4G Router VPN Configuration

1. VPN Definition

VPN (Virtual Private Network) is a technology that allows a private network to be established over a public network.

- **Definition**

A VPN is a technology that establishes a temporary, secure connection over a public network (such as the Internet). It creates a secure communication tunnel over an insecure public network, enabling remote users, branch offices, business partners, and others to securely access corporate network resources as if they were directly connected to the corporate network.

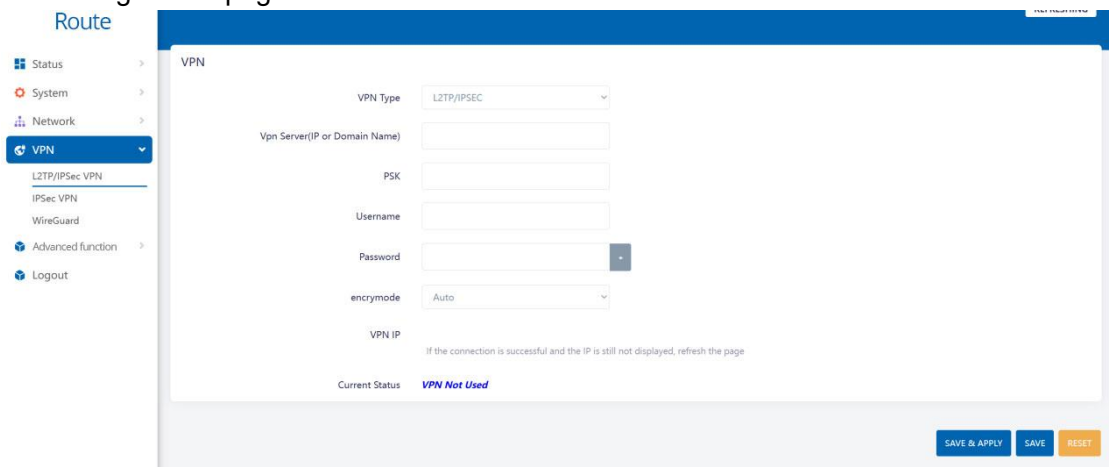
- **How it works:**

VPNs primarily utilize encryption technology and tunneling protocols to achieve secure communications. When a user initiates a connection request through a VPN client, the VPN client negotiates with the VPN server to establish an encrypted tunnel. Before being sent to the public network, the user's data is encrypted into ciphertext and transmitted through this tunnel to the VPN server. Upon receiving the ciphertext, the VPN server decrypts it and forwards the data to the target enterprise's internal network. Conversely, data returning from the enterprise's internal network undergoes a similar encryption and decryption process before being transmitted back to the user through the VPN tunnel.

2. VPN Configuration

- **L2TP/IPSEC**

The configuration page of VPN is shown below



VPN Type: Displays the currently selected VPN protocol type. Select "L2TP/IPSEC." L2TP (Layer 2 Tunneling Protocol) and IPSec (Internet Protocol Security) are a commonly

used VPN protocol combination used to establish secure tunnel connections over IP networks.

VPN Server Address (IP or Domain Name): Enter the VPN server's IP address or domain name. This is crucial information required for clients to connect to the VPN server. Entering the correct address allows clients to locate and connect to the designated VPN server.

Pre-shared key: In IPSec, a pre-shared key is used for authentication. Both the client and the VPN server must be configured with the same pre-shared key to authenticate the connection and ensure connection security.

Username: The user's login username on the VPN server. This username is used for authentication; the VPN server uses it to identify and verify the client's identity.

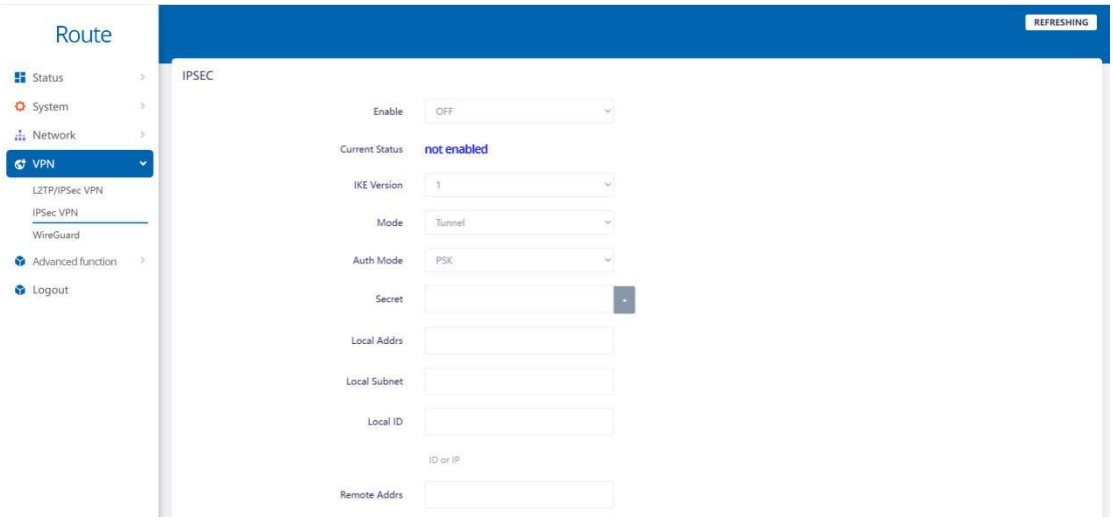
Password: The password corresponding to your username, also used for authentication. This password is crucial for protecting your account and ensuring only authorized users can connect to the VPN server.

Encryption: Displays the currently selected encryption method. "Auto" here indicates automatic encryption selection. VPN connections typically use encryption technology to protect data security during transmission. Automatic encryption allows the system to select the most appropriate encryption algorithm based on the situation.

VPN IP: After a successful VPN connection, this displays the VPN IP address assigned to the client.

Current Status: Displays the current status of the VPN connection.

- **IPSEC VPN**



Enable: Enables or disables the IPSec feature.

IKE Version: IKE (Internet Key Exchange) is a protocol used to negotiate security associations (SAs) between two parties in IPSec communication. You can select the IKE version; both IKEv1 and IKEv2 are supported.

Mode: The IPSec operating mode, supporting tunnel mode and transport mode. Tunnel mode establishes a secure tunnel between two networks, while transport mode protects end-to-end communications.

Authentication: The method used to verify the identities of both communicating parties; pre-shared keys (PSK) are supported.

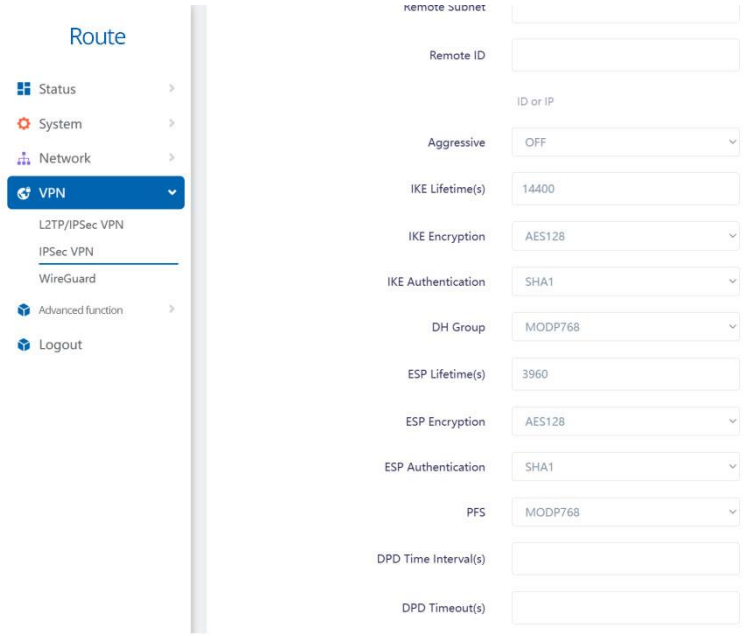
Key: A pre-shared key is required.

Local IP: The IP address of the local network.

Local Subnet: The subnet mask of the local network.

Local ID: An ID used to identify the local network or device, which can be an IP address or other identifier.

Remote IP: The IP address of the remote network.



Remote Subnet: The subnet mask of the remote network.

Remote Identifier (ID): An ID used to identify the remote network or device. This can be an IP address or other identifier.

Aggressive Mode: An IKE operating mode that reduces the number of message exchanges during the negotiation process compared to Main Mode and is suitable for certain scenarios.

IKE Lifetime (seconds): The lifetime of the IKE SA, in seconds. After this time expires, the IKE SA will be renegotiated.

IKE Encryption Algorithm: The algorithm used to encrypt data during IKE negotiation. Common algorithms include AES128 and AES256.

IKE Checksum Algorithm: The algorithm used to verify data integrity during IKE negotiation. Common algorithms include SHA1 and SHA256.

DH Group: The group used by the Diffie-Hellman key exchange algorithm. Different groups provide different levels of security.

ESP Lifetime(s): The lifetime of the ESP (Encapsulating Security Payload) SA, expressed in seconds.

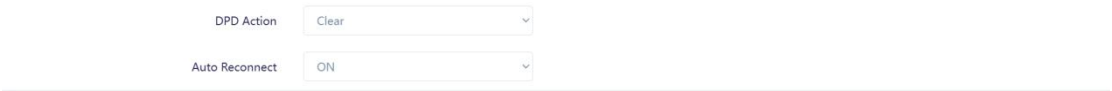
ESP Encryption Algorithm: The algorithm used to encrypt ESP data. Common examples include AES128 and AES256.

ESP Verification Algorithm: The algorithm used to verify the integrity of ESP data. Common examples include SHA1 and SHA256.

PFS: Perfect Forward Secrecy. This ensures that even if a long-term key is compromised, past communications are not compromised.

DPD Detection Period (seconds): Dead Peer Detection, used to check whether a peer is still online, is used to detect dead peers.

DPD Timeout (seconds): If no response is received from a peer within the DPD detection period, the waiting timeout is set to seconds.



DPD Operation: This is the operation performed when a peer is detected to be offline. Common examples include clearing and restarting.

Auto-reconnect: This is used to set whether to automatically reestablish a connection after a disconnection.