10.4 Build a PC-to-LAN Remote Access VPN

This section will explain how to set up a generic remote access VPN.

10.4.1 Connecting to a LAN Remotely

In enterprise situations the most widely used type of VPN is the remote access VPN. By using a remote access VPN you can utilize an extremely inexpensive network such as the Internet to connect to your company's LAN from a remote location. Also, unlike with older protocols like L2TP/IPSec or PPTP, SoftEther VPN does not use IP routing and allows you to directly connect to a layer 2 segment.

Using this type of VPN it is possible to connect to a company LAN from outside the office (for example, from an employee's house or from a hotel on a business trip) just as if they were connected by an extremely long Ethernet cable.

10.4.2 Using Local Bridging

To build a remote access network you must create a Virtual Hub in your VPN Server and connect it to the target LAN already in place via a local bridge connection. Please refer to section 3.6 Local Bridges for more information about local bridging.

10.4.3 Examining User Authentication Methods

When installing a VPN Server for a remote access VPN keep the following standard guidelines in mind when deciding on a user authentication method.

- If your company already has a UNIX server or a Windows domain controller (including Active Directory) with a large number of registered users and you want to give those users access to the VPN, then you should use RADIUS authentication or Active Directory authentication. For more information on these authentication methods please refer to sections 2.2.3 RADIUS Authentication and 2.2.4 NT Domain and Active Directory Authentication.
- If your company already has a CA (certificate authority) that issues a X.509 certificate/private key file or smart card that supports SoftEther VPN then you should use certificate authentication as your user authentication scheme. For more information please refer to section 2.2.5 Individual Certificate Authentication and 2.2.6 Signed Certificate Authentication.

- If you have no existing authentication infrastructure then you can also register individual user names and passwords for users to connect to the Virtual Hub. For more information on password authentication please refer to section 2.2.2 Password Authentication. Even if no authentication infrastructure is in place you can still use certificate authentication in order to improve your network's security.

10.4.4 Network Layout

This section will explain the following type of network layout as an example.

10-4-1.png

Network Layout.

The network example above assumes that there is an existing company LAN to which the VPN Clients make a remote VPN connection to. Basic equipment to access the Internet such as a DHCP server or router is also already in place inside the company. When introducing a remote access VPN to this type of setup you need to install VPN Server to a computer which can be reached from both inside and outside the company (somewhere that can be seen from a public IP address on the Internet). Next you have to use local bridging to connect the VPN Server's Virtual Hub to the network you want to be able to connect to remotely.

Now the Virtual Network Adapter connected to the VPN Server's Virtual Hub will have a layer 2 connection to the target network via the Internet.

10.4.5 Installing VPN Server On a LAN

This section will go over what you need to be aware of when installing VPN Server.

The computer you install VPN Server on must make a local bridge connection to the company LAN you wish to remotely connect to. Therefore, it must be installed physically close enough to the LAN to connect to the layer 2 segment via a network cable.

Because the VPN Server must receive incoming VPN connections from the Internet it must have a public IP address or be able to receive TCP/IP communication through NAT, a firewall, or a reverse proxy system as described in section 10.2.1 VPN Server Location. Please consult with your network administrator if you are unsure about any of these issues.

10.4.6 Configuring the Local Bridge

Once you have VPN Server installed, create a Virtual Hub and connect it to the layer 2 segment you wish to remotely connect to via local bridging. For a detailed explanation of this process please refer to section 3.6 Local Bridges.

You should be aware of the following things when making connections via a local bridge.

- As explained in detail in section 3.6.3 Preparing the Local Bridge network adapter, if possible, try to set aside network adapters strictly for local bridging when making your local bridge connection. We recommend that you do not use a protocol stack for your local bridge network adapters, and do not assign TCP/IP IP addresses to them.
- We also recommend that you use a high quality network adapter from a trusted maker for your local bridge connections. For more information please refer to 3.6.5 Supported Network Adapter Types and 3.6.6 Use of network adapters not supporting Promiscuous Mode.

10.4.7 Connecting to the VPN Remotely/Performing a Communication Test

Once your remote access VPN Server has been installed and configured properly it's time to test it. Try connecting to the VPN Server's Virtual Hub from a remote VPN Client. If the remote LAN already has a DHCP server then it should automatically assign an IP address to the VPN Client's Virtual Network Adapter. If the remote LAN operates with statically assigned IP addresses then you must assign a static IP address to your Virtual Network Adapter as well.

Now that you are connected, try to ping a computer on the remote LAN's network to test if the VPN is communicating properly. You should also try to ping the VPN Client from

a computer on the remote LAN as well. Next, you should try to access a server (fileserver, database server, etc.) on the remote LAN.

10.4.8 Connecting using a Windows PC with MS-SSTP VPN Server Function

If you are using Windows Vista, 7, 8, RT or 10 as client PCs, you can enjoy Microsoft SSTP-VPN protocol, as an alternative of SoftEther VPN Client's SSL-VPN protocol. SSTP is the HTTPS-based VPN protocol which Microsoft is suggesting. Windows client PCs has a built-in SSTP VPN Clients. If you enable SSTP VPN function on SoftEther VPN Server, no longer to need to install SoftEther VPN Client on each PCs.

ss1.2.jpg

10.4.9 L2TP/IPsec VPN Server

Configuration Guide Edit section

The VPN Server configuration is very easy.

Start VPN Server Manager Edit section

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.

01.png
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)Edit section

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 FunctionEdit section

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? Edit section

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.

iPhone and Android

iPhone and Android has a built-in L2TP/IPsec VPN client function. However, they are designed to work with Cisco Systems VPN Routers as the model-case. A few other hardware-based VPN routers can be work with iPhone and Android. However, it is still too difficult to construct the practical remote-access VPN which can accept iPhone and Android, by usual skilled corporate system administrators.

SoftEther VPN has **a clone function for Cisco VPN routers**. SoftEther VPN can accept VPN connections from iPhone and Android. The principles of constructing the remote access VPN for smart-phones is exactly same to the Remote Access for PCs. As an additional steps you have to enable the L2TP/IPsec function on SoftEther VPN Server.

Only that, your SoftEther VPN Server can now listening new VPN connections from iPhone and Android.

On each iPhone or Android devices, set up built-in VPN Client to connect to SoftEther VPN Server. Then iPhone or Android can be connected to your corporate network from anywhere at any time.

05.jpg 05 (2).jpg

10.4.10 OpenVPN

SoftEther VPN Server has a "clone function" of OpenVPN. If you have already installed OpenVPN for remote-access VPN or site-to-site VPN, you can replace the current OpenVPN Server program to SoftEther VPN Server program, and you can enjoy the strong functions and high-performance abilities of SoftEther VPN.

The "close function" of OpenVPN on SoftEther VPN Server works same to OpenVPN Technologies, Inc.'s implementation, not only enough but also better performance and functionality. Your OpenVPN Client devices or edge-sites of VPN can connect to new SoftEther VPN Server very easily. You can adopt SoftEther VPN on both remote-access L3 VPN and site-to-site L2 VPN.

The advantages to adopt SoftEther VPN Server instead of old OpenVPN Server program are as follows:

- SoftEther VPN Server has easier configuration than OpenVPN Server by OpenVPN Technologies, Inc.
- You can use Automated OpenVPN Configuration File Generator tool to make a configuration file (.ovpn) for VPN client.
- SoftEther VPN Server supports not only OpenVPN. It supports all standard VPN functions, including SSL-VPN, L2TP/IPsec, MS-SSTP, L2TPv3/IPsec and EtherIP/IPsec. So you can integrate OpenVPN and other protocol's VPN servers into just one VPN Server by using SoftEther VPN Server.
- User administration and security settings can be configured by GUI tools. The management functions are integrated. You can use single-path operation to manage the server.
- All operating system which supports OpenVPN (e.g. Linux, Mac OS X, Linux, UNIX, iPhone and Android) can connect to SoftEther VPN Server.

ss1.2.jpg

You can activate OpenVPN easily with GUI.

IMG_4099.PNG

Not only PC-version OpenVPN. You can also use OpenVPN Client on iPhone / Android.

See Also

- Remote Access to LAN
- 2.2 User Authentication
- 2.2.2 Password Authentication
- 2.2.3 RADIUS Authentication
- 2.2.4 NT Domain and Active Directory Authentication
- 2.2.5 Individual Certificate Authentication
- 2.2.6 Signed Certificate Authentication
- 3.6 Local Bridges
- 3.6.3 Preparing the Local Bridge network adapter
- 3.6.5 Supported Network Adapter Types
- 3.6.6 Use of network adapters not supporting Promiscuous Mode
- 10.2 Common Concepts and Knowledge
- 10.2.1 VPN Server Location