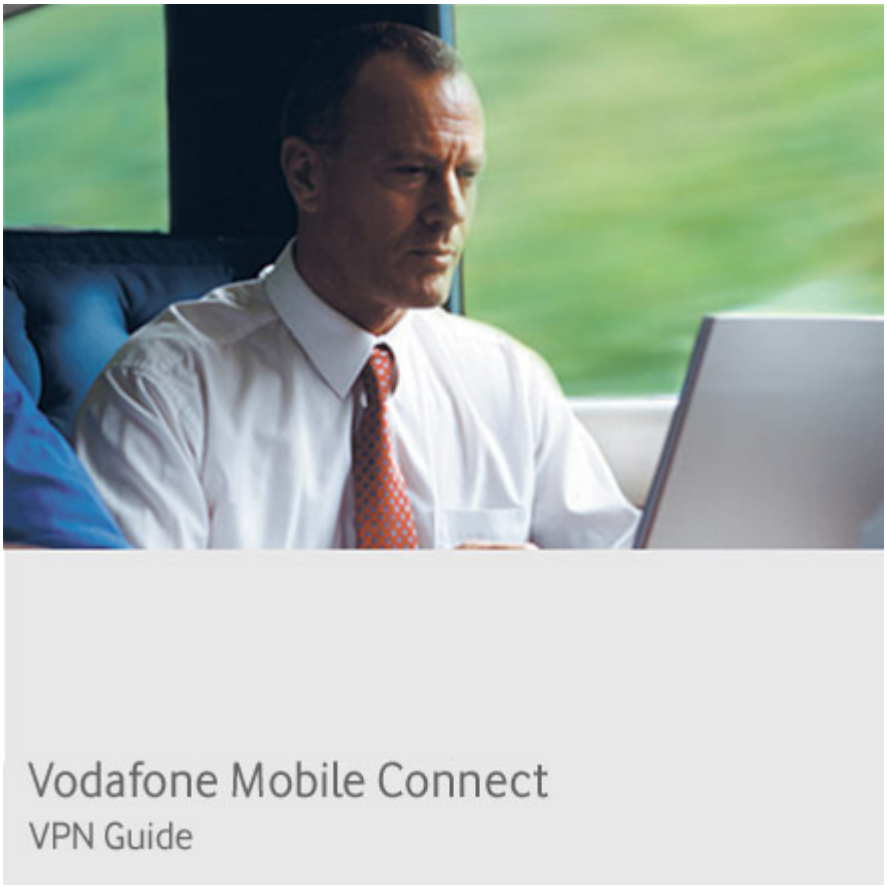
VPN End to End – Juniper NetScreen

Appendix B: Juniper NetScreen Remote Client

Technical Notes for use with Vodafone Mobile Connect services

Date: **31 May 2007**

Revision No: **3.0**



© 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	May 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	Editorial changes, R9 references

File Reference

VPN - Cisco PIX501_Appendix_B_Client.doc

Document Authors

Joerg Pfeffer, 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.

Contents

1 Executive summary 4

2 VPN Client Installation and Configuration (NetScreen-Remote Client 10.3.5) 5

2.1 VPN Client System requirements 5

2.2 VPN Client installation 6

2.3 Configuring a new Client connection (Juniper NetScreen-Remote Client 10.3.5) 8

3 Configuration & Connection Using VMC Software 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

3.4 Establishing a mobile VPN connection 16

4 Configuring & Using the VPN Client 18

4.1 Automatic Start-up 18

4.2 Keepalive Frequency 19

4.3 Event Logging 19

4.4 Connection Status 20

4.5 Import a Profile configuration File into NetScreen-Remote Client 10.3.5 20

5 Connections to Different Services 22

5.1 Connect to MS Exchange mail server / Outlook 22

5.2 Connect to file server 23

Tables & Figures

Nil

1 Executive summary

This Appendix B is in addition to the detailed document for Juniper NetScreen-Remote 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 - Juniper_Netscreen_5GT_Appendix_A_Concentrator.doc'.

- 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 manually. Options for automatic start-up are presented.
- Integration of the VPN Client with Vodafone Mobile Connect software is illustrated along with frequently used configuration settings
- Connections to corporate applications and file servers are illustrated
- Monitoring and logging of connection status is illustrated.

Further information is available from the vendor documentation and website www.juniper.net..

© VODAFONE GROUP 2007

2 VPN Client Installation and Configuration (NetScreen-Remote Client 10.3.5)

The NetScreen-Remote Client can be installed on a Windows Workstation. To install the Software a user needs Administrator rights on the local machine. This client can be used to establish a VPN connection to the Juniper NetScreen firewall/VPN appliance. Other VPN Clients have to be de-installed.

The NetScreen-Remote 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:

- A single, Pentium®-class processor or its equivalent.
- One of the following operating systems:
  - 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
- Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.)
- 5 to 35 MB hard disk space.
- RAM:
  - 16 MB for Windows 95
  - 32 MB for Windows 98 or NT or Windows ME
  - 64 MB for Windows 2000 or Windows XP
- 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 modem
  - PPPoE drivers if DSL is used

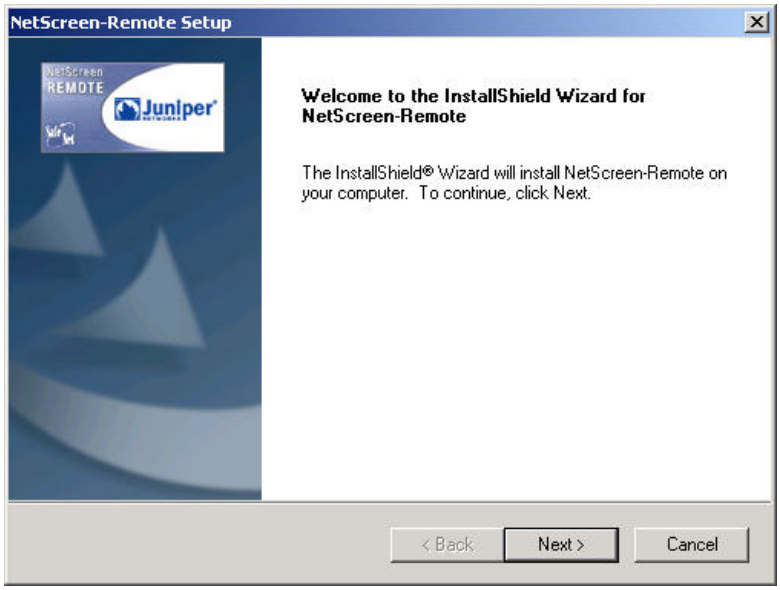
© VODAFONE GROUP 2007

- To connect using a digital certificate for authentication:
  - A digital certificate signed by a Certificate Authority (CA) installed on your PC

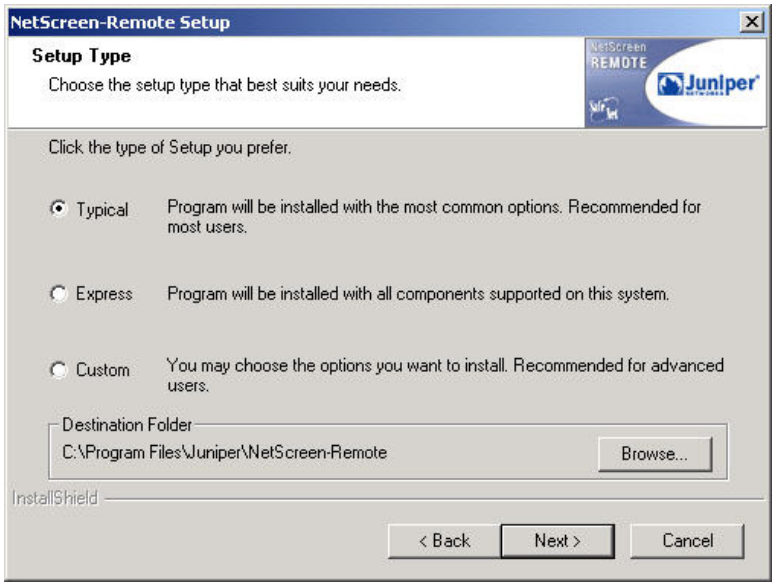
2.2 VPN Client installation

- Run the installation program according to the directions given by the program. Following slides shows the NetScreen-Remote Client 10.3.5 Installation :

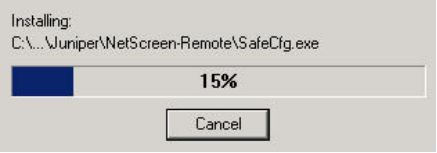
- At the “Setup” window click “Next”



- Follow the screens for “License Agreement” and “Setup Type and Destination and Program Folders” and install the NetScreen-Remote Client.

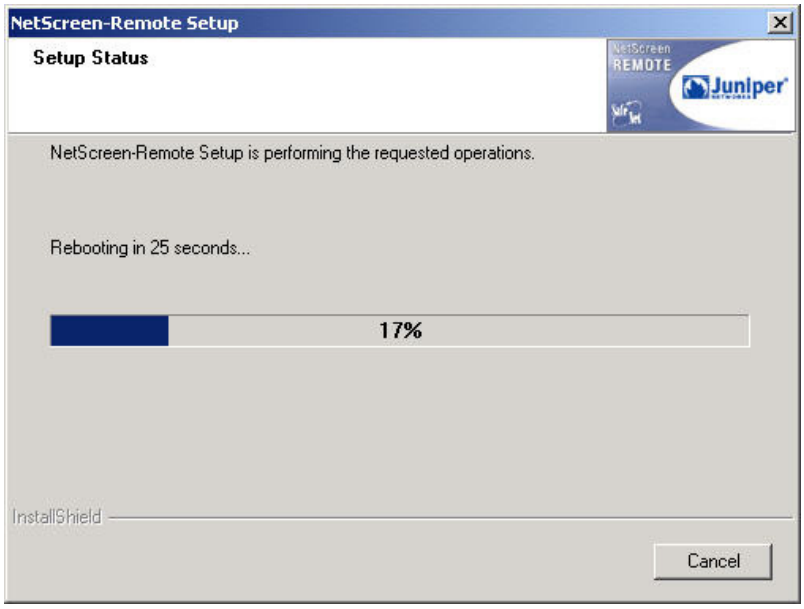


- Setup status

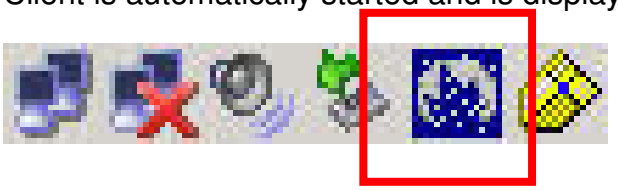


- A Deterministic Network Enhancer will be installed on all available network adapters. Additionally NetScreen-Remote Client 10.3.5 creates a new network adapter.

- After completing the installation, the system automatically reboots within 30 seconds unless the reboot is cancelled.



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

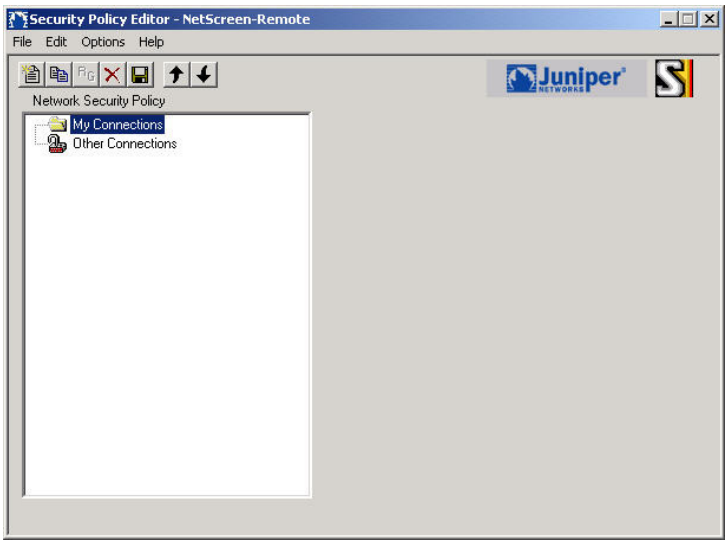


2.3 Configuring a new Client connection (Juniper NetScreen-Remote Client 10.3.5)

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 and acquire the IP address, network mask, DNS and WINS servers via the XAUTH protocol from the gateway. The advantage of this setup is, that within the corporate network, a well defined address range can be assigned to remote users, so that routing and firewalling is possible.

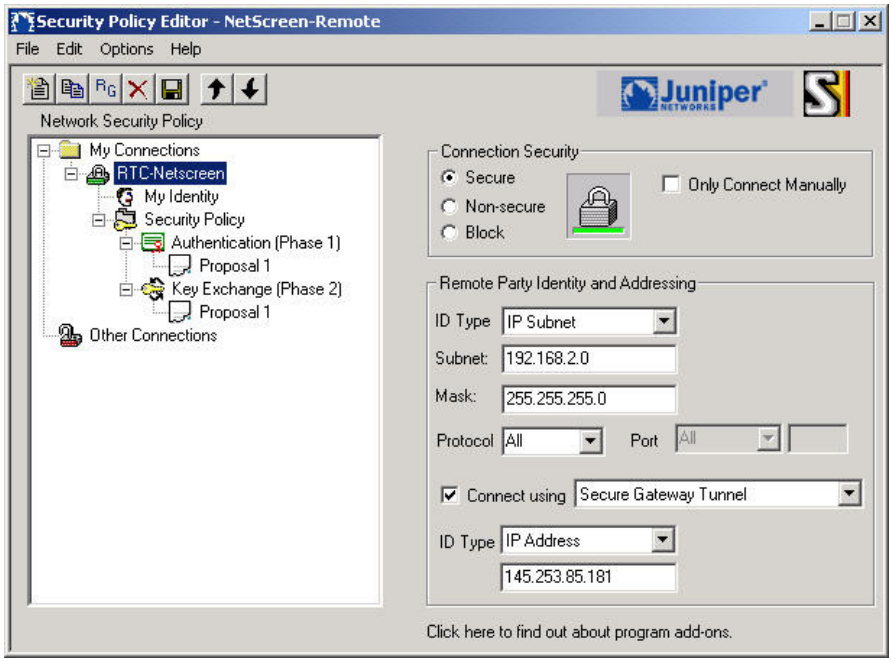
The setup here is matched to the configuration of the NetScreen appliance described in the document in appendix A.

Start the Profile Editor from the Program menu at “Programs > NetScreen-Remote > Security Policy Editor”



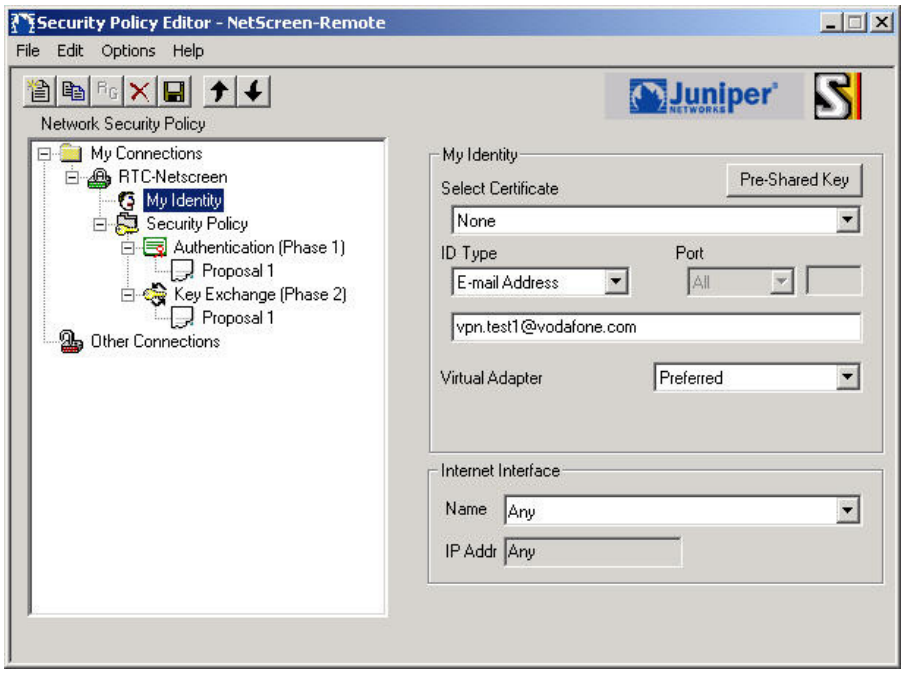
- Click on the “Add a new connection” icon on the left to define a new profile

- 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 IP Address. Enter the external IP address of the Juniper NetScreen appliance you want to connect to.

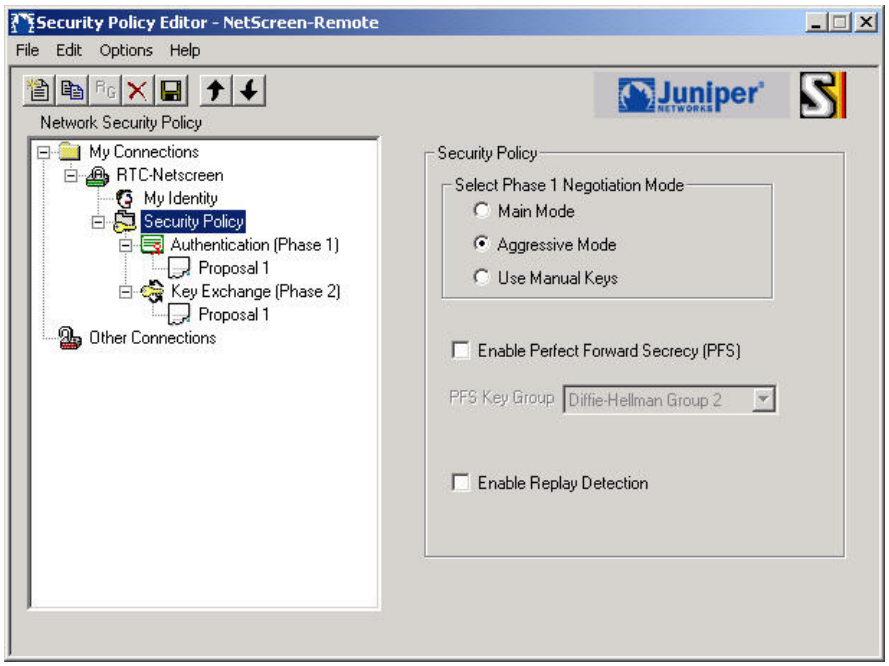


© VODAFONE GROUP 2007

- 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 the email address of one of the users configured on the NetScreen appliance is entered. It does not matter which, e.g. define a dummy user for this purpose on the NetScreen appliance. Click on “Pre-Shared-Key” to enter the same key as in the gateway configuration of the NetScreen appliance. **This is not the password of the user but the separately entered shared secret.** User and password of the real user will be requested by the client when connecting to the gateway. Set the “Virtual Adapter” setting to “Preferred” or “Required”.

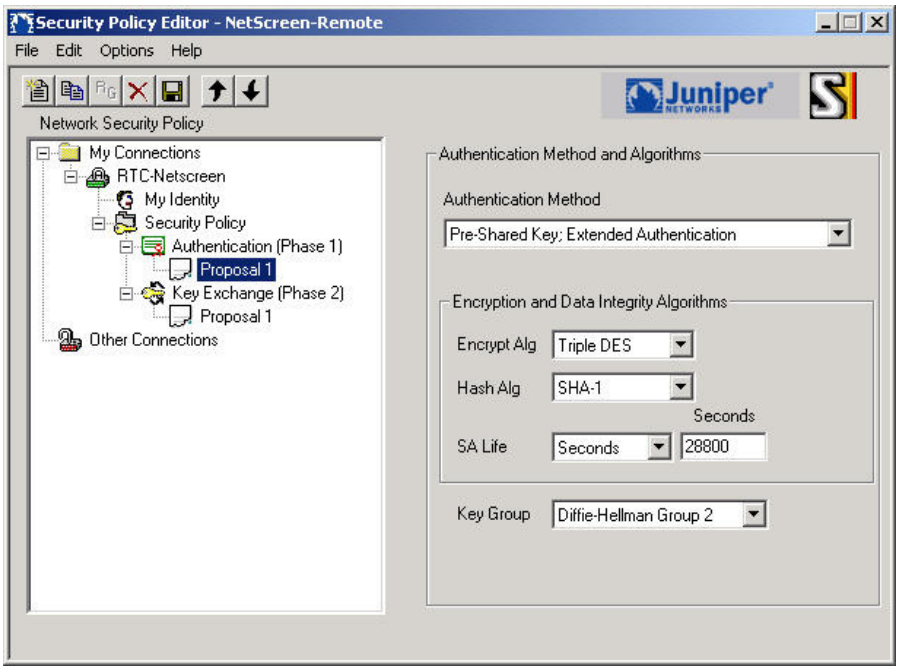


- Next, click on “Security Policy” entry in the connections tree to edit the Security Policy. Select “Aggressive Mode” for Phase 1 Negotiation. This is required for authentication with shared secret on a NetScreen device. Here, PFS and Replay Detection are not enabled to simplify the example.

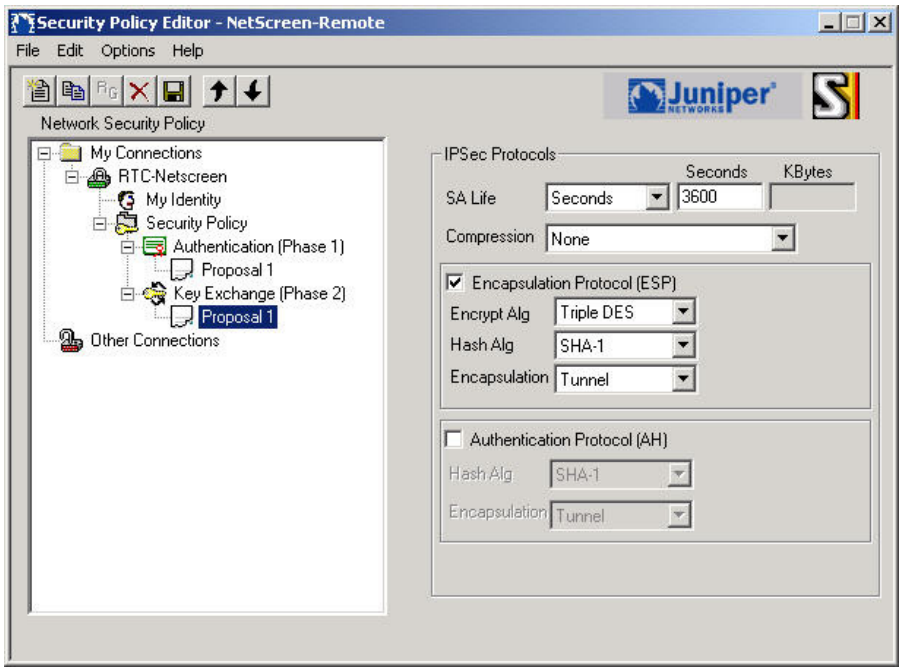


© VODAFONE GROUP 2007

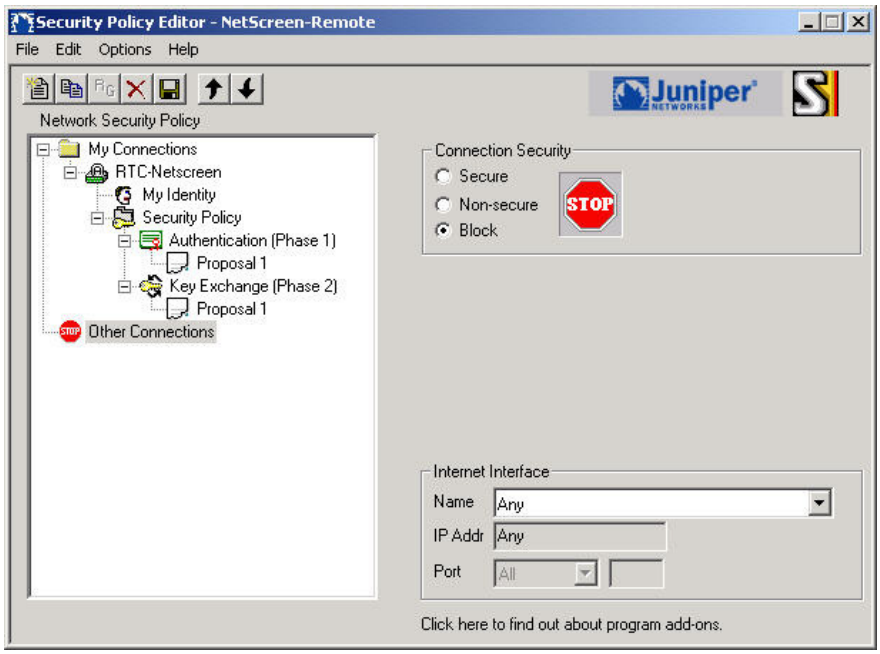
- Next, click on “Proposal 1” entry below “Key Exchange (Phase 1)” in the connections tree to edit the first IPSec Phase 1 (IKE) Encryption setup. More than one proposal is possible and a fitting one will be negotiated during connection establishment, but since both sides are known, the first proposal should fit the requirements. As “Authentication Method”, select “Pre-Shared Key; Extended Authentication” to allow XAUTH setup via the NetScreen device. **Make sure the encryption parameters (Encrypt Alg, Hash Alg, SA Life, Key Group) exactly match the settings on the NetScreen 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 can be enabled at this point, but the setup must match the setup on the NetScreen appliance. Set the Encapsulation to “Tunnel”. Make sure the encryption parameters (Encrypt Alg, Hash Alg, SA Life) exactly match the settings on the NetScreen 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.



3 Configuration & Connection Using VMC Software

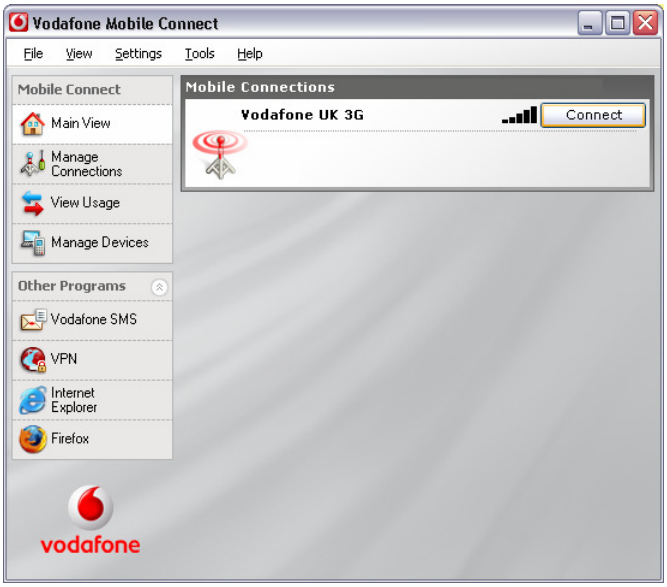
The Netscreen VPN client is installed as a system utility and runs transparently whenever the computer is started. The client is accessed via the icon in the Windows Notification Area (System Tray). As the client is always running, there is no need (and it is not possible) to configure the VPN button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

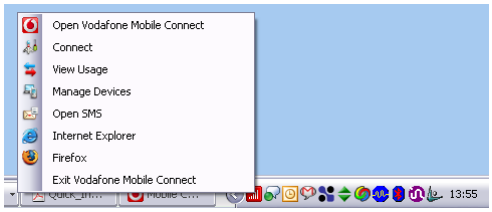
With a SIM card inserted into your datacard (or USB modem), to establish a connection:

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



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

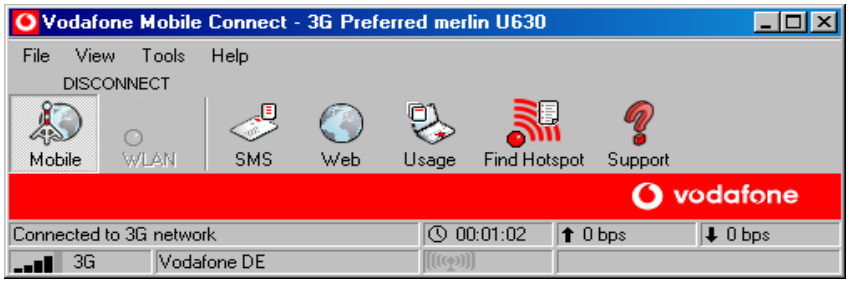
3. From the Windows Notification Area (system tray), right-click and select **Connect**.



© VODAFONE GROUP 2007

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.

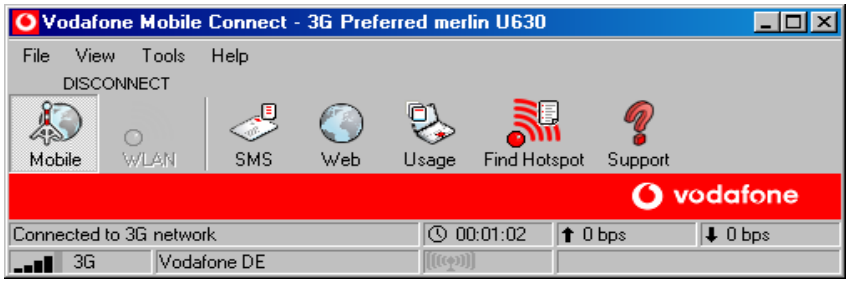


- First you need to build up a connection using your VMC. Insert SIM and PCMCIA card and open the Vodafone Mobile Connect application.
- Press the **Mobile** button in the CONNECT/DISCONNECT area of the toolbar

3.3 Establish the VPN

Start the application that needs to access the corporate data (email client such as Microsoft Outlook or web browser accessing corporate intranet location); the VPN client will start automatically.

3.4 Establishing a mobile VPN connection

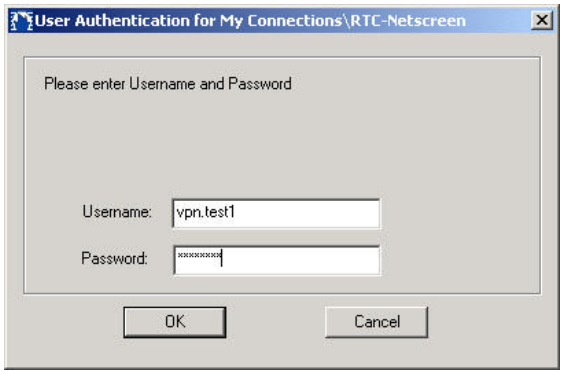


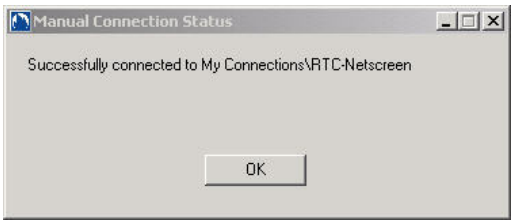
- Click the “Mobile” button on the main Dashboard screen.
  After you build up your preferred connection, the NetScreen-Remote Client is able to connect to the remote gateway automatically. Make sure that the NetScreen-Remote is running in the system tray.

© VODAFONE GROUP 2007

- 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>”.

- When the Phase 1 key exchange is executed by the client, the XAUTH setup will ensure that the user name and password is requested. On entering a correct username and password, the key exchange will be completed.

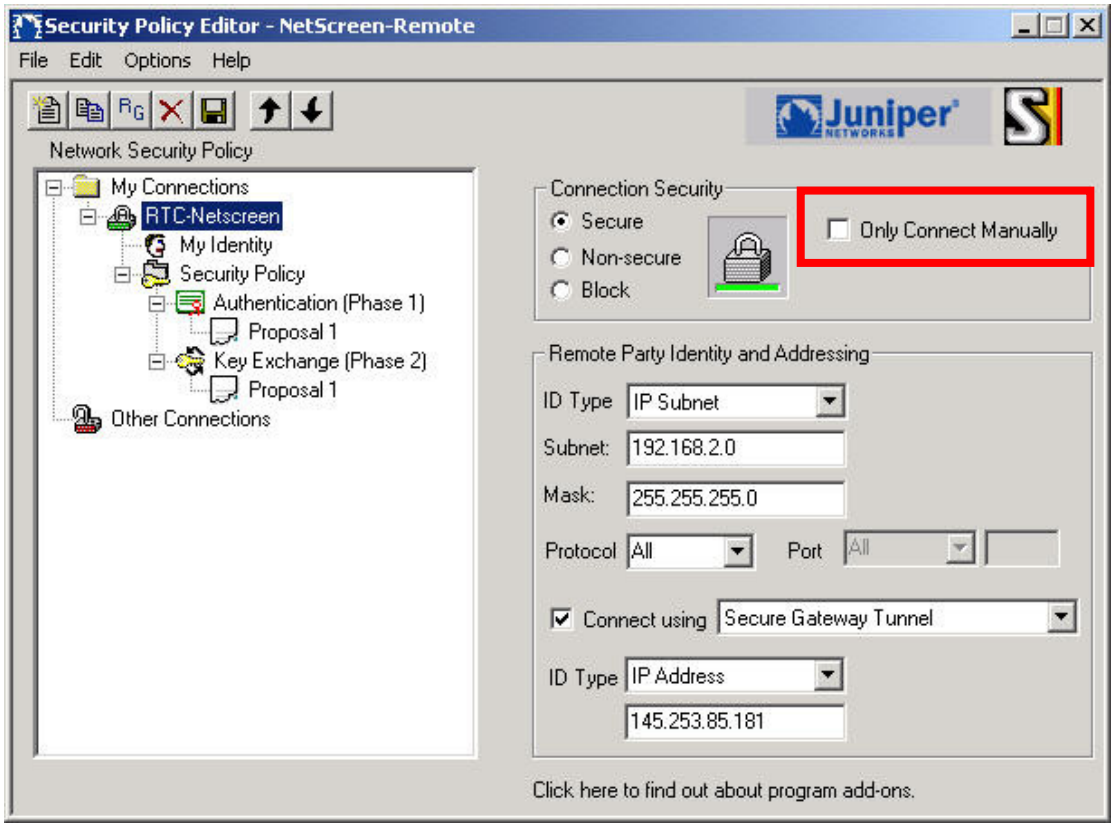




4 Configuring & Using the VPN Client

4.1 Automatic Start-up

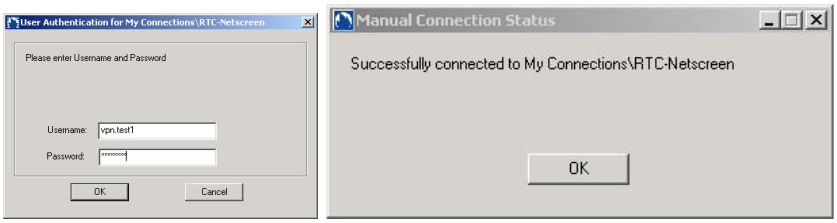
By default, NetScreen-Remote Client will be started from the “Programs > Startup” on Windows-startup. Further, the client will connect automatically when an application tries to connect to it’s server in the corporate network. This behaviour can be changed in the Policy Editor if editing of the policy 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>”.

- When the Phase 1 key exchange is executed by the client, the XAUTH setup will ensure that the user name and password is requested. On entering a correct username and password, the key exchange will be completed.

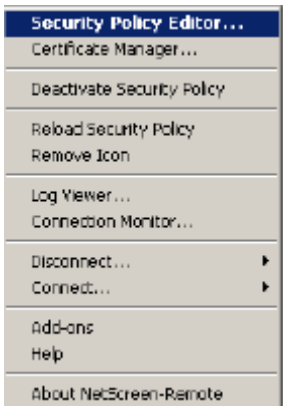


4.2 Keepalive Frequency

When NAT-Traversal is activated, as is necessary with most countries GPRS and 3G services, the Keepalive packet frequency defaults to 5 seconds. This will cause a comparatively high administrative traffic volume. Setting the Keepalive packet frequency to 15 to 30 seconds is fully sufficient.

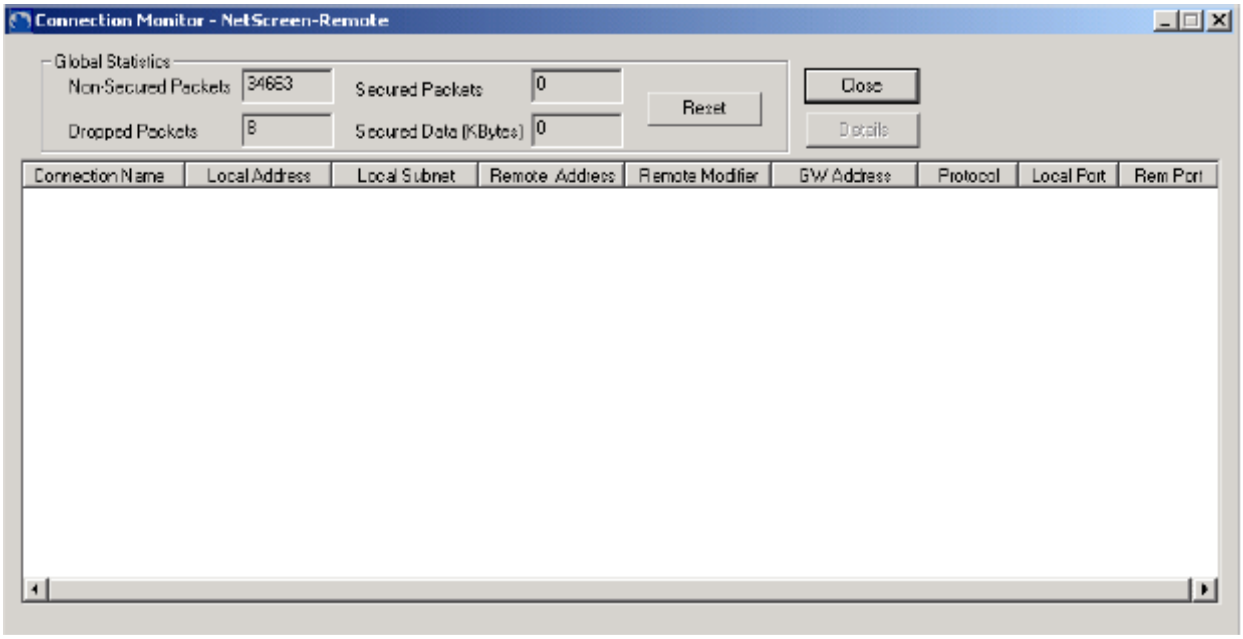
4.3 Event Logging

The NetScreen client maintains a log in the program directory – it can be viewed by selecting the 'Log Viewer' option when activating the client from the system tray:



4.4 Connection Status

Basic information about the VPN connection is shown by selecting the 'Connection Monitor' when activating the client from the system tray:

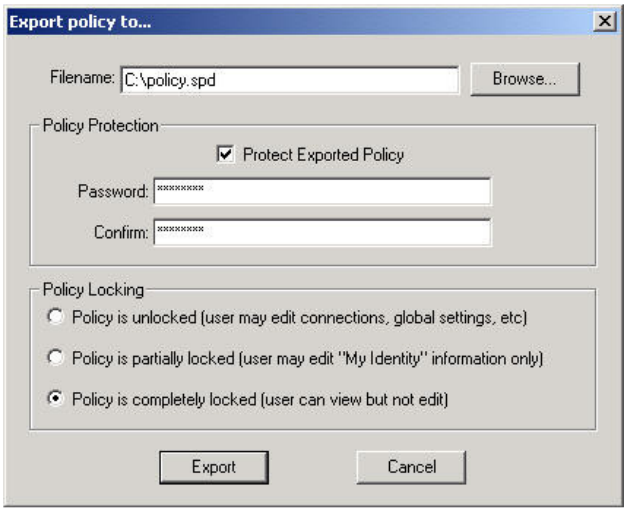


4.5 Import a Profile configuration File into NetScreen-Remote Client 10.3.5

Working profiles can be exported from the NetScreen-Remote 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 NetScreen-Remote Policy Editor from menu "Programs > NetScreen-Remote > 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”.

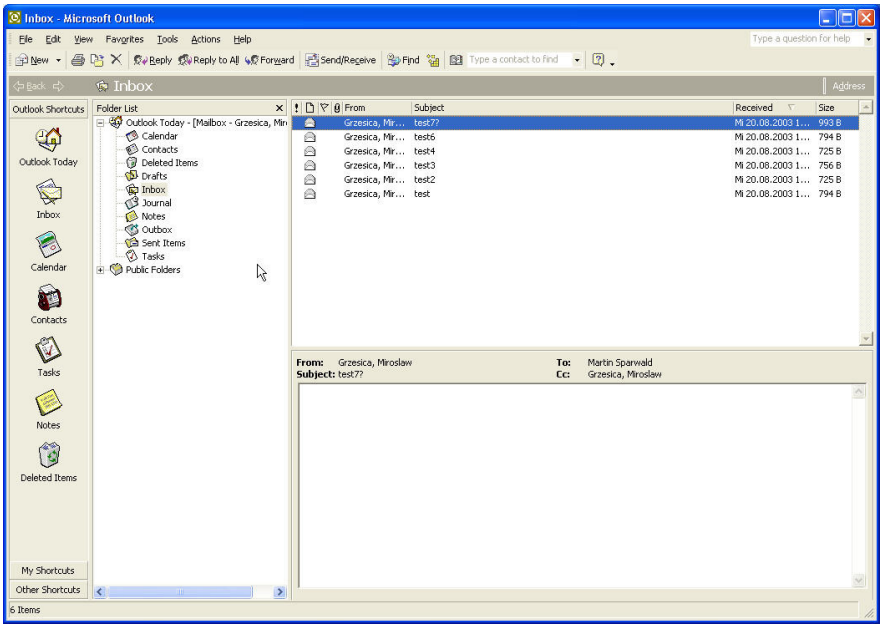
5 Connections to Different Services

You can connect to all services via the VPN tunnel; you can connect to if you are in your local LAN as long as an internet connection is established and the VPN Client has been started. If these requirements are fulfilled you can use all applications.

5.1 Connect to MS Exchange mail server / Outlook

Caused on 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.

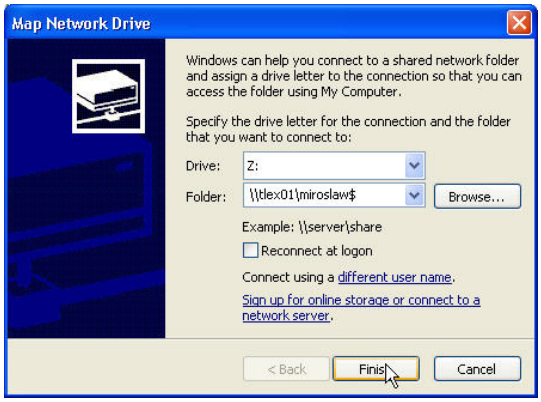
After connecting successfully to the Exchange Server, you can use MS Outlook like you are connected to your local LAN

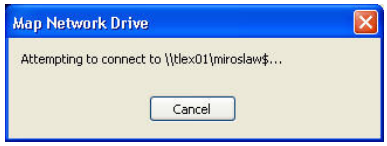


5.2 Connect to file server

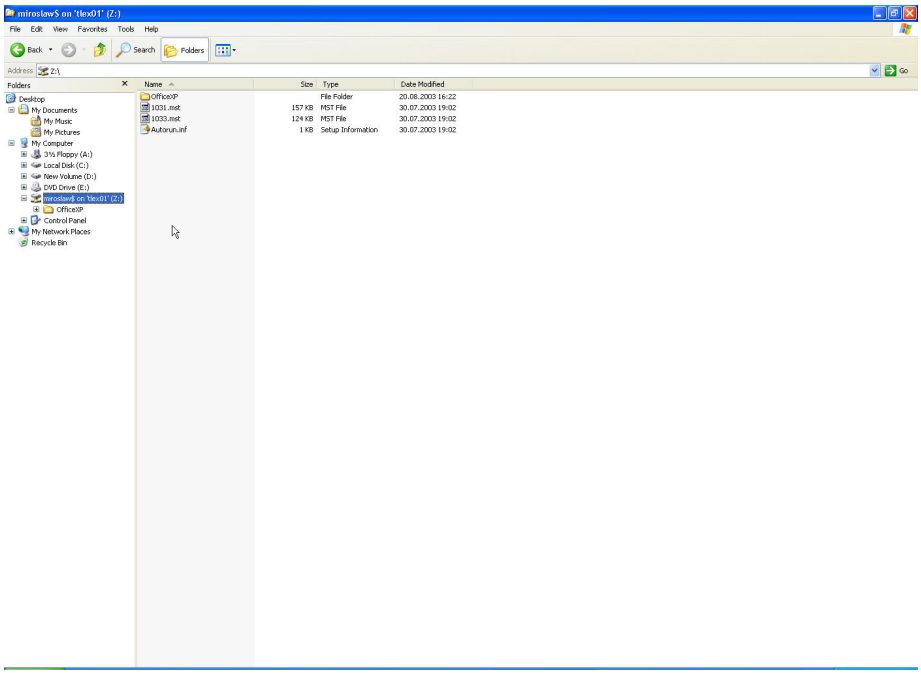
If a VPN connection is established, you have to map a shared network folder on the file server in the LAN.

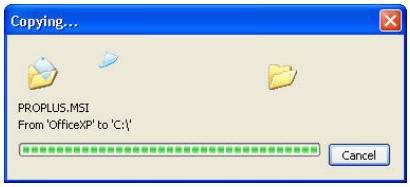
The user connecting to the shared network folder must have the permissions (in the local LAN) to connect to this folder.





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.





**** End of Document ****