11.2 Useful Information

This section will provide you with some useful tips and information when using the SoftEther VPN software.

11.2.1 Installing VPN Server With a Variable Global IP Address

If the computer you want to install VPN Server on has a variable global IP address (one that changes each time you connect to your ISP) you can use a dynamic DNS service (DDNS service) to assign a hostname that will always point to the global IP address of that computer. There are a number of free DDNS services available for free on the Internet.

If you plan to install VPN Server on a corporate network, we strongly recommend that you use a static global IP address if at all possible.

11.2.2 Making a VPN Connection to a LAN Consisting of Only Private IP Addresses

If you are installing VPN Server to a LAN that only has private IP addresses, you will have to configure the NAT, proxy server, or firewall that converts the private IP address into a global IP address to perform port mapping or static NAT to the VPN Server.

Also, if your VPN Server is on the Internet you can set up a VPN Bridge that stays connected via a cascade connection to the VPN Server. This will allow remote access VPN clients to access the layer 2 network within the LAN by going through the VPN Server on the Internet. This method makes it possible to connect to a LAN that only has private IP addresses from a remote location. For this configuration a VPN Bridge will be connected to the LAN you want to connect to remotely via a local bridge connection, as well as to the VPN Server on the Internet via a cascade connection.

Furthermore, if your LAN only has private IP addresses and VPN Bridge can only be installed with system administrator rights, you can still set up a remote access VPN by using SecureNAT. (See section 10.11 Exploit SecureNAT for Remote Access into Firewall without Any Permission for details.) In this case, you are dealing with a LAN that has many limitations imposed upon it, but by utilizing SecureNAT you should be able to enable remote access to the LAN without the need for any administrator rights. However, you will still need to receive permission to do so from the network's administrator beforehand.

11.2.3 The way of Using Basic DHCP Server in Virtual Hub

VPN Server and VPN Bridge of virtual Hub have basic DHCP server function. When this DHCP server function is enabled, client computers connected to layer 2 segment of virtual Hub are assigned IP addresses, and receive notification of default gateway and the address of DNS server. The way of using basic DHCP server, see 3.7 Virtual NAT & Virtual DHCP Servers.

11.2.4 Using an IPv6 over IPv4 Tunnel

You can create an IPv6 over IPv4 tunnel easily with SoftEther VPN. An IPv6 over IPv4 tunnel encapsulates IPv6 packets into IPv4 packets, allowing IPv6 packets to be sent between LANs when traffic must pass through areas that only allow IPv4 packets to pass through.

Many older IPv6 over IPv4 tunneling technologies could not pass through NATs or firewalls. However, SoftEther VPN encapsulates all network traffic at the layer 2 (Ethernet) level. This allows even IPv6 packets to be processed as VPN traffic.

Therefore, you can use SoftEther VPN to provide IPv6 over IPv4 tunneling solutions for nearly every type of network environment.

11.2.5 About Wake On Lan (WOL)

If you use SoftEther VPN to set up your remote access VPN or LAN-to-LAN VPN, you can start a computer on the network remotely by sending a Wake On Lan (WOL) packet to that computer's physical network adapter.

11.2.6 Installing VPN Server Behind a NAT Enabled Router

If you are installing VPN Server behind a consumer or small business targeted generic broadband router or a router with a built-in firewall that contains NAT functionality, you will have to configure it properly for VPN Server to work. You can enable static NAT or port mapping on the router so that traffic from the Internet will be forwarded to a port on the VPN Server, allowing it to be accessed from the Internet. Please refer to your broadband router's instruction manual for more information on how to achieve this.

11.2.7 Using an IDS to View Packets Going In/Out of a Virtual Hub

You can use the following two methods to view all of the Virtual Ethernet frames going through a Virtual Hub with an IDS or virus scanning system in order to search for unauthorized access attempts or viruses.

1. Connect to the Virtual Hub from VPN Client in monitoring mode. This will enable the VPN Client's Virtual Network Adapter to capture all packets going through the Virtual Hub. Now you can use snort or some other IDS software on the Virtual Network Adapter to view the packets going through the Virtual Hub. For more information please refer to 1.6 VPN Communication Details and 4.4 Making Connection to VPN Server. However, this method only allows for the use of a software based IDS.
2. By using the method described in section 3.6 Local Bridges, you can out all of the packets going through the Virtual Hub from the LAN port of the physical network adapter connected to the computer running VPN Server. This method will allow you to use hardware based IDS to view all of the packets going through a Virtual Hub.

While it is possible to monitor all frames, if there is so much traffic that the Virtual Hub's buffer is nearly full then the network adapter you output to may lose some of the data due to the limitations of that network adapter.

11.2.8 Recreating a Switch's Port VLAN Functionality

VPN Server can achieve the same functionality as the VLAN functionality (which groups multiple ports by a VLAN number, and communicates through these VLAN numbers only) found on commercial layer 2 switching Hubs or layer 3 switches. By creating Virtual Hubs for each section of a segment you want to separate, traffic will be separated between these Virtual Hubs. By using this method you can recreate the same functionality provided by a switch's port VLAN functionality. You can also maintain the MAC address table database and other administrative settings for each Virtual Hub in this way.

11.2.9 Hello World !

So be it.

11.2.10 Performing Administration Via TELNET as Supported in SoftEther 1.0 (old version)

With SoftEther 1.0 (old version), you could perform Virtual Hub administration with TELNET. You can use TELNET or SSH to perform administration on SoftEther VPN Server as well. For this, you will need a separate TELNET or SSH server. (Operating systems such as UNIX or Windows 2000 and higher usually come with a TELNET or SSH server already.) From the administrative console you can connect to the server you want to perform administration on. Then, in that console session you can execute vpncmd which will allow you to perform administrative tasks through TELNET or SSH. Please see section 6. Command Line Management Utility Manual for more information on how to use vpncmd.

11.2.11 Increasing Cluster Controller Redundancy

As described in section 3.9 Clustering, VPN Server's clustering capabilities will automatically introduce fault-tolerance between the cluster member servers. However, the standard capabilities of VPN Server do not implement any fault-tolerance for the cluster controller itself. Therefore, if the cluster controller has a power failure, hardware failure (such as a memory error), or some other failure, the cluster controller's job can not automatically be transferred to another computer. We strongly recommend that you use Registered ECC memory, RAID, UPS, and other such features to increase the stability of your cluster controller server if you are setting up a large scale cluster.

You can implement the following ideas in a shell script or other program, or seek a commercial solution to increase redundancy for your cluster controller.

1. Set aside two machines for your cluster controller computer: one as your main machine, and one as a backup.
2. Ensure that both computers have the same operating system, hardware configuration (network adapter, etc.), and VPN server type installed.
3. While your main server is running, periodically backup the contents of the VPN Server configuration file (vpn_server.config) to a backup device.
4. If your main server fails due to a power failure, hardware failure (such as a memory error), or some other failure, you can detect this and begin operation of your backup server. Set the backup server's global IP address to that of your main server and use the latest backup of your VPN Server configuration file to start the VPN Server service. You will need to be careful here to avoid conflicting with the main server's IP address. With this method you can set up a temporary cluster controller as a backup with the same configuration data as your main cluster controller that can take over in the case of a hardware failure.
5. When you have finished repairing your main server you can copy the latest configuration file back to it and put it back into operation as your main cluster controller.

6. Implement the ideas written above in a shell script or other program, or use a commercial solution to increase redundancy and test your system thoroughly.

11.2.12 When Limiting Computers which Access to Virtual Hub not only Username but also Physical IP Address

As described in 3.5 Virtual Hub Security Features, you can limit computer access not only username but also physical IP address.

11.2.13 The Way of Selecting Encryption Algorithm with SSL Communication

When connecting to VPN Server, the encryption algorithm with SSL encryption session uses RC4-MD5 by default. You can change the encryption algorithm which has longer bit length than that. In detail, see 3.3 VPN Server Administration.

11.2.14 About Tagged VLAN

The detail about using tagged VLAN packet on virtual Hub and localbridge connection function when using VPN Server and VPN Bridge, see 3.6 Local Bridges.

11.2.15 The Way of Changing the MAC Address of Virtual Network Adapter

The MAC address of virtual network adapter on VPN Client can be changed. The way of changing, see "Changing Advanced Setting" of 4.3 Virtual Network Adapter. you can also change the setting with **NicSetSetting** of vpncmd command.

11.2.16 The Way of Changing the Communication Speed Reported to Windows

The virtual network adapter of VPN Client reports a communication speed as 100Mbps to windows. This value can be changed at will. In detail, see "Changing Advanced Setting" of 4.3 Virtual Network Adapter.

11.2.17 The Way of not Saving Password of the Connection Settings of VPN Client

When connecting to VPN Server with VPN Client, you can enter a password with password authentication not to save one. In detail, see "Information Required for Standard Password Authentication and RADIUS or NT Domain Authentication" of 4.4 Making Connection to VPN Server.

11.2.18 Connecting to Multiple VPN Servers or Virtual Hubs at Once

You can create multiple Virtual Network Adapters and connection configurations with VPN Client and designate each connection configuration to use a separate Virtual Network Adapter. This allows a single VPN client computer to easily connect to multiple VPN Servers or Virtual Hubs at the same time. This is the same concept as if you installed multiple physical network adapters to your computer and connected each one to a different LAN. Please refer to section 4. SoftEther VPN Client Manual for more information.

11.2.19 Using SecureNAT to Provide Remote Access to an Otherwise Inaccessible Network.

By using SecureNAT you can easily provide remote access to a network which normally can not be connected to from the Internet. You can even do so without having administrator rights on the computers on that network. However, you will still need permission from that network's administrator beforehand. Please refer to section 10.11 Exploit SecureNAT for Remote Access into Firewall without Any Permission for more information.