11.1 Troubleshooting

This section will describe common problems encountered when using SoftEther VPN and how to solve them. Please look over the information presented here and attempt to fix any problems you can before contacting technical support.

11.1.1 Programs Suddenly Terminate during Normal Operation.

In some cases, a SoftEther VPN program's process will suddenly terminate without warning. If this occurs, confirm the following:

- Check to see if the program's executable file (an EXE file under Windows) is corrupted or if it has been overwritten. If the contents of executable files such as vpnserver, vpnclient, or vpnbridge have been modified, they may not function properly. If you think a program's executable file may be corrupted, re-install SoftEther VPN.
- Check to see if the files necessary to execute the program (such as hamcore.se2, etc.) are corrupted. If you think a file may be corrupted, re-install SoftEther VPN.
- Check to see if there is a problem with your computer's physical memory. If you are using inexpensive, low quality memory in your computer, it may cause programs currently running to crash. We recommend using a memory checking tool such as memtest86 to test for any possible memory defects. For computers that are required to be highly reliable such as a server machine, we recommend using ECC or Registered ECC memory.
- If you are running resident software such as a personal firewall or an anti-virus program, try temporarily disabling that software. If, upon disabling this software, the program in question stops crashing and begins behaving normally, that third party software is likely the cause of the problem.

If you have tried all of the above suggestions but your problem has not been solved, please contact technical support.

11.1.2 I am unable to communicate with the IP address of the Virtual Network Adapter used for local bridging from within the VPN.

In some cases, communication can not be established from VPN Server or VPN Bridge to the IP address assigned to the physical network adapter connected to by the bridge from

the Virtual Hub even when the Virtual Hub is connected to the physical network adapter by a local bridge connection. Some possible causes of this are as follows:

- From Windows 2000 on, this type of problem may occur right after defining a local bridge that connects to a network adapter with hardware offloading capabilities. If this is the case, try restarting your computer. Please refer to section 3.6 Local Bridges for more details.
- If you are using Linux or Solaris, you can communicate within the Virtual Hub (VPN) from the network adapter connected to by the local bridge to the LAN, but you can not communicate to the network adapter itself. This is a restriction imposed by the Linux kernel. For more information please refer to 3.6 Local Bridges.
- If you are using local bridging to make a bridged connection between a Virtual Hub and a physical LAN as described in section 3.6 Local Bridges, we recommend you set aside a network adapter specifically for this purpose. This will result in the best performance when using local bridging.

11.1.3 A Protocol Error is occurring.

In some cases, a protocol error will occur when connecting to a VPN Server over the Internet from a VPN Client or a cascade connection. If this happens, check the following:

- Check to make sure that the host name or IP address of the VPN Server you are trying to connect to is correct. Also, make sure the TCP/IP port number is the same as the VPN Server's listener port. Furthermore, confirm that that listener port is not being used by some other server software (such as a webserver like IIS or Apache). Please refer to section 3.3 VPN Server Administration for more information.
- The global address of the connecting computer to be recognized by VPN Server may not have reverse DNS lookup configured.
- If there is a proxy server, transparent firewall, or some other special networking devices between the connecting computer and the VPN Server, these devices may misinterpret the SoftEther VPN protocol and write over it or block it completely. In this case, check with the administrator of these networking devices.
- If your network uses a HTTP proxy or SOCKS proxy, check with the proxy server's administrator to confirm if the proxy can be used to forward the SoftEther VPN protocol.

11.1.4 I am getting the message "The time on the server and the client does not match".

If the time set on the VPN Server and that of the connecting VPN client computer are significantly different from each other, the message [The time on the server and the client

does not match.] may be displayed. If this occurs, check to see if the clocks on both computers are set to the correct time, and correct them if they are not.

11.1.5 I am getting slow transfer speeds when using Windows file sharing on the VPN.

You may experience slow transfer speeds when uploading or downloading files over a VPN from a remote location in the following cases:

- **If there is a network delay of 10 milliseconds or higher on the physical network between the two LANs.**
  The Windows file sharing protocol is based on the NetBIOS protocol used in LAN Manager which is over 10 years old. When Windows file sharing is used between computers on the same segment (with a network delay of 10 milliseconds or less) the protocol allows for fast file transfer speeds. However, if it is used over the Internet with a network delay of 10 milliseconds or higher, the file transfer throughput decreases. This delay is not due to SoftEther VPN. No matter what VPN system is used, the delay over the physical network's lines can not be reduced due to their physical limitations.
- **If the transfer speed or throughput between the LANs is unstable and each packet incurs some packet loss.**
  The Windows file sharing protocol is greatly affected if there is jitter in the network delay between LANs and the throughput between them is often changing.
- **Your Windows domain controller is also a file server and downloads/ uploads to that file server are slow.**
  If Windows 2000 Server or Windows Server 2003 is your domain controller open the [Control Panel] and go to [Administrative Tools]. Here, open [Local Security Policy] or [Domain Controller Security Policy]. Under [Local Policy] find [Security Options] and check to see if **[Microsoft network server: Digitally sign communications (always).]** and **[Microsoft network server: Digitally sign communications (if client agrees).]** are enabled. If they are, disable them and restart the file server. You should notice a big improvement in file transfer speeds.

The above problems are almost all caused by problems such as not enough throughput over the physical network or too high of a network delay. To solve these problems you may need to contact your network administrator or increase your network's bandwidth in order to decrease network delay.

When using the Windows file sharing protocol, making the following changes to the registry on the computer acting as a file server and restarting it can significantly improve communication throughput on a network with high delays. This configuration must be done in a registry editor. Only a system administrator or someone knowledgeable about

computers should make these changes. Be sure to make a backup of the registry before making any changes.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\param
"Size"=dword:00000003
"SizReqBuf"=dword:0000ffff
```

Making the above changes to the registry and restarting Windows may improve the transfer speed of the file sharing server. If you do not understand the above information, please do not modify the registry with any registry editor.

11.1.6 There is a large number of broadcast packets constantly being sent over the network. What should I check?

In some cases, when setting up a SoftEther VPN there will be a large number of broadcast Ethernet frames being sent within the Virtual Hub or within the physical LAN connected to the Virtual Hub via a local bridge. If this occurs, check the following:

- If there are Virtual Hubs making cascade connections to each other, make sure a layer 2 loop is not occurring.
- Check to make sure there is not a layer 2 loop occurring in your physical connections.
- If a Virtual Hub is connected to two or more physical network adapters by a bridge connection, make sure those network adapters are not connected to the same layer 2 segment.
- If you are using SoftEther VPN's Virtual Hub with local bridging or SecureNAT, check your overall network topology very carefully to make sure there are no layer 2 loops occurring.

11.1.7 The CPU load increases after enabling Virtual NAT for SecureNAT.

SecureNAT may not be configured properly. Check to make sure the following things are not occurring on your network. Also check the items listed in section 3.7 Virtual NAT & Virtual DHCP Servers.

- If your computer has SecureNAT enabled as well as local bridging, check to see if the physical network adapter connected to via the local bridge is obtaining an IP address from a DHCP server.

- Check to see if the computer with SecureNAT enabled is not routing its communication through SecureNAT itself, creating an infinite loop. (This often happens when VPN Client is installed on the same computer and is connected to localhost, creating a loop.)

The SecureNAT functionality is designed for creating a simple remote access VPN under special circumstances (see section 10.11 Exploit SecureNAT for Remote Access into Firewall without Any Permission), and therefore we do not recommend it for continuous use in a corporate setting. Remember, SecureNAT is not required to set up a normal LAN-to-LAN VPN or remote access VPN.

11.1.8 Protocols that use many broadcast packets are not working properly.

In some cases, protocols that use many broadcast packets (broadcast Ethernet frames) such as gaming systems, home digital appliances, etc. may not work properly when used over a SoftEther VPN. If this occurs, check the following:

- Check to make sure that you have not enabled a security policy that has a broadcast limit in the security policies for VPN Client or for any cascade connections you need for your VPN. Note that the default policy does have a broadcast limit enabled. Please refer to section 3.5 Virtual Hub Security Features for more details.
- If you are using local bridge connections, the physical network adapter connected to via the local bridge or that segment's layer 2 switching Hub may not be able to handle the large number of broadcast frames and will fail to forward them properly.

11.1.9 Multicast packets are being dropped.

In some cases, multicast packets sent through a SoftEther VPN may not function properly. If this occurs, check the following:

- Multicast packets will be treated the same as a broadcast packet by a VPN Server's Virtual Hub. Check to make sure that you have not enabled a security policy that has a broadcast limit in the security policies for VPN Client or for any cascade connections you need for your VPN. Note that the default policy does have a broadcast limit enabled. Please refer to section 3.5 Virtual Hub Security Features for more details.
- If you are using local bridge connections, the physical network adapter connected to via the local bridge or that segment's layer 2 switching Hub may not be able to handle the large number of broadcast frames and will fail to forward them properly. Your layer 2 switching Hub/router, or layer 3 switch may not recognize multicast packets and may be filtering them out.

All multicast packets at the layer 2 level will be broadcast to all VPN sessions by the Virtual Hub. Even if a VPN Server on a remote access VPN wants to send a client connected to it a multicast packet, the Virtual Hub will individually encapsulate that packet for each session. Therefore, it is technologically impossible to reduce traffic by using multicast technology. Also, be aware that the Virtual Hub and Virtual Layer 3 Switch does not process IGMP packets.

11.1.10 Even though I have installed VPN Server and connected to it from outside the network, I still can not connect to the local network.

In most cases, if you have installed VPN Server, configured the Virtual Hub, and are connected to the VPN Server remotely via VPN Client but you can still not use the VPN, the problem is a forgotten local bridge connection between the Virtual Hub and the physical network adapter.

- Refer to section 3.6 Local Bridges and configure a proper local bridge connection.
- For a simple remote access server you can also use the Virtual NAT functionality as described in section 3.7 Virtual NAT & Virtual DHCP Servers.

11.1.11 I forgot my VPN Server's administrator password.

If you have forgotten the administrator password for your VPN Server, refer to 3.3 VPN Server Administration and delete the following lines from the VPN Server configuration file with a text editor:

```
declare ServerConfiguration
{
        uint64 AutoDeleteCheckDiskFreeSpaceMin 104857600
        uint AutoSaveConfigSpan 30
        string CipherName RC4-MD5
        bool DisableDosProction false
        byte HashedPassword ******* (hashed password data)
```

As written above, by deleting the **[HashedPassword]** field under the **[ServerConfiguration]** node you can reset the VPN Server password to an empty password.

11.1.12 Hello!

Hi, Hello!

11.1.13 RADIUS authentication is not functioning properly. What should I check?

If you are unable to use RADIUS authentication, refer to section 3.5 Virtual Hub Security Features and confirm the following:

- Make sure that your RADIUS server has your VPN Server's IP address (as seen from the RADIUS server) registered as a RADIUS client and the shared secret is set correctly.
- Check that the RADIUS server can use the Password Authentication Protocol (PAP).
- Look in the RADIUS server's log file to see if an authentication attempt from the network device "SoftEther VPN Server" was recorded. If there is no such log entry, the connection to the RADIUS server is failing. If there is a log entry use the details in the log to troubleshoot the problem.
- Try connecting to the RADIUS server from another RADIUS client to check if it is functioning properly. If other RADIUS clients can not be authenticated through the RADIUS server either, the problem is likely something on the RADIUS server.

11.1.14 NT Domain or Active Directory authentication is not functioning properly. What should I check?

If NT Domain or Active Directory authentication is not functioning properly, check the following:

- Confirm that the OS running VPN Server is Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, or Windows Vista (excluding Windows XP Home Edition or Windows Vista Home Basic/Home Premium) and that it belongs to the Windows domain you want to use for Active Directory authentication.
- Check to see if the VPN Server process is running in service mode.

If you have performed all of the above actions and NT Domain or Active Directory authentication still is not functioning properly, try performing a clean install of the operating system on the computer you want to run VPN Server. Join the domain again and see if you still get the same error as before.

11.1.15 Setting the listener port to port 443 always gives an error.

If you use VPN Server Manager or vpncmd to check the status of VPN Server or VPN Bridge after you have started the service and port 443 as the listener port is always showing an error, check the following:

- Check to see if there is another resident process (such as a webserver using HTTPS like Apache or IIS) currently active. If another process is already using port 443 you will have to configure that program to use a different port or configure VPN Server to use a port other than port 443.
- If you are using the Linux or UNIX version of VPN Server or VPN Bridge, check to see if it is running in general user mode. Due to the limitations set by these operating systems, general users other than root can not use any port lower than port 1024.

11.1.16 I added a local bridge but it is always offline or showing an error.

If you have defined a local bridge connection but it is always offline or showing an error, check sections 3.6 Local Bridges and the following:

- Check if the Virtual Hub instance you have defined as a local bridge connection exists in the VPN Server. If it does not exist, the status will stay as offline until it does.
- Confirm that the device name of the physical network adapter you have designated for the local bridge to connect to is correct. The local bridge status will stay offline if the device name does not exist or if it has been disabled by the operating system. You may have made a typo in the device name, especially when using a program like vpncmd to add local bridge connections from the command line.
- Also confirm that the physical network adapter you have designated for the local bridge to connect to is being recognized by the operating system and functioning properly.

11.1.17 The local bridge to my wireless network adapter is not functioning properly.

If you have defined a local bridge connection between a Virtual Hub and a wireless network adapter but the local bridge is not functioning properly, refer to section 3.6 Local Bridges.

11.1.18 I created a Virtual Layer 3 Switch but it is always offline or showing an error.

If you have created a Virtual Layer 3 Switch, defined a Virtual Interface to a Virtual Hub, and started it up but it remains offline or shows an error, refer to section 3.8 Virtual Layer 3 Switches.

11.1.19 I have set up a cluster but I can not communicate between Virtual Hubs on the cluster.

If you have set up a cluster but can not communicate between Virtual Hubs you have made on the cluster, refer to section 3.9 Clustering. Also verify that you have correctly set up and configured the cluster as described in section 10.8 Build a Large Scale Remote Access VPN Service.

If you have set up a cluster and only want to allow communication within each individual Virtual Hub (such as for a Virtual Hub hosting service VPN Server as described in section 10.9 Build a Large Scale Virtual Hub Hosting Service), make sure that you have made your Virtual Hubs dynamic, not static.

11.1.20 I am not performing any communication over the VPN, but packets are being sent to the Internet periodically.

Even if you have not established a VPN connection the VPN Client sometimes sends some packets through the physical network interface. These packets are described in section 4.9 Other Functions. (You can modify some settings to stop VPN Client from sending these packets.)

If you have established a VPN connection and a VPN session, but are not performing any communication over the VPN, any communication you may see between VPN Client and the VPN Server is most likely the following type(s) of packets:

- Packets for ARP polling by the Virtual Hub as explained in section 3.4 Virtual Hub Functions.
  (By setting the [NoArpPolling] option in the configuration file to 'true' you can stop ARP polling from occurring.)
- Packets sent by the SoftEther VPN protocol to confirm the existence of each TCP/IP connection, or KeepAlive packets sent to prevent the TCP/IP connection from timing out. The interval that KeepAlive packets are sent by the TCP/IP connections that make up the SoftEther VPN protocol is approximately half of the timeout interval defined in that VPN session's security policy.

11.1.21 After I have created a Virtual Network Adapter I get the message, "No network cable is connected".

If you create a Virtual Network Adapter with VPN Client, you must be connected to a VPN Server its status will stay as [No network cable is connected.]. This is the same as if an Ethernet cable is not connected between a physical network adapter and a switching Hub. Please refer to section 4. SoftEther VPN Client Manual for more information on this topic.

11.1.22 I forgot my password for VPN Client.

If you have forgotten the administrator password for your VPN Client, delete the following lines from the VPN Client configuration file vpn_client.config with a text editor:

```
declare root
{
        bool DontSavePassword false
        byte EncryptedPassword ******* (hashed password data)
        bool PasswordRemoteOnly false
        uint UseSecureDeviceId 1
```

As written above, by deleting the **[EncryptedPassword]** field you can reset the VPN Client password to an empty password. Remember to stop the VPN Client service before overwriting the vpn_client.config file.

11.1.23 My Windows 98 Second Edition or Windows Millennium Edition system becomes unstable when I use a Virtual Network Adapter.

There are many problems with Windows 98 Second Edition and Windows Millennium Edition as they are legacy operating systems. These operating systems differ from Windows NT/2000 or later operating systems in that they are fundamentally extensions of MS-DOS and consist internally of many 16-bit processes.

The kernel in these operating systems is old and unstable. Therefore, while it is possible to install SoftEther VPN Client and create a Virtual Network Adapter under these systems, we do not recommend using them for prolonged use. If you plan on maintaining a VPN connection on these systems for a long period of time, there is a chance it will become unstable, unable to communicate over the network, and eventually result in a

blue window error. SoftEther does not support VPN Client if it is run on the Win 9x kernel.

11.1.24 I uninstalled VPN Client but my Virtual Network Adapter is still there.

Any user modified files, Virtual Network Adapters, and configuration data created after VPN Client is installed are not automatically deleted and thus remain on the system even after VPN Client is uninstalled. If you want to delete the configuration files (vpn_client.config) or Virtual Network Adapters registered to your system, delete them manually when you are sure that you do not need them anymore. Please refer to section 8.3 Uninstall SoftEther VPN Client for information on how to delete a Virtual Network Adapter.

11.1.25 I am having trouble when using a smart card.

If you are having problems when using a smart card or hardware security device with SoftEther VPN, check the following:

- Make sure that the device driver(s) for your smart card reader, etc. and PKCS #11 drivers necessary to access the smart card are installed properly. After you have installed new drivers for your smart card you must restart your computer in order to use that device with SoftEther VPN.
- Confirm that the correct smart card type is selected. Please refer to section 4.6 Using and Managing Smart Cards for more information.
- Some smart card drivers will not function properly if there are multiple smart card readers on your system. Make sure you read the manual for your smart card to determine if these limitations exist.
- Some smart card drivers require you to use a separate utility to format the smart card before it can be used. Refer to your smart card's manual for instructions on how to do this.

11.1.26 I am unable to create a Virtual Network Adapter with VPN Client under Linux.

If you are using VPN Client under Linux and are unable to create a Virtual Network Adapter, check the following:

- Confirm that the Universal TUN/TAP device is supported in your kernel, and that it can be accessed as the file /dev/net/tun.
- Confirm that you are running the vpnclient process with root access.

11.1.27 My VPN connection is disconnected when I designate the Virtual Network Adapter as the default gateway in VPN Client under Linux.

The Linux VPN Client does not support automatic adjustment of the routing table. Therefore, when you make a VPN connection to VPN Server on a remote computer with VPN Client in Linux and use the router on the network connected to by the Virtual Network Adapter (tap device) as your default gateway, TCP/IP communication tries to pass through that default gateway as well. To solve this problem, you have to use the route command to add a static route to the VPN Server. Only use the Linux VPN Client if you are comfortable with these types of operations dealing with TCP/IP and routing.

11.1.28 I forgot my VPN Bridge's administrator password.

You can reset the administrator password for VPN Bridge by using the same method used for VPN Server. Refer to section 11.1.11, changing vpn_server.config to vpn_bridge.config where appropriate.

11.1.29 I have connected LANs together with bridge connections using VPN Server and VPN Bridge, but I still can not communicate between computers on the LANs. What should I check?

If you have used the methods described in section 10.5 Build a LAN-to-LAN VPN (Using L2 Bridge) to connect multiple network segments together with a layer 2 connection by using VPN Server and VPN Bridge, but can still not communicate between the computers on these networks, use the following method to determine if the networks are properly connected at a layer 2 level.

1. If you are dealing with two LANs you can try this test. Set up one computer on LAN A with an unused IP address (for example, 192.168.222.1) and a computer on LAN B with an unused IP address on the same IP network as the computer you set up on LAN A (such as 192.168.222.2). Now try the ping command on both computers to see if they can ping each other. If they succeeded in communicating with each other, both networks are properly connected at a layer 2 level and the problem lies in the configuration of the rest of the computers. Remember that both LANs are logically functioning as a single Ethernet segment, so check settings such as TCP/IP, etc. very carefully.
2. If the computers failed to communicate with each other by using the method above, you have probably made a mistake somewhere in the process of setting up your LAN-to-LAN VPN. In this situation, refer to sections 10.5 Build a LAN-to-

LAN VPN (Using L2 Bridge), 3. SoftEther VPN Server Manual, or 5. SoftEther VPN Bridge Manual and confirm your VPN configuration.

3. If each LAN has a different IP network structure and you want to allow communication between the computers on each LAN, refer to the method described in section 10.6 Build a LAN-to-LAN VPN (Using L3 IP Routing).

11.1.30 I am getting a warning message in syslog stating that ARP packets are being received from the IP address "0.0.0.0" when using local bridging under FreeBSD.

This is caused by polling packets sent from a Virtual Hub to confirm the existence of an IP address.

Some operating systems (such as FreeBSD) will not respond to an ARP request packet from 0.0.0.0 and will instead report that an unauthorized ARP request packet from 0.0.0.0 was received in a log file such as syslog.

Normally you can just ignore this message with no problems, but if there are many FreeBSD machines on the same segment this could cause problems for the administrator of those machines. In this situation you can stop these polling packets from being sent. For instructions on how to stop a Virtual Hub from sending polling packets to confirm the existence of an IP address, please refer to section 3.4 Virtual Hub Functions.