Site-to-Site VPN

https://www.synology.com/en-global/knowledgebase/SRM/help/VPNPlusServer/vpnplus_server_site2site

Site-to-Site VPN allows networks in multiple fixed locations to establish secure connections to each other over the Internet.

When you first set up a Site-to-Site IPSec VPN, you may need to manually add a profile on your Synology Router, and then export/import the profile to another VPN Plus supported Synology product. When you choose to manually add or edit the profile, you will see the configuration window with the **General** and **Encryption** tabs. Please refer to the following sections for details.

Note:

- The function of profile export/import is not available if you set up a Site-to-Site VPN tunnel to another IPSec supported device other than Synology product.

General

- **Profile name**: customizable name of this profile.
- **Pre-shared key**: Specify the pre-shared key on both sites to enhance the security. Connections will be successful only when the identical pre-shared key has been specified on both sites.
- **Enable this connection**: Tick this checkbox to start the connection right after setup. This function will take effect only when enabled on both sites.
- **Local Site**:
    - **Outbound IP**: Specify one of the network interfaces on your Synology Router to set up Site-to-Site VPN service.
    - **Local ID**: Specify the Local ID, which can be either a public IP address or FQDN.
    - **Private subnet**: Specify the local network under the private subnet.
      Note: The options in the drop-down list have been defined in Object. Address pool objects in **IP range** type is not supported by Site-to-Site VPN configuration. You will only see the objects in **Subnet** type in the drop-down list.
- **Remote Site**:
    - **IP address/FQDN**: Fill in your remote site's public IP address or FQDN which ensures external access.
    - **Remote ID**: Specify the Remote ID, which can be either a public IP address or FQDN.
    - **Private subnet**: local network under the private subnet of the remote site.
- **Dead Peer Detection**:
    - **Enable**: Tick the checkbox to enable **Dead Peer Detection** (DPD).
        - **DPD Delay**: Specify the time interval between DPD packets.
        - **DPD Timeout**: Specify a time threshold for the system to recognize the loss of connection to the remote site when not having received any DPD packets for longer than such time threshold.

Note:

- The private subnets of local and remote sites cannot overlap.
- You may read the RFC 3706 document for more technical information on Dead Peer Detection.

Encryption

- **IKE version**: Select **IKEv1** or **IKEv2**. Both sites must have the same IKE version.
- **Mode**: Select **Main Mode** or **Aggressive Mode**. Both sites must have the same mode.
- **Encryption**: Select any one or more from AES256, AES192, AES128, and 3DES. You must select at least one encryption method which is adopted by the other site.
- **Authentication**: Select any one or more from SHA-512, SHA-384, SHA-256, SHA1, MD5. You must select at least one authentication method which is adopted by the other site.
- **DH group**: Specify the same Diffie-Hellman (DH) group for both sites.
- **Key lifetime**: Specify how long the key will be valid. Once the key expires, both sites will exchange the new key.

- **Enable Perfect Forward Secrecy (PFS)**: Enabling this option may subtly affect the performance, but will enhance the security.

Note:

- Inconsistency of configuration between the two sites may result in connection failure. We recommend export/import the configuration on one site into the other site to facilitate the setup and minimize the possibility of errors.