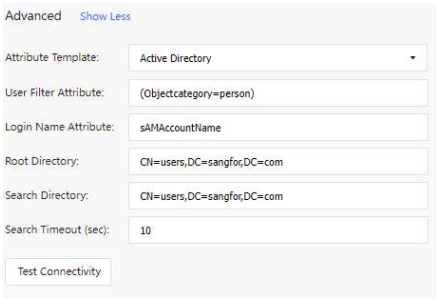
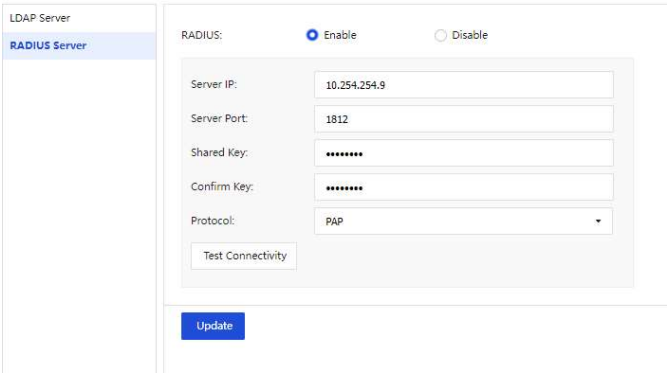


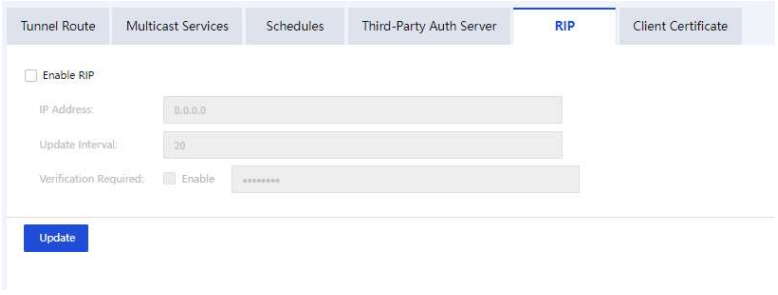
RADIUS Server

The VPN service for Sangfor devices supports third-party LDAP authentication. If you want to enable third-party RADIUS authentication, configure information about the third-party RADIUS server on the **RADIUS Server** page, including **Server IP**, **Server Port**, **Shared Key**, and **Protocol**, as shown in the following figure.



RIP

You can enable routing information protocol (RIP) to allow a Sangfor device to advertise routing information to other routers so that routing information on intranet routers can be dynamically updated, as shown in the following figure.



The parameters are described as follows:

Enable RIP: Specify whether to enable dynamic route updates based on RIP. If you check **Enable RIP**, the Sangfor device will advertise information about the peer device that has established a VPN connection to the local device to the specified intranet router. The routing tables of other devices are updated, and a route from the VPN peer device to the Sangfor device is added. If the VPN connection fails, the router is instructed to delete the route.

IP Address: Enter the IP address of the router to which route updates will be advertised.

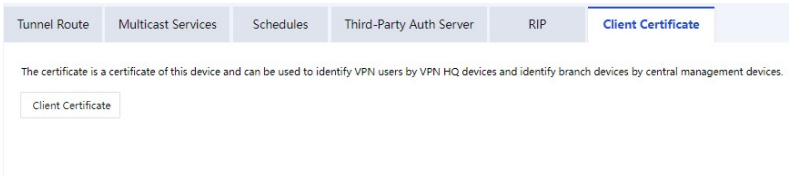
Update Interval: The interval for route updates. The Sangfor device will trigger a route update when the route changes. In this case, this parameter does not take effect.

Verification Required: Specify whether a password is required for exchanging RIP packets.

Client Certificate

The certificate authentication system based on hardware features is one of Sangfor's patented inventions. Sangfor devices also use this technology for authentication among VPN nodes. The client certificate of a Sangfor device is an encrypted certificate generated based on the hardware features of the device. The client certificate is unique and unforgeable due to the uniqueness of device hardware features. The hardware features are verified so that only the specified device is authorized to access the network, this helps avoid security risks.

You can click **Client Certificate** to generate a client certificate and store it on your local computer, as shown in the following figure.

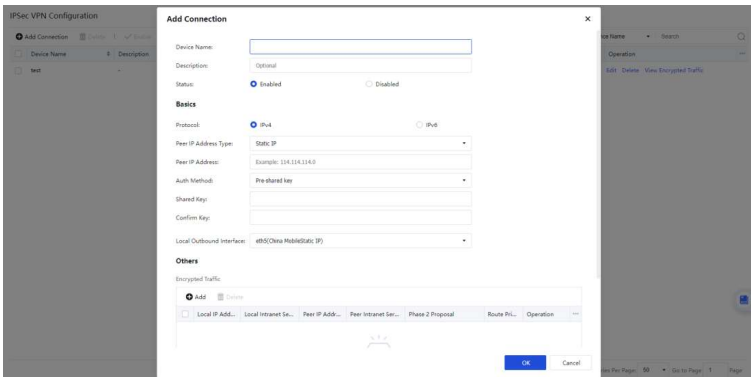


Send the client certificate to the HQ device administrator. When you add a VPN user, the HQ device administrator can select the client certificate for authentication and bind the user to the client certificate.

5.10.5 IPSec VPN Configuration

Network Secure supports IPSec VPN connections to third-party devices. IPSec VPN of Network Secure conforms to the international IPSec VPN protocol. Provided that the peer device also adopts the standard IPSec VPN, you can establish a VPN connection between the local device and the peer device.

You can click **Add Connection** on the **IPSec VPN Configuration** page to add IPSec VPN connections. The **Add Connection** dialog box appears, as shown in the following figure.



The parameters are described as follows:

Device Name: Set a name for the tunnel.

Status: Specify whether to enable the VPN connection.

(Optional) **Description**: Enter a description of the tunnel.

Peer IP Address Type: Select **Static IP**, **Dynamic IP**, or **Dynamic Domain** as required. If you select **Static IP**, enter the IP address of the peer device. If you select **Dynamic Domain**, enter the WAN domain name of the peer device.

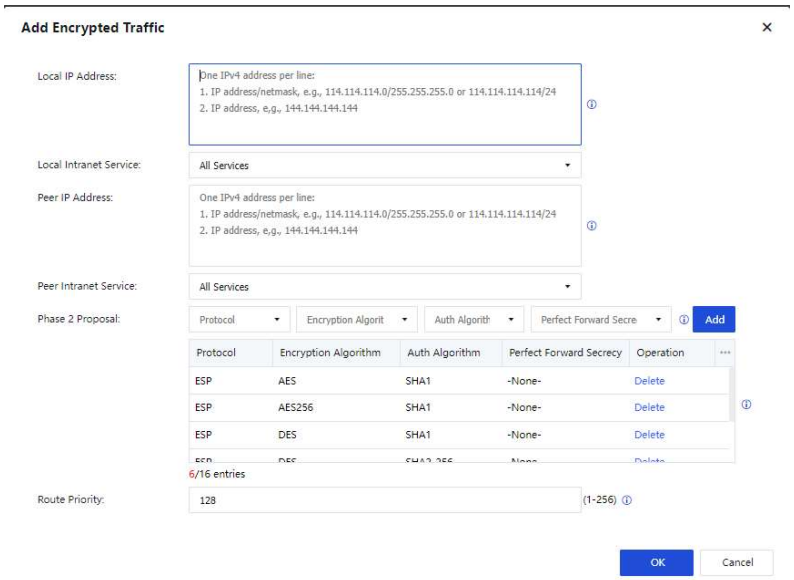
Auth Method: Select **Pre-shared key** or **Certificate based** as required.

Shared Key and **Confirm Key**: Enter the correct pre-shared key. Ensure that both devices use the same pre-shared key.

Local Outbound Interface: Select an outbound interface based on the link status.

Encrypted Traffic: Set parameters for protected data flows and Phase 2 negotiation of IPSec VPN as required.

Click **Add** in the **Encrypted Traffic** section. The **Add Encrypted Traffic** dialog box appears, as shown in the following figure.



The parameters are described as follows:

Local IP Address: Enter a source IP address or IP range for matching protected data flows of IPSec VPN.

Local Intranet Service: Select a source intranet service type for matching protected data flows of IPSec VPN. You can select **All Services**, **All TCP Services**, **All UDP Services**, or **All ICMP Services** as required.

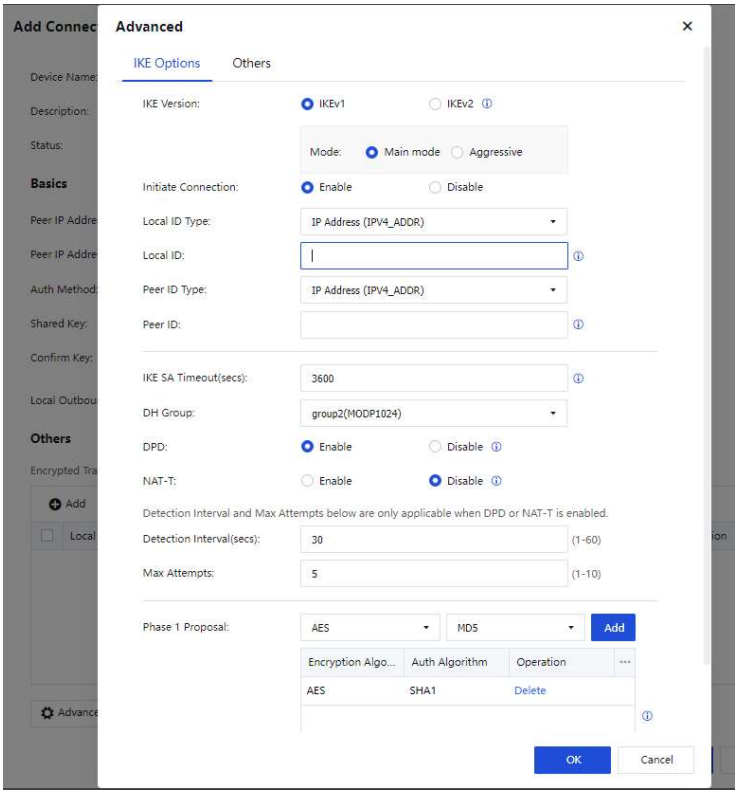
Peer IP Address: Enter a destination IP address or IP range for matching protected data flows of IPSec VPN.

Peer Intranet Service: Select a destination intranet service type for matching protected data flows of IPSec VPN. You can select **All Services**, **All TCP Services**, **All UDP Services**, or **All ICMP Services** as required.

Phase 2 Proposal: Set the parameters required for Phase 2 negotiation, including **Protocol**, **Encryption Algorithm**, **Auth Algorithm**, and **Perfect Forward Secrecy** (PFS). Options for **Protocol** include **AH** and **ESP**. Options for **Encryption Algorithm** include **DES**, **3DES**, **AES**, **AES192**, **AES256**, and **SANGFOR_DES**. Options for **Auth Algorithm** include **MD5**, **SHA1**, **SHA2-256**, **SHA2-384**, and **SHA2-512**.

Route Priority: Set a priority for local and peer IP addresses to identify the route priority.

Click **Advanced** to configure IKE and IPSec options, as shown in the following figure.



IKE Options:

IKE Version: Select IKEv1 or IKEv2. The setting must be the same as that of the peer device.

Mode: The connection mode. Options include **Main mode** and **Aggressive**. The main mode is applicable when both devices use static IP addresses or one uses a static IP address and the other uses a dynamic domain name. It does not support NAT traversal. The aggressive mode is applicable when one of the devices establishes connections through dial-up, and it supports NAT traversal. Select either mode based on your business requirements.

Initiate Connection: Specify whether the device can actively initiate a VPN connection.

Local ID Type: Select an ID type for the local device to ensure that the peer device can identify the local device. Options include **IP Address (IPV4_ADDR)**, **Domain String (FQDN)**, and **User String (USER_FQDN)**.

Local ID: Set an ID for the local device based on the selected local ID type.

Peer ID Type: Select an ID type for the peer device to ensure that the local device can identify the peer device. Options include **IP Address (IPV4_ADDR)**, **Domain String (FQDN)**, and **User String (USER_FQDN)**.

Peer ID: Set an ID for the peer device based on the selected peer ID type.

IKE SA Timeout(secs): Set the Phase 1 lifetime for IPSec negotiation, in seconds.

DH Group: Select a DH group type, including DH groups 1, 2, 5, 14, 15, 16, 17, and 18. The setting must be the same as that of the peer device.

DPD: Specify whether to enable the dead peer detection (DPD) feature to detect the life status of the peer device in IPSec.

NAT-T: This feature is available only in aggressive mode. It avoids failure of IPSec negotiation when NAT is enabled on one of the devices. After you enable NAT traversal, data will be encapsulated based on UDP instead of ESP, in case ESP is not allowed on the intranet.

Detection Interval(secs): Set an interval for DPD and NAT-T detection.

Max Attempts: Set the maximum number of DPD and NAT-T detection attempts. If the number of attempts exceeds this value, the local device determines that the peer device fails and disconnects from the peer device.

Phase 1 Proposal: Set the parameters required for Phase 1 negotiation, including **Encryption Algorithm** and **Auth Algorithm**. Options for **Encryption Algorithm** include **DES**, **3DES**, **AES**, **AES192**, **AES256**, **SANGFOR_DES**, and **SANGFOR_NULL**. Options for **Auth Algorithm** include **MD5**, **SHA1**, **SHA2-256**, **SHA2-384**, and **SHA2-512**.

After you configured the IKE options, click **OK** and then click the **Others** tab to configure IPSec options.

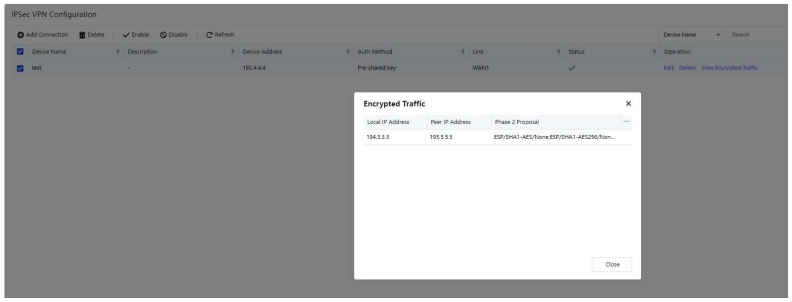
Others:

Max Attempts: Set the maximum number of attempts for IPSec VPN connection.

IPSec SA Timeout(secs): Set a timeout interval for IPSec security associations (SAs).

Expiration Time: Specify whether to enable expiration time for IPSec VPN tunnels.

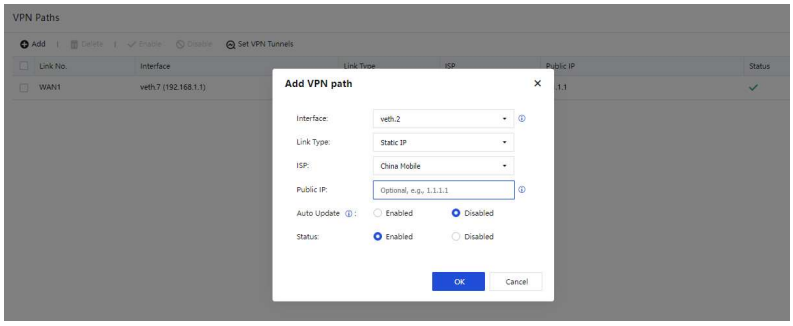
Click **OK** to save the settings. In the **Operation** column, you can click **Edit** to modify the parameters of the VPN connection or click **View Encrypted Traffic** to view the matching rules for encrypted traffic.



5.10.6 General Settings

5.10.6.1 VPN Paths

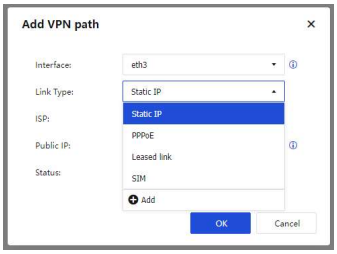
If multi-link licensing is enabled for the device, multiple WAN interfaces are configured. In this case, you can add multiple VPN paths on the **VPN Paths** page. On the **VPN Paths** page, click **Add**. The **Add VPN path** dialog box appears, as shown in the following figure.



The parameters are described as follows:

Interface: Select a WAN interface.

Link Type: Select a preset link type or click **Add** to create one, as shown in the following figure.



ISP: Select a preset ISP or click **Add** to create one, as shown in the following figure.

Public IP: Enter a public IP address.

Auto Update: Specify whether to enable auto updates for the public IP address. In a dial-up scenario, you can enable this feature to automatically obtain the public IP address of the outbound interface. If you want to manually set the public IP address, select **Disabled** so that the public IP address is not automatically updated.

Click **OK**. The VPN path appears in the VPN path list.

Set VPN Tunnels

You can select local and peer links for establishing Sangfor VPN connections. Unselected links cannot be used for establishing Sangfor VPN connections. This avoids Sangfor VPN connections across ISPs or link types. For example, link 1 for the HQ device and link 1 for the branch device are private links of China Telecom, and link 2 for the HQ device and link 2 for the branch device are internet links of China Telecom. In this case, only two Sangfor VPN connections are allowed between the HQ and branch devices: a Sangfor VPN connection between their private links, and a Sangfor VPN connection between their internet links.

Click **Set VPN Tunnels** on the **VPN Paths** page. The **Set VPN Tunnels** dialog box appears, as shown in the following figure.