



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.

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](#)