Setup L2TP/IPsec VPN Server on SoftEther VPN Server

The IPsec VPN Server Function is disabled by default. You can enable it easily as the following steps.

Configuration Guide

The VPN Server configuration is very easy.

Start VPN Server Manager

Start SoftEther VPN Server Manager (which runs on Windows, but it can connect to remote SoftEther VPN Server running on Linux, Mac OS X or other UNIX). On the Server Manager, you can see the "L2TP/IPsec Setting" button. Click it.

VPN Server Manager Main Window

The following screen will appear. Each IPsec Server Function can be turned on / off on this screen.

02.png

IPsec / L2TP / EtherIP / L2TPv3 Settings Screen

The meanings of each option are followings:

- **L2TP Server Function (L2TP over IPsec)**
  This function is for accepting VPN connections from iPhone, iPad, Android, and other smartphones, and built-in L2TP/IPsec VPN Client on Windows or Mac OS X. Enable it if you want to support one of these devices as VPN Client.

- **L2TP Server Function (Raw L2TP with No Encryption)**
  Some special-configured VPN router or client devices have only just a L2TP protocol without IPsec encryption. To support such a strange device, you have to enable it.

- **EtherIP / L2TPv3 over IPsec Server Function**
  If you want to build site-to-site VPN connection (Layer-2 Ethernet remote-bridging), enable EtherIP / L2TPv3 over IPsec. You have to add your edge-side device definition on the list.

- **IPsec Pre-Shared Key**
  IPsec Pre-Shared Key is sometimes be called "PSK" or "Secret" . This string is

"vpn" by default. However, changing it is recommended. You have to inform the latest key to all VPN users.

How to enable and configure IPsec with vpncmd

If you cannot use VPN Server Manager GUI for Windows, alternatively you can use vpncmd to activate and configure the IPsec VPN Server Function, by the **IPSecEnable command.** To learn how to do it in vpncmd, run **"IPsecEnable ?"** command in the vpncmd prompt.

How does a L2TP/IPsec VPN user have to specify his username to login? (with Standard Password Authentication)

The principal is; when a VPN user wants to establish a VPN connection to the SoftEther VPN Server with IPsec/L2TP VPN Server Function he have to specify the destination Virtual Hub Name in the username field.
For example, assume that the SoftEther VPN Server has two Virtual Hubs: **"HUB1"** and **"HUB2"** . And there is a user **"yas"** in **"HUB1"** , and **"jiro"** in **"HUB2"** .
In that case, specify the destination Virtual Hub Name after the username with appending **'@'** character, suchlike **"yas@HUB1"** or **"jiro@HUB2"** . Note that both user-name and hub-name are case insensitive.
However, you can specify the "Default Virtual Hub" on the IPsec setting screen. If the destination Virtual Hub Name in the login-attempting username is omitted, then the default Virtual Hub is to be assumed to be designated by the user.
For example in the case if the default Virtual Hub is **"HUB2"** , the user **"jiro"** on the HUB2 can be logged on by just **"jiro"** . **"@HUB2"** can be omitted.

How does a L2TP/IPsec VPN user have to specify his username to login? (with RADIUS OR NT Domain Authentication)

The principal is; when a VPN user wants to establish a VPN connection to the SoftEther VPN Server with IPsec/L2TP VPN Server Function he have to specify the destination Virtual Hub Name in the username field.
For example, assume that the SoftEther VPN Server has two Virtual Hubs: **"HUB1"** and **"HUB2"** . And there is a user **"yas"** in **"HUB1"** , and **"jiro"** in **"HUB2"** .
In that case, specify the destination Virtual Hub Name before the username with appending **'\'** character, suchlike **"HUB1\yas"** or **"HUB2\jiro"** . Note that both user-name and hub-name are case insensitive.

However, you can specify the "Default Virtual Hub" on the IPsec setting screen. If the destination Virtual Hub Name in the login-attempting username is omitted, then the default Virtual Hub is to be assumed to be designated by the user.
For example in the case if the default Virtual Hub is **"HUB2"** , the user **"jiro"** on the HUB2 can be logged on by just **"jiro"** . **"HUB2\"** can be omitted.

User Authentication with L2TP/IPsec VPN Function

You have to create a user-object before the user attempts to connect a VPN connection by using L2TP/IPsec function. You cannot use certificate authentication for L2TP/IPsec VPN Function on the current version of SoftEther VPN Server.

Configuration for EtherIP / L2TPv3

EtherIP and L2TPv3 is for accepting VPN routers to build site-to-site VPNs. You can click the "EtherIP / L2TPv3 Detail Settings" button on the configuration screen to add the client-device entry on the list. On a client-device entry on the list, the ISAKMP (IKE) Phase 1 ID string, and the related credentials (username and password on a user which has been registered on the destination Virtual Hub.)

You can specify the asterisk ('*') as the wildcard on the username on an entry. Such an entry will be applied for any VPN client router's login attempts from remote side.

EtherIP / L2TPv3 Server Detail Settings

Note

Disable any IPsec/L2TP function on the server computer which might conflict with SoftEther VPN Server's IPsec/L2TP function. If the UDP ports (500, 4500 and 1701) conflicts with other programs, IPsec communication will not work well.
For example, disable the "Routing and Remote Access" service on Windows Server.
If you enable IPsec/L2TP function of SoftEther VPN Server, the IPsec/L2TP function of Windows will be shutdown temporary.

IP Address Assignment for L2TP Logged-in Users

In L2TP function, an IP address of a VPN Client must be assigned automatically by a DHCP server on the destination Virtual Hub's segment.

Therefore, you have to at least one running DHCP server on the destination L2 segment which the L2TP VPN Client attempts to login.

An IP address will be leased from the DHCP server, and the IP address will be assigned on the L2TP VPN client session. Default gateway, subnet mask, DNS address and WINS address will be also applied on the L2TP VPN client. So if no DHCP server, no login successes.

You can use any DHCP Server which is already existing on your local network. You can use SecureNAT's Virtual DHCP Server Function which is implemented on SoftEther VPN Server if you don't any DHCP servers on the LAN.

How to Traverse a NAT / Firewall?

If your SoftEther VPN Server is behind the NAT or firewall, you have to expose the **UDP port 500 and 4500**. On the NAT, **UDP 500 and 4500** should be transferred to the VPN Server. If any packet filters or firewalls are existing, open **UDP 500 and 4500** ports.

See Also

- 6.3.69 "IPsecEnable": Enable or Disable IPsec VPN Server Function
- 3.4 Virtual Hub Functions