 30 30 30 30 30 30 31 30 31 30 31 30 32 32 40 54 54 00060310 1633 MTT	
					0000 50 27 31 20 31 00 84 48 67 73 74 3a 20 31 39 32 P/1.1 H ost: 192 0030 22 31 36 32 20 39 20 31 37 00 08 57 36 57 22 d 168,9.1 7 User-	
					167 65 66 74 3a 29 4d 6f 7a 69 6c 6c 61 2f 35 Agent: M ozilla/5	
					0000 20 30 20 20 20 50 51 30 20 20 76 3a 31 50 20 76 2	
					0940 29 47 65 63 65 67 72 32 30 31 30 30 31 30 31 20 Geckv/2 0100101 0070 46 69 72 65 65 67 78 27 31 39 35 02 39 69 16 41 Etrefyv/185 0-4	
					0100 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63 65 ccept: * /* Acce	
					0110 70 74 2d 4c 61 66 67 75 61 67 65 3a 20 65 6e 2d pt-Langu age: en- 0120 55 53 2c 65 6e 3b 73 3d 30 2e 35 00 9a 41 63 US en: e= 0.5 - Acc	
					1130 65 70 74 24 45 66 83 67 64 69 6e 67 3a 20 67 7a ept-Enco ding; g2	
					0140 09 /9 22 20 04 05 05 05 00 00 01 /4 05 00 04 43 01 06 11, 001 attr-Com 0150 66 65 63 74 69 67 66 36 20 66 65 70 24 61 60 meg-al	
					0180 69 76 65 69 69 85 25 65 66 65 72 65 72 38 20 68 74 ive Referer: ht	
					0100 77 05 07 27 65 07 69 27 67 61 77 61 79 27 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 61 77 77 77 77 77 77 77 77 77 77 77 77 77	
					0 0190 6d 69 6e 2f 6e 65 74 77 6f 72 6b 2f 76 74 73 66 min/netw ork/vtsh	
					6175 75 75 68 36 38 33 32 31 39 66 34 35 65 61 61 auth=832 19745eaa	
					1 11.00 b6 39 36 34 61 35 33 62 32 39 51 63 34 65 63 39 T6043530 298464669 11.01 60 65 37 31 38 86 3b 20 70 65 16 37 57 46 83 d6 2 67365 p1 Autheb	
					66 32 64 34 64 37 66 11 39 35 39 37 38 64 33 30 f23407fa 95978330	
07	vtshark.result.pca	0			Packets: 18 - 000	Profile: Defau