11.3 General Supplementary Information

This section will give you some general supplementary information we think you should know when using the SoftEther VPN software.

11.3.1 Using This Software Together With Anti-Virus Software or a Personal Firewall

You need to be aware of the following things when using SoftEther VPN alongside third party anti-virus software or a personal firewall.

- Many personal firewalls will block any incoming TCP/IP connections to the computer once it is installed. In this state you will not be able to install VPN Server. When you install VPN Server make sure you configure your personal firewall to allow access to the listener port used by VPN Server.
- In some cases you will be unable to make a TCP/IP connection to localhost (your own computer) after installing some personal firewalls. Therefore, you may be unable to make a connection to VPN Client with VPN Client Manager. If this is the case, try disabling your personal firewall.
- If you ever feel that SoftEther VPN is not operating properly, try temporarily disabling any third party anti-virus software or personal firewall or uninstalling them completely to see if that fixes the problem. If that does solve your problem, your third party anti-virus software or personal firewall is not compatible with SoftEther VPN.
- If this is the case, you may have to disable the third party software or uninstall it completely in order to use SoftEther VPN.

11.3.2 About the 1/1000 Second Delay Encountered When Communicating Over a VPN

When using SoftEther VPN to perform VPN communication, you may experience a 1/1000 second delay when compared to communicating directly over a physical line. This delay is due to the time it takes to encrypt and encapsulate data (Virtual Ethernet frame) sent over the VPN, and is processing time that is absolutely necessary for the VPN system. However, it will not cause any problems during standard use.

11.3.3 NTLM Authentication Support for Connections Via Proxy Server

At this time SoftEther VPN does not support NTLM authentication when routing through a HTTP proxy server. Therefore, if your setup requires NTLM authentication on an old

version of Microsoft Proxy Server you will need to change this setting in order to access the proxy server with basic authentication or no authentication at all.

11.3.4 How Far Away Can You Establish a VPN Session Connection From?

SoftEther VPN encapsulates Ethernet frames when it performs any communication over a VPN. Normal Ethernet standards do state a maximum distance for a single Ethernet segment due to the electrical characteristics of the physical line. However, as SoftEther VPN encapsulates all Ethernet frames and sends them over existing IP networks, there is technically no limitation to the distance between LANs that you can perform a VPN connection, given that you have access to the Internet. However, if you plan on sending data to the other side of the earth there will be approximately a 140 millisecond delay or more due to the physical limitations of the speed of light when making this type of extremely distant connection.

11.3.5 I measured the throughput of traffic through my VPN with my usual measurement utilities, and they are showing very low transfer speeds. What's wrong?

If you are receiving low speed results from your current speed measurement software or throughput measurement service, try the Communication Throughput Measurement Tool that comes with SoftEther VPN or vpncmd's TrafficClient/TrafficServer functions to try and obtain the correct throughput of your VPN. Please refer to section 4.8 Measuring Effective Throughput for more information. Be aware that older throughput measurement software can especially give varying results based on the type of line it is testing.

11.3.6 The Difference Between VPN Bridge's SecureNAT and VPN Server's SecureNAT

The SecureNAT program in SoftEther VPN Bridge and the SecureNAT program in SoftEther VPN Server are exactly the same. They have the same capabilities and are logically no different at all.

11.3.7 Can a single user open multiple VPN sessions?

A single user account can open multiple VPN sessions at the same time.

11.3.8 According to the Windows end user license agreement, is it OK to use a client based operating system such as Windows XP as a VPN server?

If you are planning to use Windows XP, Windows Vista, Windows 2000 Professional, or other such operating system designed for clients to run SoftEther VPN Server as a VPN server machine, the issue of whether or not the Windows EULA allows this is between the consumer involved and the manufacturer, Microsoft. This issue does not involve SoftEther in any way. For your reference, please refer to the following passage from the Windows XP Professional SP1 EULA under "1.3 Device Connections": "You may permit a maximum of ten (10) computers or other electronic devices (each a "Device") to connect to the Workstation Computer to utilize one or more of the following services of the Software: File Services, Print Services, Internet Information Services, Internet Connection Sharing and telephony services. ... This ten connection maximum does not apply to other uses of the Software, such as synchronizing data between a Device and the Workstation Computer, provided only one user uses, accesses, displays or runs the Software at any one time". This means that if you are using functionality other than that provided by Windows XP (such as by installing and using SoftEther VPN Server) you may allow more than 10 computers to connect without violating the terms of the EULA.

11.3.9 Things to Consider When Using Windows 98. 98 SE, or ME as a VPN Server

SoftEther VPN Server will run on any Win 9x system higher than Windows 98. However, due to the instability of these operating systems we do not recommend them for use as a VPN server computer. If you want to run a VPN server, we recommend using an operating system with a newer kernel such as Windows NT/Windows 2000 and higher or Linux.

11.3.11 About MAC Addresses Starting With "00:AE"

All Virtual Hubs have a MAC address that begins with "00:AE". This MAC address is used as the origin of the ARP polling packets sent by Virtual Hubs as described in section 3.4 Virtual Hub Functions.

11.3.12 How MAC Addresses Are Assigned to Virtual Hubs

The MAC address assigned to a Virtual Hub is determined by hashing some information of the computer running VPN Server (such as the computer's hostname or physical IP address) and attaching "00:AE" to the beginning of that value. Therefore, even if you restart VPN Server the Virtual Hub's MAC address should stay the same.

11.3.13 Naming Computers Running VPN Server

When you set up a clustered VPN you must choose a different computer name or hostname for each computer running VPN Server.

11.3.15 VPN Server Computer Specifications and the Number of Possible Simultaneous Connections

The theoretical maximum number of simultaneous connections that can be handled by VPN Server is 4,096. However, the problem is not limitations with the software, but limitations with the hardware (such as CPU speed limitations or memory limitations). Therefore, we always recommend limiting the number of simultaneous connections to less than this theoretical maximum. If you expect a large number of simultaneous connections, you should think about using clustering to handle the load.

SoftEther does not provide an exact number of simultaneous connections possible for different hardware configurations. However, you can estimate that a computer with a 2.8 GHz Pentium 4 processor and 1 GB of RAM could handle anywhere from 200 to 1000 simultaneous sessions. However, the amount of load on the VPN Server can vary greatly depending on the type of data and volume of traffic on the VPN, so these numbers are only an estimation.

11.3.16 Determining When to Use Clustering and Load Balancing

VPN Server's clustering functionality is always capable of adding a new node (cluster member server) to the cluster without having to shut down the cluster. Therefore, if you are unsure as to how many VPN Servers to put in place when you are designing your network, start with just two. If you find that the load on one or both of the servers is too high, you can simply add another VPN Server to the cluster to lower the load. You can continue this process until you find out exactly how many VPN Server machines you need.

11.3.17 When Using a Special PPPoE Connection Tool to Connect to the Internet

If the VPN client computer you installed VPN Client to uses a special PPPoE connection tool (the most common are those distributed by ISPs, but they are not the only kind) to connect to the Internet, the routing table controlled by that software and the routing table controlled by VPN Client may conflict with each other. In this case processes like the one described in section 4.4 Making Connection to VPN Server may not function properly. If this applies to you, try using a broadband router that supports PPPoE to connect to the Internet instead of the PPPoE connection tool.

11.3.18 Things to Consider When Using Your Operating System to Make a Bridged Connection Between a Virtual Network Adapter and a Physical Network Adapter

As explained in section 3.6 Local Bridges, using SoftEther VPN to make a local bridge connection between a Virtual Network and a physical network is the quickest and easiest way to set up a VPN. However, you can also use the bridging functionality built into Windows or Linux to connect a Virtual Network and a physical network together into a single segment. However you will need to be using an operating system that supports bridged connections. For Windows, this would be Windows XP Professional or higher, editions of Windows Vista that support bridged connections, or Windows Server 2003 or higher. Even if you use this method you should still set aside a new network adapter for the sole purpose of this bridged connection.

11.3.19 What if the Virtual Network Adapter and the physical network adapter both have the same network address?

Try to avoid a network configuration where the Virtual Network Adapter on your VPN Client computer is on the same IP network as the physical network adapter, or partially overlapping. This would be the same mistake as a computer that has two physical network adapters and connecting each one to the same IP network, then connecting each one to a different layer 2 network segment.

11.3.20 How is the Virtual Network Adapter's MAC address generated?

The default MAC address for a Virtual Network Adapter will automatically be determined when it is created. The user can change a Virtual Network Adapter's MAC

address to anything they want at any time. Please refer to section 3.4 Virtual Hub Functions for more information on how to change the necessary settings to do so.

11.3.21 Are Virtual Network Adapters' MAC addresses unique?

MAC addresses for Virtual Network Adapters begin with "00:AC". The address after this consists of a random string created by hashing a combination of the time that the adapter was created and unique parameters obtained from the other computer. Therefore, the chance that two Virtual Network Adapters on the same layer 2 segment will hold the same MAC address is without a doubt extremely low.

11.3.22 Things to be aware of when using SSH port forwarding software to connect to a VPN server

Are you trying to use third party SSH port forwarding software to connect to a remote VPN Server via a SSH server? Are you trying to connect to localhost via VPN Client, then forward ports from localhost to the remote VPN Server? If you are attempting these types of special connections, you should create a static route with the physical network as the default gateway beforehand to the remote computer your computer will actually directly connect to (for SSH port forwarding this would be the SSH server). Otherwise, the Virtual Network Adapter would be the default gateway. If this is the case, once the VPN Client establishes a connection, connection to the SSH server would also attempt to pass through the Virtual Network Adapter. This, of course, will not allow you to communicate with the SSH server and thus not allow for VPN communication either.

11.3.23 Concerning the priority of default gateways when one exists on both the Virtual Network Adapter network and on the physical network

When using Windows 2000 or higher and there are default gateways set up on both the VPN Client side and the physical network, the network adapter with the lower interface metric value will generally have the higher priority. Because there can be only one default gateway active at once, any other routing tables pointing to 0.0.0.0/0 will temporarily be deleted. (If that VPN connection is disconnected it will automatically be restored.) The default interface metric for Virtual Network Adapters is 1. This gives them higher priority over normal network adapters that usually have interface metrics of 1020 or 30.

11.3.25 If you are unable to create a Virtual Hub with VPN Bridge...

VPN Bridge has a single Virtual Hub with the name of **"BRIDGE"** by default. This Virtual Hub is for defining local bridge connections, configuring cascade connections to VPN Servers, and other VPN bridge software functionality. Therefore, VPN Bridge does not allow the creation of new Virtual Hubs. Please refer to section 5.3 Differences between VPN Server and VPN Bridge for more information.

11.3.26 If you are unable to use local bridging in FreeBSD, Solaris, or Mac OS X...

Due to internal differences between FreeBSD, Solaris, and Mac OS X from Windows or Linux, local bridging is not supported on these versions at the time of the writing of this manual. Local bridging may become available for these operating systems in the future.

11.3.27 Connecting to a VPN Bridge Listener Port From VPN Client

As explained in section 5. SoftEther VPN Bridge Manual, VPN Bridge can not accept connections from VPN Client like VPN Server can. If you do attempt this type of connection you will receive the message "Not supported".