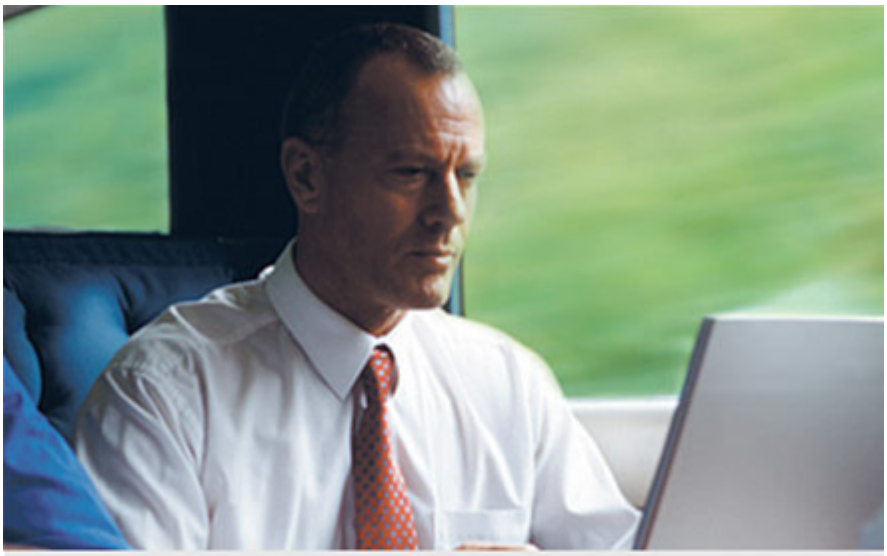
VPN End to End – Netgear VPN Router ProSafe VPN Client – Appendix B

Appendix B: Netgear VPN Router ProSafe VPN Client

Technical Notes for use with Vodafone Mobile Connect services

Date: **29 May 2007**

Revision No: **3.0**



Vodafone Mobile Connect

VPN Guide

© VODAFONE GROUP 2007

Scope

This document presents results of installation, configuration, and operations testing of VPN components with the Vodafone Mobile Connect service. The document is not intended to be a tutorial on VPN concepts nor does it supersede or replace the vendor's documentation. The reader is referred to the VPN vendor for definitive guidance on the proper and recommended use of their product. While Vodafone Group has taken care to ensure that the information contained herein is accurate, no responsibility can be accepted for errors, omissions, or inaccuracies.

Document History

Version	Date	Reason
1.0	October 2003	Initial release using GPRS network. Client documentation included in main document.
2.0	June 2006	Creation of separate document for client configuration. Update to new versions of VPN software and focus on 3G network performance.
3.0	May 2007	Minor changes & R9 updates

File Reference

VPN_Netgear_FVS318_Appendix_B_Client.doc

Document Authors

Peter Jäger, TECON Terenci

Document Distribution

Public via websites of Vodafone, its Affiliates, and its Partner Networks

© Vodafone Group 2007.

Other than as permitted by law, no part of this document may be reproduced, adapted, or distributed, in any form or by any means, without the prior written consent of Vodafone Group Plc.

Contents1 ..... Executive summary 4

2 VPN Client Installation and Configuration (Netgear ProSafe VPN Client 10.1) 5

2.1 VPN Client System requirements.....5

2.2 VPN Client installation 6

2.3 Configuring a new Client connection (Netgear ProSafe VPN Client 10.1) 9

2.4 Name Resolution 14

3 Configuring VMC Software for VPN Usage 15

3.1 Establish the connection (VMC R9) 15

3.2 Establish the connection (VMC R7 and earlier) 16

3.3 Establish the VPN 16

4 Configuring the VPN Client 17

4.1 Automatic Start-up 17

4.2 Keep-alive Frequency 18

4.3 Export a Profile configuration file 18

5 Connections to Different Services.....19

5.1 Connect to MS Exchange mail server / Outlook.....19

5.2 Connect to file server 20

6 Logging 21

6.1 Logging Client (client side).....21

6.2 Connection Monitor (client side).....21

Tables & Figures

Figure 1 – Mapping Network Drive for VPN Access 20

Figure 2 – File Transfer between LAN and local drives 20

© VODAFONE GROUP 2007

1 Executive summary

This Appendix B is in addition to the detailed document for Netgear VPN Router-ProSafe VPN Client and describes the set up process in a detailed way with example screen shots taken from the initial processes. It is a companion guide to 'Appendix A: VPN_Netgear_FVS318_App A.doc' providing additional detail beyond that covered in the VPN Overview document for Netgear FVS318.

- Initial installation of the client software is reviewed.
- Configuration of the VPN client using sample parameters is illustrated
- The default configuration for the client is to start up automatically when a target address is referenced, although this can be modified to require manual start-up
- As the VPN client starts automatically, no special steps are required for integration with Vodafone Mobile Connect software
- Frequently used configuration settings are illustrated
- Connections to corporate applications and file servers are illustrated

© VODAFONE GROUP 2007

2 VPN Client Installation and Configuration (Netgear ProSafe VPN Client 10.1)

The Netgear ProSafe VPN Client can be installed on a Windows Workstation. A user needs Administrator rights to install the software on the local machine. This client can be used to establish a VPN connection to the Netgear VPN Router firewall/VPN appliance. Other VPN Clients have to be de-installed.

The Netgear ProSafe VPN Client uses the "Deterministic Network Extender" (DNE) Package of Deterministic Networks, Inc.

2.1 VPN Client System requirements

Verify that your computer meets these requirements[1]:

- A single, Pentium®-class processor or its equivalent.
- One of the following operating systems[2]:
  - Microsoft® Windows® 95 (build 950B and 950C only)
  - Microsoft® Windows® 98, or Windows 98 (second edition)
  - Windows ME
  - Windows NT 4.0 (with Service Pack 4, or higher)
  - Windows 2000 Professional
  - Windows XP Professional or Home Edition
- Native Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.)
- Microsoft Internet Explorer 4.0 or later
- 10 MB hard disk space.
- RAM:
  - 16 MB for Windows 95
  - 32 MB for Windows 98 or NT
  - 64 MB for Windows ME or 2000
  - 64 MB / 128 MB recommended for Windows XP

[1] These are minimum requirements to run the client software but won't provide satisfactory performance in typical office configurations.

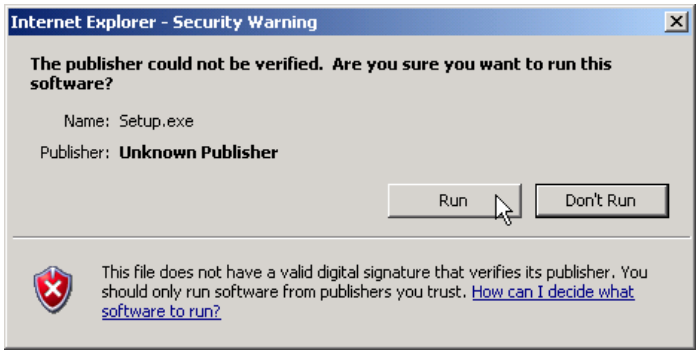
[2] Note that early versions of Microsoft® Windows® are no longer supported by VMC software.

© VODAFONE GROUP 2007

- To install the VPN Client:
  - CD-ROM drive, network drive or web site
  - Administrator privileges if installing on Windows NT or Windows 2000
- To use the VPN Client:
  - Direct network connection (cable, WLAN or DSL modem and network adapter/interface card)
  - Internal or external non-encrypting modem if dial-up connection
  - Native Microsoft PPP dialer if dial-up connection
  - PPPoE drivers if DSL is used
- To connect using a digital certificate for authentication:
  - A digital certificate signed by a Certificate Authority (CA) installed on your PC

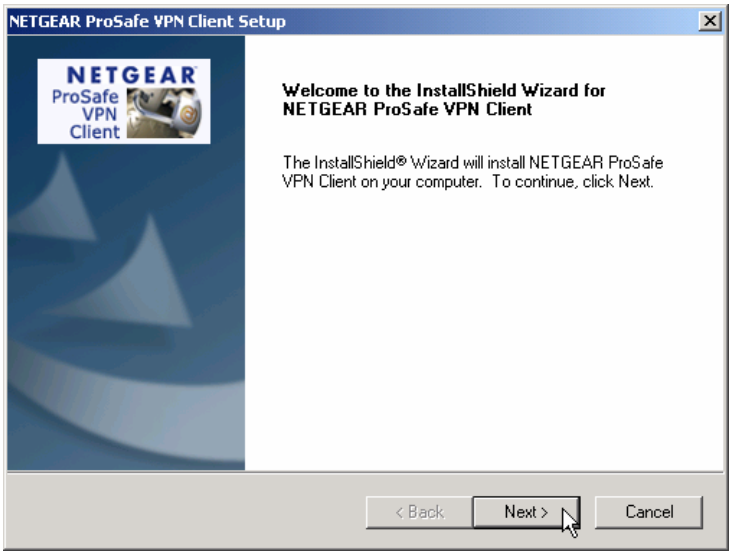
2.2 VPN Client installation

- Run the installation program ("Setup.exe") according to the directions given by the program. There may be warnings from the Microsoft Windows XP SP2 Security Center, which can be safely ignored.

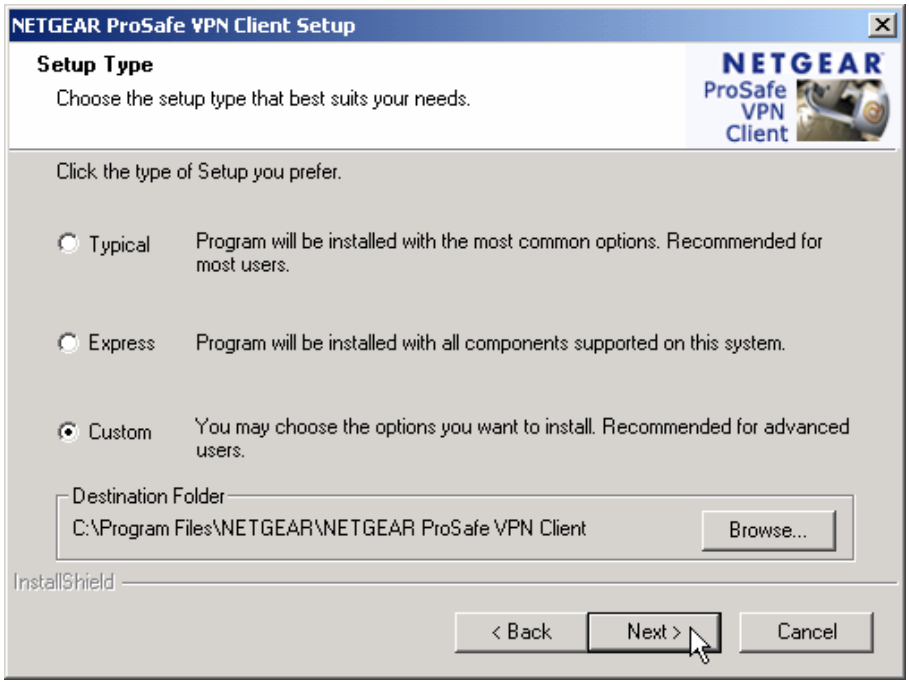


Following slides shows the Netgear ProSafe VPN Client 10.1 installation:

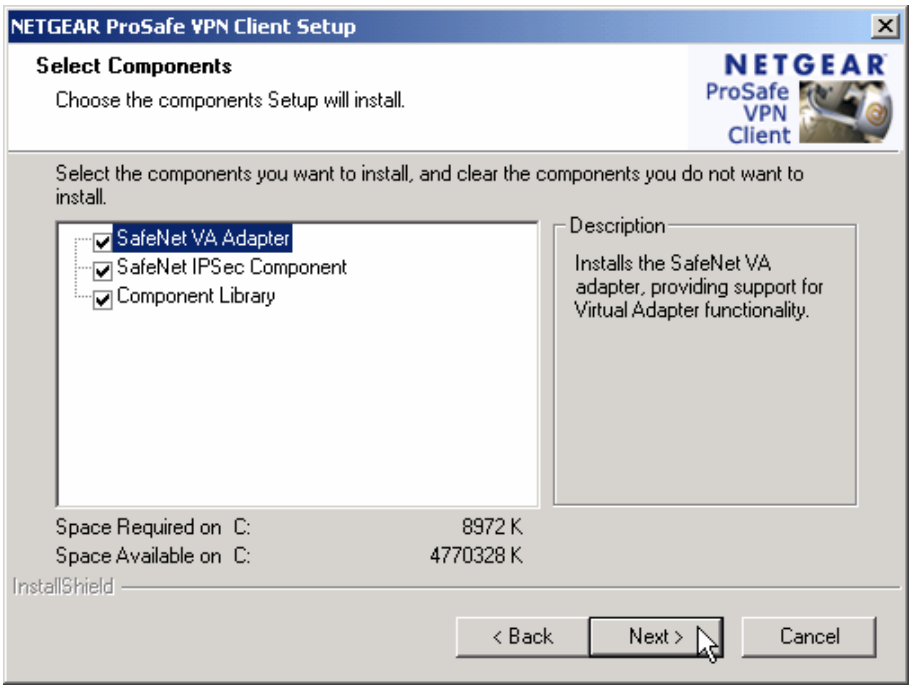
- At the "Setup" window click "Next"



- Follow the screens for “License Agreement” and “Setup Type and Destination and Program Folders” and install the Netgear ProSafe VPN Client.

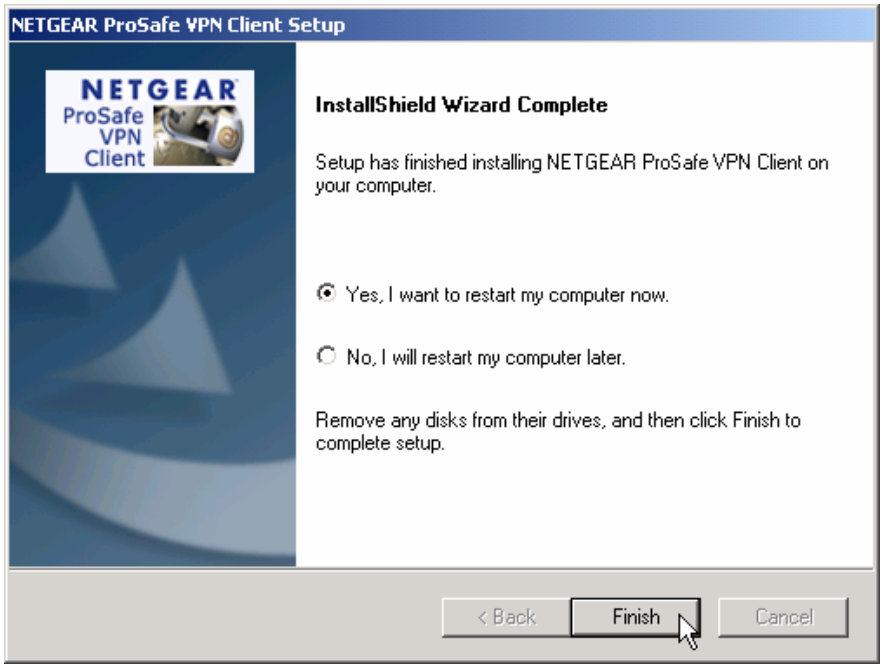


- If custom installation is selected, the “Select Components” screen is shown. Select all components.



- Confirm the selected settings in the next screen and the setup will start. Make sure any unsigned driver warnings are confirmed to install the driver anyway. These warnings may appear behind a screen and may not be visible. If the installation seems to stop, minimize the visible windows and look for a driver installation warning.
- A Deterministic Network Enhancer will be installed on all available network adapters. Additionally Netgear ProSafe VPN Client 10.1 creates a new network adapter.

- After completing the installation, the system will ask you to reboot the system.



- After the reboot, the Client is automatically started and is displayed in the system tray.

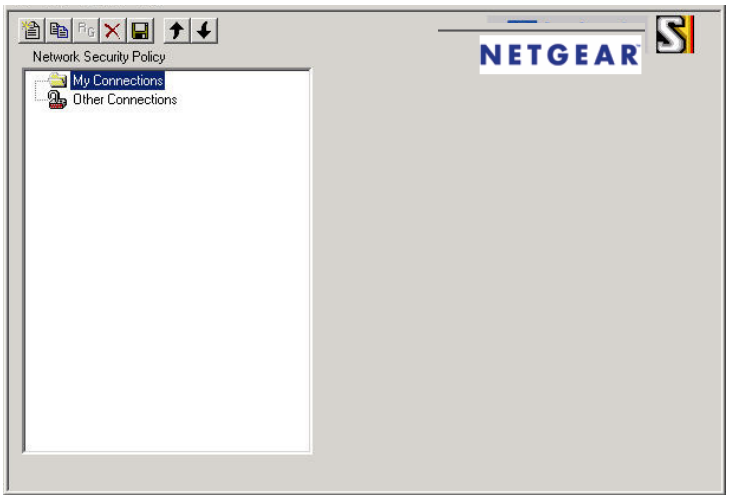
2.3 Configuring a new Client connection (Netgear ProSafe VPN Client 10.1)

In this example, the client is configured for a typical scenario. Here, a shared secret is used for the initial connection to the gateway. The user is identified by a username and password. The client is configured to set up a virtual network interface. Unlike in more expensive VPN systems, the parameters for each user must be entered on the client side.

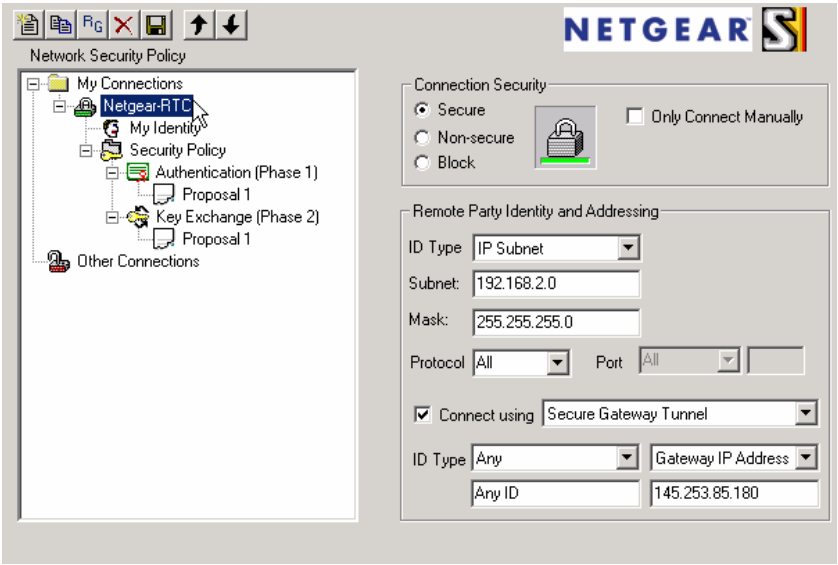
The advantage of the virtual network interface is, that within the corporate network, a well defined address range can be assigned to remote users, so that routing and firewalling of VPN client users is possible.

The setup here is matched to the configuration of the Netgear appliance described in the document in appendix A: “VPN_Netgear_FVS318_App A.doc“

- Start the Profile Editor from the Program menu at “Programs > Netgear-ProSafe VPN Client > Security Policy Editor”

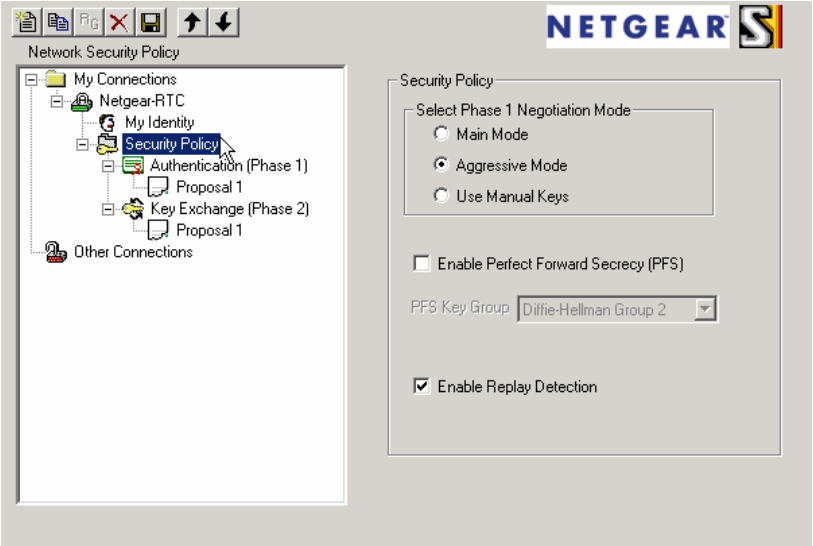


- Click on the “Add a new connection” icon on the left to define a new profile
- Rename the profile by clicking on the connection name once. Set the ID Type at the top of the Remote Party Identity and Addressing” box to “IP Subnet” and enter the subnet to which you want to send the encrypted data. Check the checkbox in front of “Connect using” and select “Secure Gateway Tunnel”. The ID Type here is Any / Gateway IP Address. Enter the external IP address of the Netgear VPN Router you want to connect to.



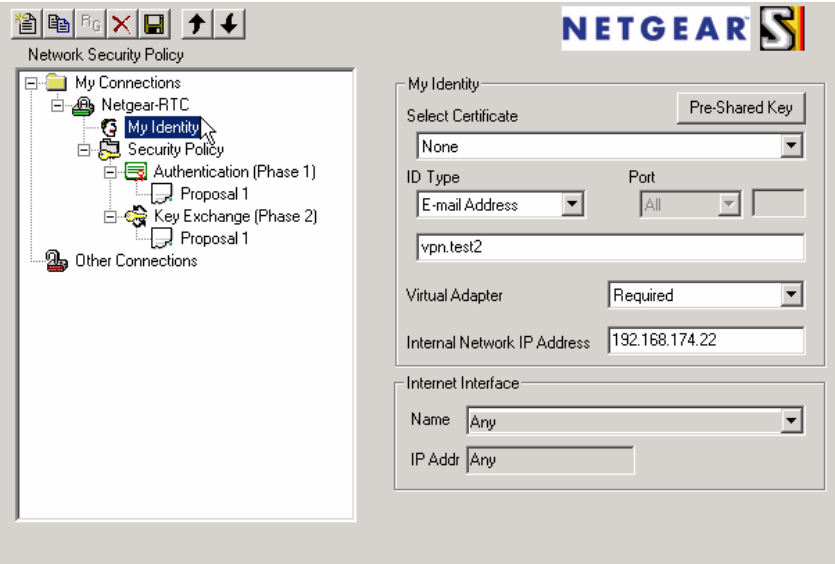
- Open the menu “**Options > Global Policy Settings**”. Set the Retransmit Interval to 45 seconds. Make sure that “Allow to Specify Internal Network Address” and “Send status notifications to peer hosts” are checked. For debugging purposes, check “Enable IPSec Logging”.

- Next, click on “Security Policy” entry in the connections tree to edit the Security Policy. Select “Aggressive Mode” for Phase 1 Negotiation. This is required for authentication with shared secret on a Netgear device. Selecting “Aggressive Mode” will enable the “ID Type” “E-mail Address”
  Here, PFS is not enabled to simplify the example. Replay detection may be checked.

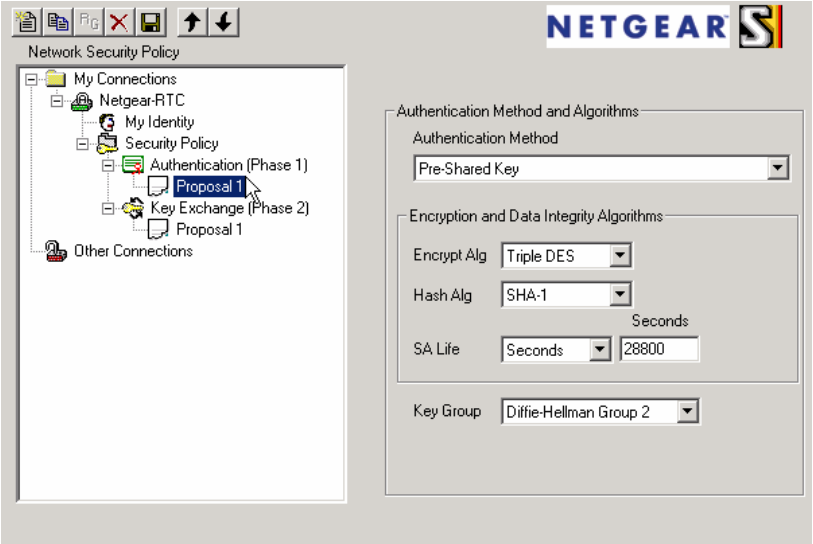


- Next, make sure the connection is expanded and click on “My Identity” to edit the Identity tab. The “ID Type” is set to “E-mail Address” and in the edit field, the same string as on the Netgear appliance is entered. Click on “Pre-Shared-Key” to enter the same key as in the gateway configuration of the Netgear appliance. Set the “Virtual Adapter” setting to “Required”.

© VODAFONE GROUP 2007

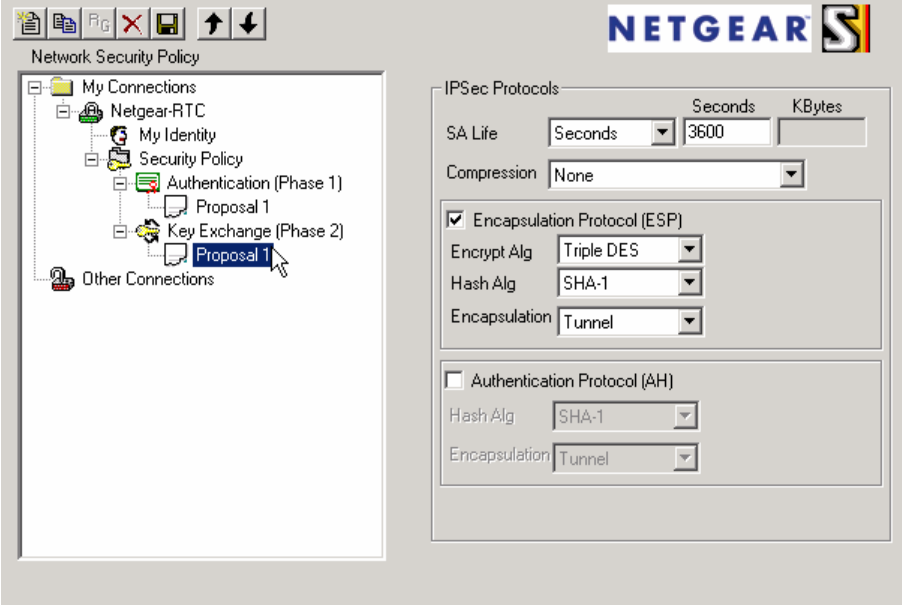


- Next, click on “Proposal 1” entry below “Key Exchange (Phase 1)” in the connections tree to edit the first IPSec Phase 1 (IKE) Encryption setup. More than one proposal is possible and a fitting one will be negotiated during connection establishment, but since both sides are known, the first proposal should fit the requirements. As “Authentication Method”, select “Pre-Shared Key”. **Make sure the encryption parameters (Encrypt Alg, Hash Alg, SA Life, Key Group) exactly match the settings on the Netgear appliance, otherwise the connection will fail.**



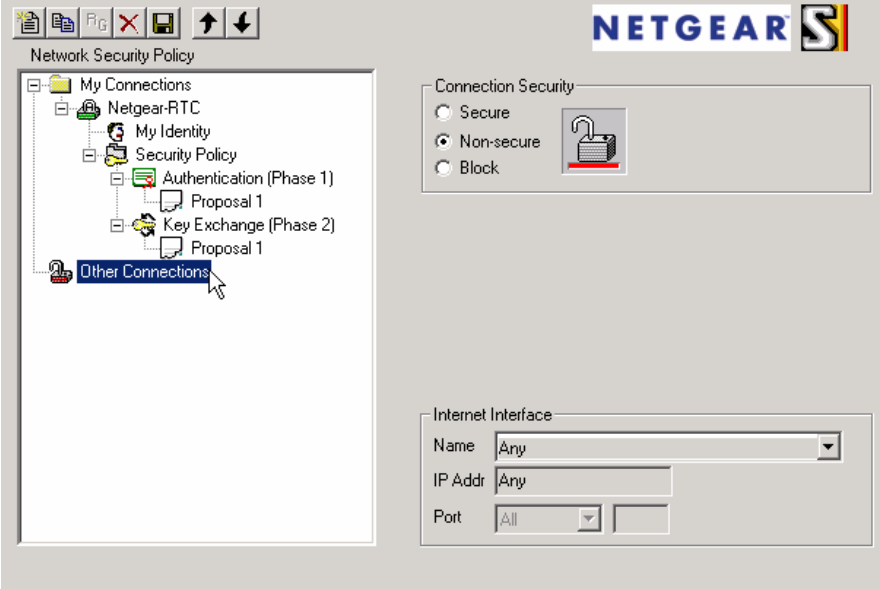
- Next, click on the “Proposal 1” entry below “Key Exchange (Phase 2)” in the connections tree to edit the first IPSec Phase 2 (ESP) Encryption setup. Again, more than one proposal is possible. Compression must be switched off since it is not supported on the Netgear appliance. Set the Encapsulation to “Tunnel”. Make sure the

encryption parameters (Encrypt Alg, Hash Alg, SA Life) exactly match the settings on the Netgear appliance, otherwise the connection will fail.



- Next, click on the “Other Connection” entry in the connections tree. Here, the unencrypted connection settings can be configured. If Split Tunnelling is needed, set the Connection Security setting to “Non-secure”. This will allow unencrypted internet traffic as well as encrypted traffic to the corporate.

We recommend blocking all unencrypted traffic by selecting “Block”. As long as the security policy is loaded, this will ensure that no unencrypted connection to the internet is possible.



2.4 Name Resolution

Unfortunately the client does not receive any DNS or WINS server IP addresses from the appliance during the connection phase and therefore the client is not able to resolve internal VPN host names to IP addresses. This means that the user has to add all needed internal VPN hosts names and their IP addresses manually to the hosts file of Windows, which can be found in either 'C:\WINDOWS\system32\drivers\etc' or in 'C:\WINNT\system32\drivers\etc'. A sample entry would look like this:

192.168.2.10rtcex01.rtc.vf-globallab.com

Please note that some applications may need the fully qualified host name and some others only the host name without the domain. It is possible to enter both variants if unsure.

© VODAFONE GROUP 2007

3 Configuring VMC Software for VPN Usage

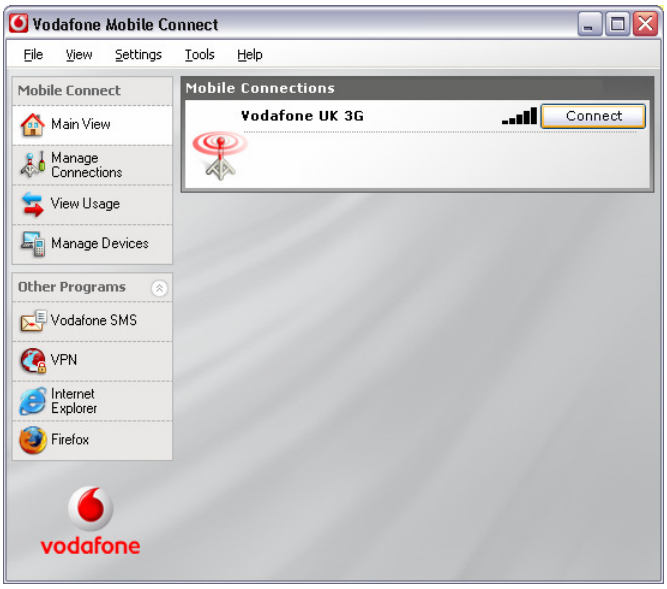
The Netgear VPN client is installed as a system utility and runs transparently whenever the computer is started. The client is accessed via the icon in the Windows Notification Area (System Tray). As the client is always running, there is no need (and it is not possible) to configure the VPN button in the Vodafone Mobile Connect software to launch the client.

3.1 Establish the connection (VMC R9)

The new R9 of Vodafone Mobile Connect software offers the same features as earlier versions but with a different user interface.

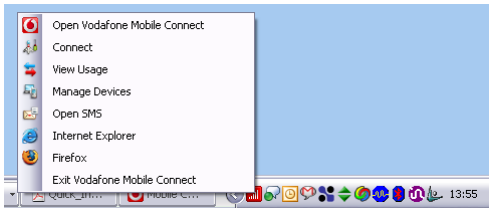
With a SIM card inserted into your datacard (or USB modem), to establish a connection:

1. In the main view, use the **Connect** button, or



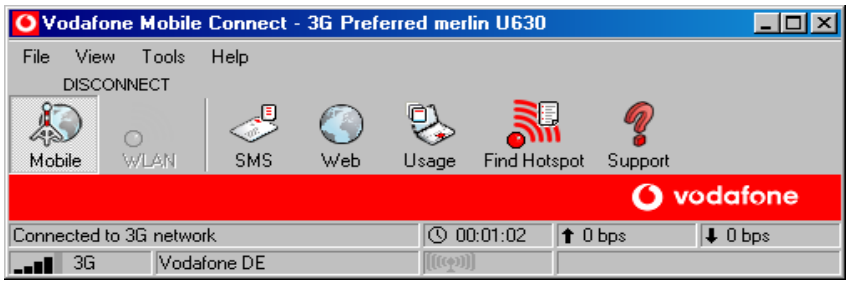
2. In the mini-view, use the **Connect** button, or

3. From the Windows Notification Area (system tray), right-click and select **Connect**.



3.2 Establish the connection (VMC R7 and earlier)

Note: The following steps apply to the legacy version of Vodafone Mobile Connect software R7 and earlier.



- First you need to build up a connection using your VMC. Insert SIM and PCMCIA card and open the Vodafone Mobile Connect application.
- Press the **Mobile** button in the CONNECT/DISCONNECT area of the toolbar

3.3 Establish the VPN

As the Netgear ProSafe VPN client is placed into the system tray by default, there is no need to configure the Vodafone Mobile Connect software for the VPN, see appendix B for further details.

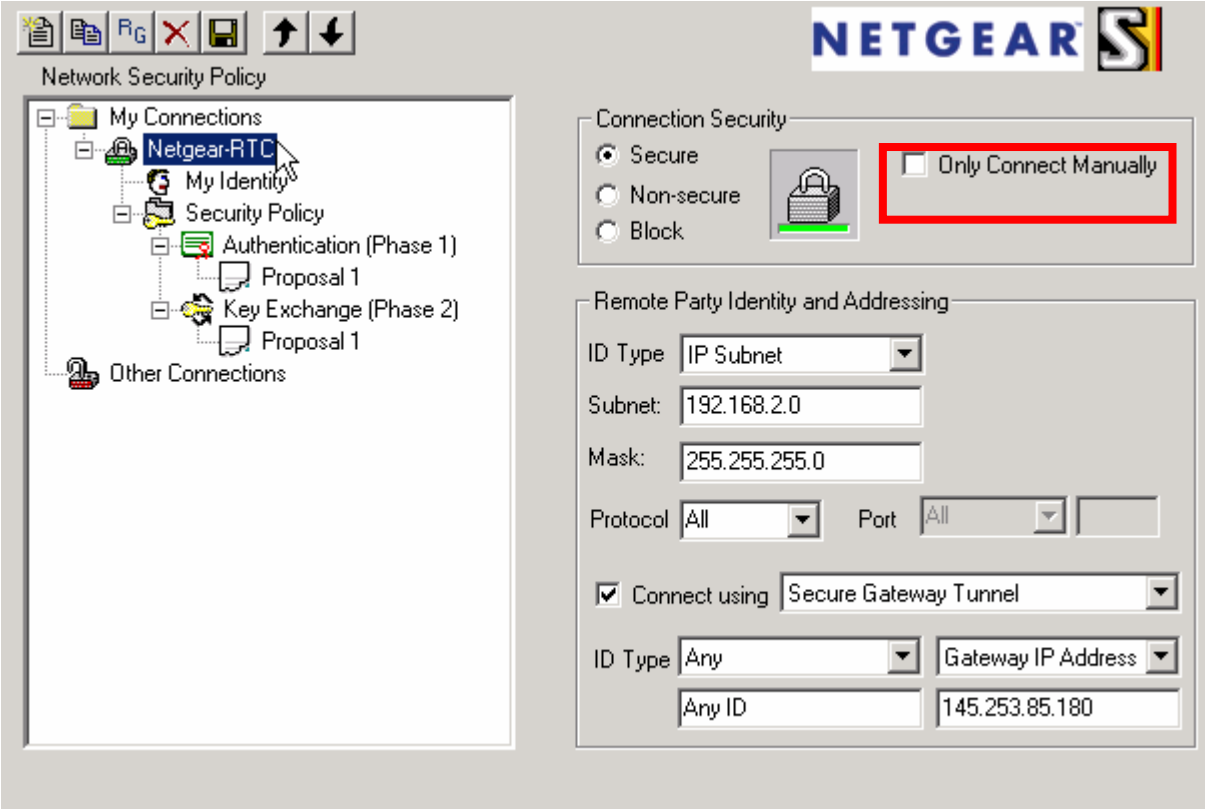
After you build up your preferred connection, the Netgear ProSafe VPN Client is able to connect to the remote gateway automatically. Make sure that the Netgear ProSafe VPN Client is running in the system tray.

Optionally, the VPN connection can be forced to start by right-clicking the Icon in the system tray and select “Connect… > MyConnections\<VPN Connection Name>”. Since the authentication parameters are configured in the client, no additional user authentication is necessary.

4 Configuring the VPN Client

4.1 Automatic Start-up

By default, Netgear ProSafe VPN Client will be started from the “Programs > Start up” on Windows-start up. Further, the client will connect automatically when an application tries to connect to it’s server in the corporate network. This behaviour can be changed in the Policy Editor if editing of the policy was not disabled by the administrator.



If the “Only Connect Manually” checkbox is checked, the connection must be initiated manually.

Start the connection by right-clicking the Icon in the system tray and select “Connect… > MyConnections\<VPN Connection Name>”.

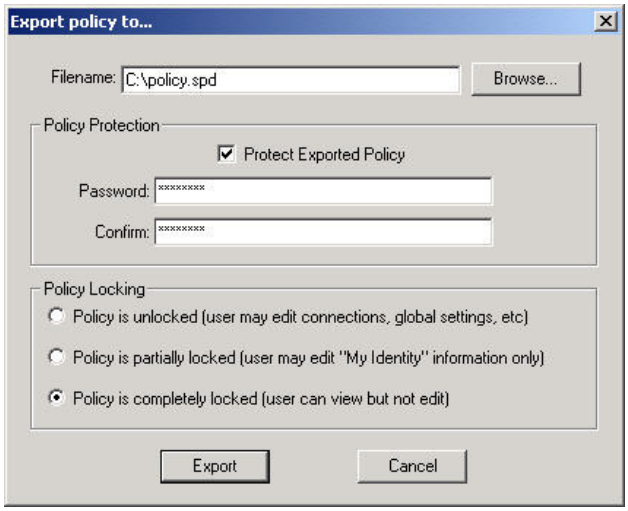
4.2 Keep-alive Frequency

If NAT-Traversal is activated, as is necessary with most countries using GPRS and 3G services, the Keep-alive packet frequency defaults to 20 seconds. Unfortunately, this setting cannot be changed.

4.3 Export a Profile configuration file

Working profiles can be exported from the Netgear ProSafe VPN Client Policy Editor into a policy file. When exported, the administrator can decide if the policy will be editable after import or not. Further, the policy can be protected by a password.

- Start the Netgear ProSafe VPN Client Policy Editor from menu “Programs > Netgear ProSafe VPN Client > Security Policy Editor”.
- Select “File > Export Security Policy”. There, select a file name and optionally a password. Further, it can be selected if the user should be able to edit the policy after import.



Export the policy by clicking “Export”.

5 Connections to Different Services

You can connect to all services via the VPN tunnel that you can connect to while in your local LAN.

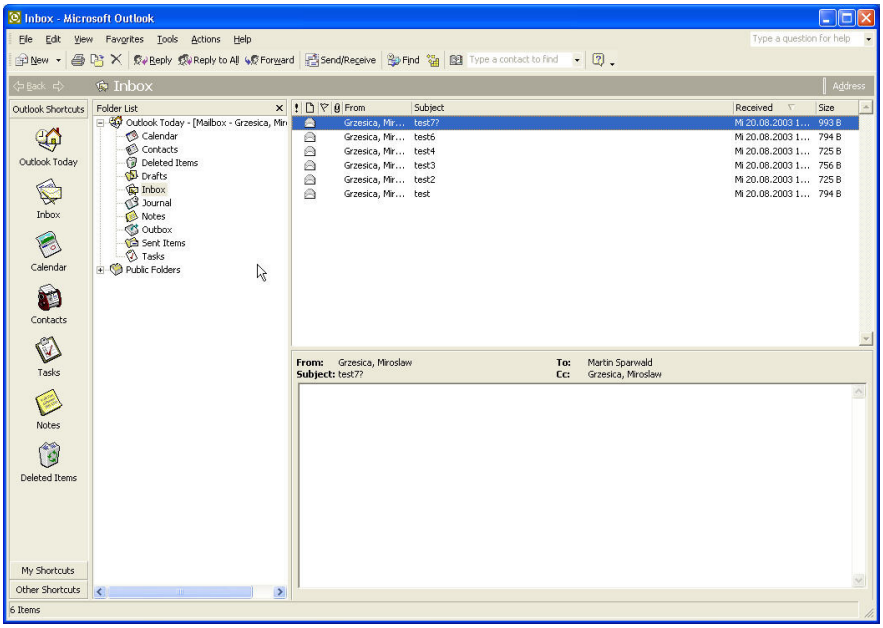
An internet connection must be established and the VPN Client has to be started. If these requirements are fulfilled you can use all applications.

5.1 Connect to MS Exchange mail server / Outlook

Please refer to chapter 2.4 – Name Resolution for important information how to allow Outlook to resolve the Exchange server name.

Due to time-outs and other problems depending on the VPN tunnel, sometimes you have to repeat the connection procedure. The dialog boxes (displayed below) will appear. Click **Retry** till you get a connection to the Exchange Server.

After connecting successfully to the Exchange Server, you can use MS Outlook like you are connected to your local LAN



5.2 Connect to file server

Please refer to chapter 2.4 – Name Resolution for important information how to resolve the file server name.

Once a VPN connection is established, you have to map a shared network folder on the file server in the LAN.

The user connecting to the shared network folder must have the permissions (in the local LAN) to connect to this folder.

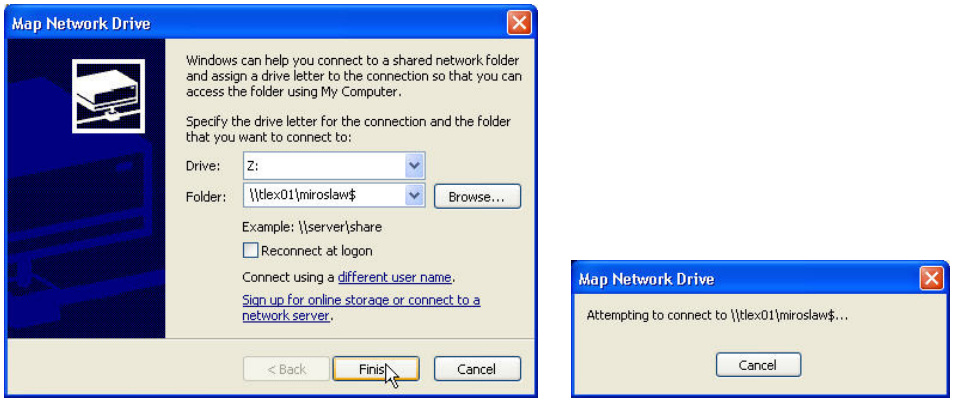


Figure 1 – Mapping Network Drive for VPN Access

After the connection to the file server via VPN is established, the user is able to transfer files between the file server and the local machine like he is connected to the local LAN.

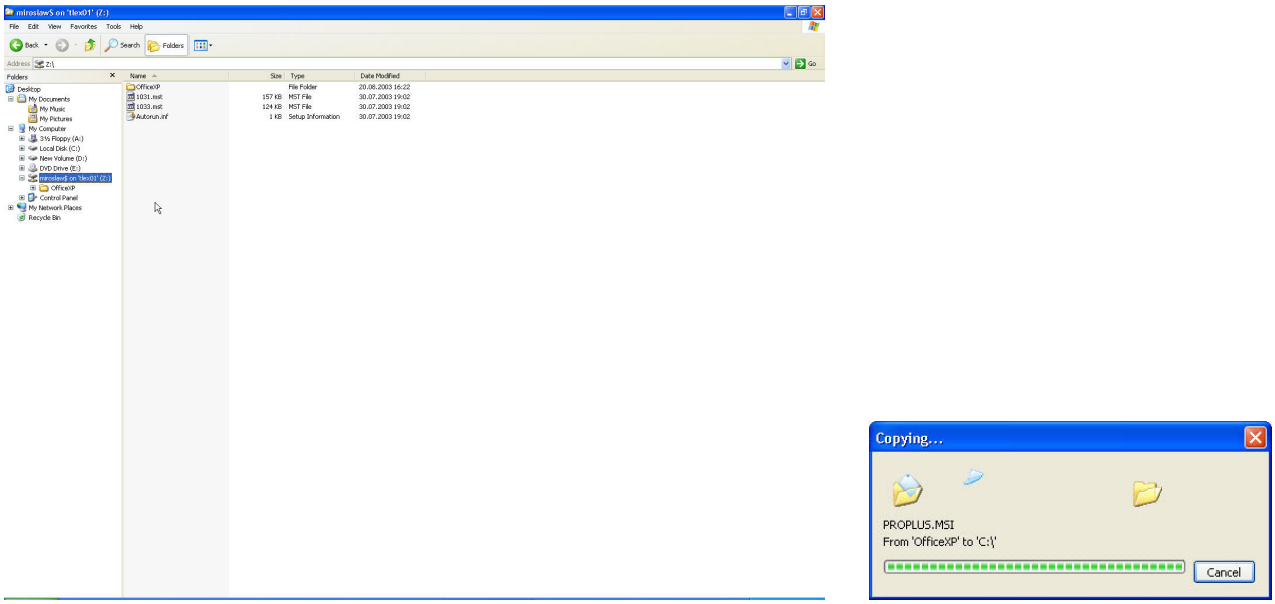


Figure 2 – File Transfer between LAN and local drives

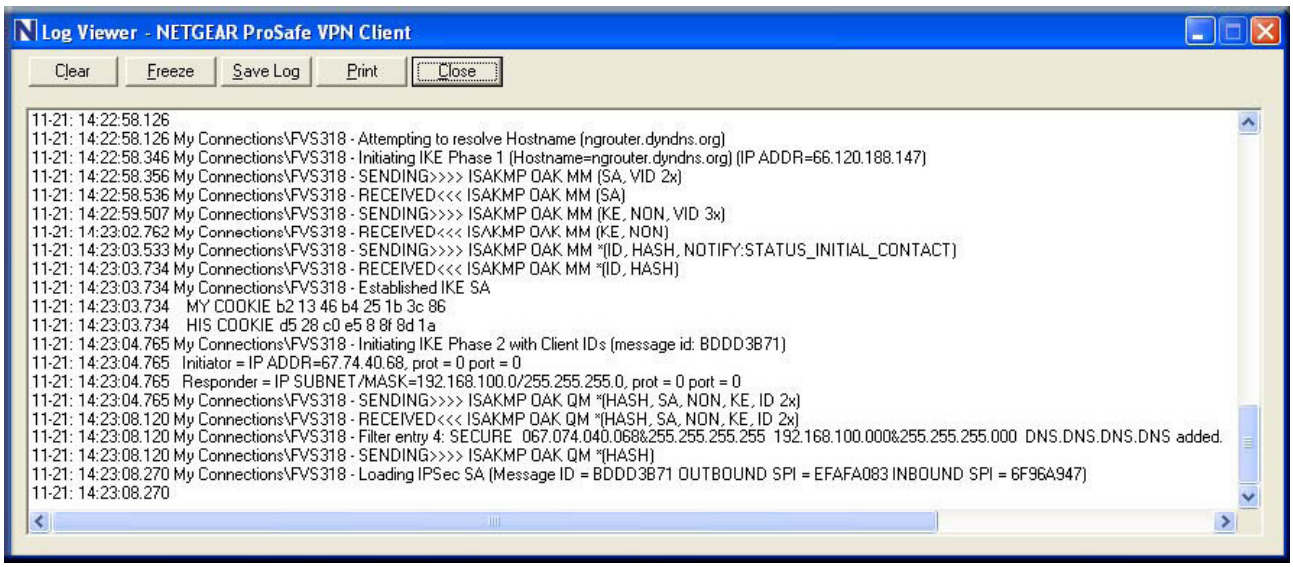
6 Logging

For more information please refer to the Netgear ProSafe VPN Client's documentation.

6.1 Logging Client (client side)

After the client installation, a log viewer can be found in the Windows start menu:

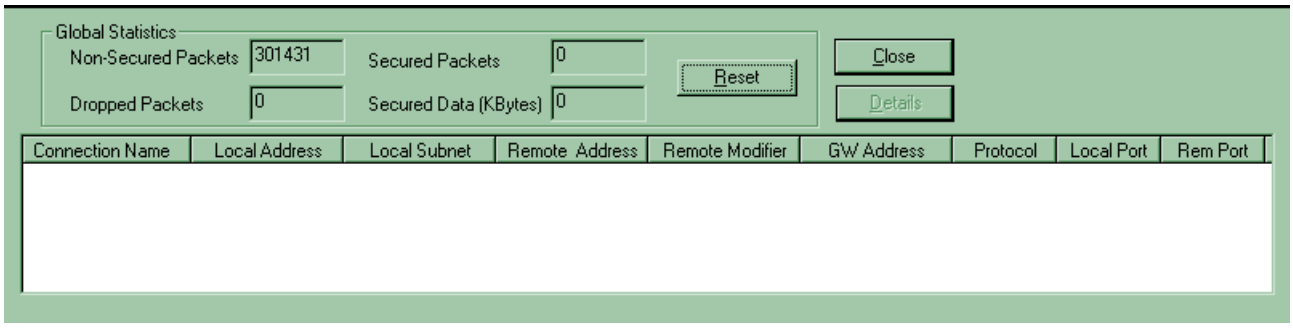
e.g.: "Programs > VPN > Log Viewer". The log can be cleared, printed and saved to a file. The log display can be stopped and restarted.



6.2 Connection Monitor (client side)

The Connection Monitor shows statistical and diagnostic information for each active connection.

The Connection Monitor is viewed by selecting the client icon from the Windows Notification Area (system tray), right-click and select **Connection Monitor**.



**** End of Document ****