10.2 Common Concepts and Knowledge

This section will look at topics that you need to know about when setting up any type of VPN.

10.2.1 VPN Server Location

VPN Server Reachability at The TCP/IP Level

A VPN Server must deal with connection requests from VPN Clients, VPN Bridges, and, in some situations, from other VPN Servers. Therefore, a VPN Server must be installed to a location that meets the following requirement:

- TCP/IP communication must be possible between the VPN Server and any VPN clients that wish to connect to it. (If you can go through a proxy server or change your NAT settings to allow traffic through certain TCP/IP ports to your private IP addresses then that is sufficient.)

When setting up a VPN network with older VPN protocols such as PPTP or L2TP/IPSec, the VPN server must be a computer with a public IP address to the Internet.

However with SoftEther VPN you don't have to install VPN Server on a computer with a public IP address. VPN Server will work just fine on a computer behind NAT or a firewall in your private IP address space. Please refer to section **10.2 Common Concepts and Knowledge** for more details on setting up a server under these circumstances.

10-2-1.png

10.2.2 Deciding the VPN Server / Virtual Hub Administrator

VPN Server Administrator

When you install VPN Server you must first decide who will be the VPN Server administrator.

- **When the administrator of the server you are about to install VPN Server on will be the same as the VPN Server administrator**
  In this case you can install VPN Server yourself. Once the VPN Server install is completed you will be able to set all administrator passwords.
- **When the administrator of the server you are about to install VPN Server on is not going to be the VPN Server administrator**
  In this case you must request that the server's administrator (root or Administrator) install VPN Server for you. Once the installation has been completed log in locally or remotely to the VPN Server service by using the VPN server administration tool and set all administrator passwords.
  If you are going to operate VPN Server in User Mode (see section 3.2 Operating Modes for more information) and you can log into the server machine as a general user then you can use VPN Server under your own user privileges without asking the system administrator. However, this method is not recommended.

Virtual Hub Administrator

Once you have installed VPN Server you must decide how many Virtual Hubs to create, their names, and what purpose each will serve. If you wish to give Virtual Hub administrator rights to another user then set the Virtual Hub administrator password and give your administrator rights to that user. (See section 3.4 Virtual Hub Functions for more information.)

In most cases the VPN Server administrator will also be administrating the Virtual Hub, so there is no need to give administrator rights to another user.

10.2.3 Changing Existing NAT/Firewall Configurations

Installing VPN Server Behind NAT or a Firewall

If you install VPN Server on a computer in your private network space behind NAT or a firewall, you will have to configure NAT or the firewall to forward data to specific TCP/IP ports on the VPN Server computer. Please refer to your NAT/firewall's manual, or ask your NAT/firewall administrator, to properly set up this configuration.

You must allow TCP/IP traffic to pass through at least 2 of the VPN Server TCP/IP listen ports described in section 3.3 VPN Server Administration. Under most situations we recommend you to open traffic to port 443. The reason for this is that using this port VPN Clients can easily send VPN packets through firewalls or proxy servers masked as HTTPS data.

10-2-2.png

Installing VPN Server Behind NAT or a Firewall.

Using a Reverse Proxy

Another method of installing VPN Server on a computer in your private network space is by utilizing a proxy server. If your network uses a HTTP proxy server to transmit data out to public IP addresses from your private IP addresses then it can also be configured to route data from the Internet through itself to the listen port on the VPN Server sitting in your private network space.

Things To Consider when Installing VPN Server in Your Private Network Space

When using the above methods to install VPN Server in your private network space, always make sure that equipment such as your NAT, firewall, proxy server, etc. will be able to handle the extra load. The NAT and/or firewalls built into inexpensive hardware such as generic broadband routers are usually very slow, so be careful when using these.

If the performance of this hardware is insufficient, your VPN network speed will also suffer a significant speed reduction.

Configuring Hardware that Restricts TCP/IP Traffic

With conventional firewall or NAT hardware you can configure them to allow TCP/IP traffic to pass through at least port 443 (HTTPS). However a few extremely secure

networks will filter data addressed to port 443 from the Internet. In that case, if there is another port which you can route TCP/IP traffic through you can use that port to allow VPN Server to be seen from the Internet. (See section 3.3 VPN Server Administration for more information on how to change port numbers.)

If there is no way to open access to your VPN service under your network configuration you must either request for the firewall to be re-configured or set up a VPN Server computer outside the private network space.

10.2.4 Selecting a User Authentication Method

You must decide on a user authentication method for the VPN Server's Virtual Hub.

Because the user authentication settings used when establishing a LAN-to-LAN cascade connection will usually be completely configured by the system administrator, password verification is a sufficient authentication procedure as long as the password is long enough.

However, if there will be many users logging in to the VPN Server with each entering their own authentication data (such as for a PC-to-PC VPN or a remote access VPN) you must choose your user authentication method wisely. Please refer to section 10.4 Build a Generic Remote Access VPN for more information on selecting an authentication method for remote access VPNs.

For more information on all the user authentication methods utilized by VPN Server, please refer to section 2.2 User Authentication.

10.2.5 Selecting what Functionality to Use

As was explained in Chapter 3. SoftEther VPN Server Manual, VPN Server contains a lot of functionality. However, there rarely comes a time when you need to use all of these features at once.

In most cases you can build a sufficient VPN with only the local bridging functionality to connect the Virtual Hub to a physical LAN (see section 3.6 Local Bridges) and the cascade connection functionality to connect Virtual Hubs together (see section 3.4 Virtual Hub Functions).

However, you may need to use some of the functions listed below depending on the type of VPN you wish to set up. Before configuring the Virtual Hub, you will want to determine exactly what functionality you will need to use for your VPN.

10.2.6 Virtual Layer 3 Switching

You can use Virtual Layer 3 Switching when performing IP routing between multiple layer 2 segments. By placing multiple logical layer 2 segments (Virtual Hubs) within the VPN Server and by separating the IP subnets between Virtual Hubs to a layer 3 level, you can perform layer 3 switching between each network to further partition segments and achieve layer 3 transmission between them. Virtual Layer 3 Switching is especially useful for LAN-to-LAN VPNs when you have a high number of LANs to deal with, or when you want to separate each individual LAN's network.

For more information on Virtual Layer 3 Switching please refer to section 3.8 Virtual Layer 3 Switches.

10.2.7 Virtual DHCP Server

The Virtual DHCP Server functionality is used when there is no DHCP server in a layer 2 segment under a Virtual Hub and you want to assign IP addresses via DHCP to clients connected to that segment. In order to use Virtual DHCP Server you must enable SecureNAT and configure a few other settings. If you only want to use Virtual DHCP Server you do not need to enable Virtual NAT.

Please refer to section 3.7 Virtual NAT & Virtual DHCP Servers for more information about the Virtual DHCP Server functionality.

10.2.8 Virtual NAT

In most enterprise situations you will not need Virtual NAT when setting up your VPN. The only time you may need Virtual NAT would be in the following situations:

- When you wish to communicate with an existing physical LAN via the Virtual Hub but you can not use local bridging. This situation is most commonly encountered when you do not have administrator rights on the target system to install VPN Server / VPN Bridge, or the target system's OS is something other than Windows, Linux, or Solaris.
- When you want to use VPN Server / VPN Bridge for some special situation. (See section 10.11 Exploit SecureNAT for Remote Access into Firewall without Any Permission)

Normally you will just use local bridging to connect a Virtual Hub to a physical LAN to form a layer 2 segment without the use of Virtual NAT.

Please refer to section 3.7 Virtual NAT & Virtual DHCP Servers for more information about Virtual NAT.

10.2.9 Advice about Protocol Conflicts when Making a LAN-to-LAN Connection

Be careful when setting up a LAN-to-LAN VPN that uses both local bridging and cascade connections. If there are DHCP servers running on the previously separated segments then there will be conflicting data sent from those DHCP servers resulting in erroneous data. The solution to this is to use the cascade connection's security policy to filter DHCP packets.

There are also other network services which can not be running more than once on the same network segment.

These types of problems occur when making a layer 2 LAN-to-LAN connection so make sure you find out what kind of services are running on all networks before setting up the VPN.