10.10 Your Home PC as VPN Relay for Protect WiFi Using

An individual user can install VPN Server at home to enable access to their home LAN from a remote location. This section will focus on using VPN Server for use as a single user.

10.10.1 Dangers of the Internet and the Need for VPN

The Internet is full of individuals and groups that will attempt to commit illegal acts such as data theft or data manipulation. Many different groups manage the networks that data travels through on the Internet. This means that data could be passed through un-encrypted and leaked at any time.

By using SoftEther VPN even a single user can easily set up a VPN network. They can then easily perform TCP/IP communications such as transferring files or using a remote desktop application through the VPN directly to their home network safely and securely.

10.10.2 Installing the VPN Server at Home

If you have a global IP address at home you can simply install VPN Server on your home computer, then use VPN Client to connect to it through the Internet at a remote location.

10.10.3 Assigning IP Addresses and the DDNS Service

When setting up VPN Server at your home some extra configuration will be required depending on your home network environment (where you receive an IP address assigned by an ISP).

- If your home network is assigned a global static IP address then you can install VPN Server under that IP address and set it to accept connections from the Internet.
- If your home network is assigned a dynamic global IP address (one that changes every time you connect to your ISP) then you will be unable to reliably connect to your VPN remotely. In this case you can use the dynamic DNS service (DDNS service) which will allow you to have a consistent domain name

(hostname) that your dynamic IP address will be registered to. You can then access your VPN remotely through VPN Client by entering that hostname. This type of DDNS service is available on the Internet for free, or for a nominal fee.

- If your home network is assigned a private IP address (which is converted into a global IP address by the ISP's NAT) then unfortunately you will not be able to access your VPN Server at home from the Internet. The only solution in this situation is to either change ISPs or consult with your ISP's system administrator.

10.10.4 Adjusting Settings For Broadband Routers or Other Networking Hardware

If your home network has a broadband router with NAT enabled and the computer you plan on installing VPN Server to is behind that NAT you will not be able to access it directly from the Internet. In this case you will have to configure your NAT settings and use static port mapping, port forwarding, or DMZ to map traffic to a port on your VPN Server computer when a request is made to access it from the Internet. This will allow you to successfully connect to your VPN Server from the Internet.

Please refer to your broadband router's instruction manual for details on how to configure these settings.

10.10.5 Determining the Necessity of Local Bridging

Whether or not you will have to use local bridging on the computer you install VPN Server to depends on the type of VPN you want to set up.

For example, what if you only want to access shared files on a single computer from a remote location, or make a remote desktop connection? In this case there is no need to enable local bridging to connect the Virtual Hub to the physical LAN. You can simply install VPN Client to the computer you installed VPN Server to and have it stay connected to itself (localhost). If you then make a connection to that VPN Server remotely you will be able to communicate with it through its Virtual Network Adapter. If you want to use this method to communicate with a single computer only, you just need to install VPN Server to that computer. Local bridging is not necessary.

If you wish to access all computers on your home network remotely (like the remote access VPN described in section 10.4 Build a Generic Remote Access VPN) you will need to utilize local bridging as described in detail in section 10.4.2 Using Local BridgingEdit section .

10.10.6 Accessing Your Home Network From a Remote Network Safely

Once you have VPN Server installed and properly configured try and connect to through VPN Client from a remote network such as a free wireless access point or a hotel's Internet connection when on a business trip.

If the remote network you will be connecting from routes its traffic through a firewall or proxy server we recommend you set the VPN Server's listener port to **Port 443** (the port used for HTTPS communication). Most HTTP proxy servers or firewalls will allow TCP/IP traffic directed to port 443 pass through.

If you want to use VPN Client on your company's network to access your home network but VPN usage is restricted, you should consult with your network's system administrator beforehand.

10.10.7 Using Electronic Devices that can only Communicate over the same Network

Some types of digital home electronics can only communicate over a local network (the same layer 2 Ethernet segment). For example, a video capture board with a TV tuner may contain software that allows you to watch TV over the network. However, both the client and server must be connected to the same network for this to work. Other examples include HD recorders or DVD recorders that allow the transfer of video only over the same local network.

By using SoftEther VPN you can set up a remote access VPN or LAN-to-LAN VPN and access these types of devices from a remote location over the Internet as if you were directly connected to your network from home.

See Also

- 10.4 Build a PC-to-LAN Remote Access VPN
- 10.4.2 Using Local Bridging