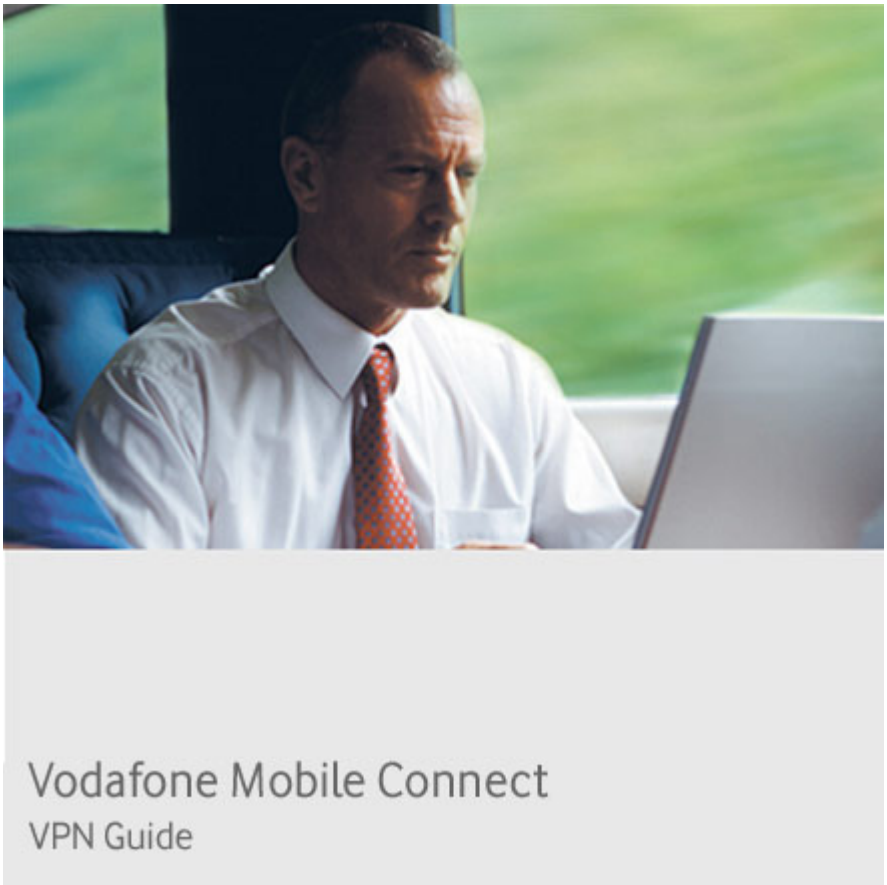
VPN End to End – Appendix A: MS Windows 2003 L2TP/IPSec

Appendix A: MS Windows 2003 L2TP/IPSec

Technical Notes for use with Vodafone Mobile Connect services

Date: **14 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	Minor edits and R9 updates.

File Reference

VPN - MS_2003_L2TP_IPSec_Appendix_A_Concentrator.doc

Document Authors

Joerg Pfeffer, TECON Terenci
Peter Jaeger, TECON Terenci
Miroslaw Grzesica, 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 Gateway Installation and Configuration 5

2.1 Initial setup 5

2.2 Routing and Remote Access configuration 6

2.3 Configure Server to use preshared key authentication 12

2.4 Advanced settings 18

2.5 Keep alive messages 19

2.6 Data compression 20

3 Configuration of Split Tunnelling 21

4 User Management and Profile Handling 23

5 Logging 26

6 Name Resolution 28

Tables & Figures

Nil

© VODAFONE GROUP 2007

1 Executive summary

This Appendix is in addition to the detailed document for Microsoft Windows 2003 L2TP/IPSec VPN Server and describes the setup and update process in a detailed way with example screen shots taken from the initial processes.

Furthermore logging and additional functionality is available in the appropriate chapters.

© VODAFONE GROUP 2007

2 VPN Gateway Installation and Configuration

The following description is intended for network administrators who are familiar with networking and IP concepts. The Server has to be integrated into the internal company network. The Server setup therefore has to comply with the configuration of the internal networking. This description is intended to allow a network administrator not yet familiar with the Windows L2TP/IPSec VPN to configure a VPN with UMTS/GPRS usage.

2.1 Initial setup

The Microsoft Windows VPN solution is based on the standard Windows 2003 installation. After basic installation of Microsoft Windows 2003 Server install also the latest service pack as well as the latest updates and patches using the Microsoft download web page (http://windowsupdate.microsoft.com). You can install the Server on any machine which meets the minimum system requirements for this operating system. For detailed information please refer to the following web page: http://www.microsoft.com/windowsserver2003/evaluation/sysreqs/default.mspx.

Be sure the IP-addresses are configured correctly on the server for the public and private interface. The default gateway should be entered only for the public interface.

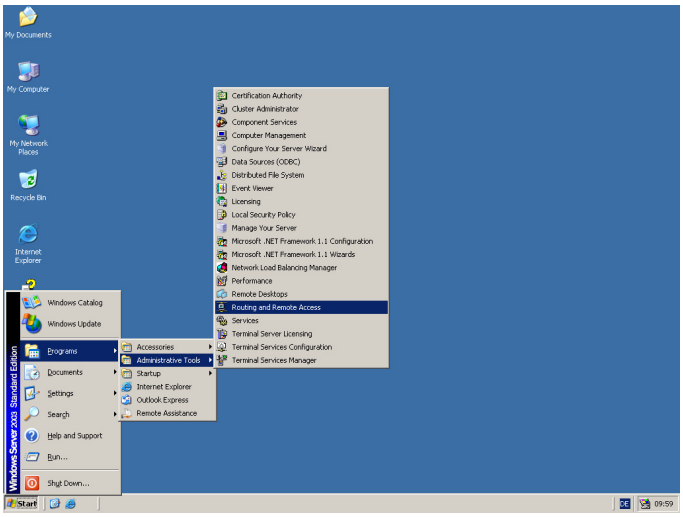
Note: You can either place the Server besides or behind your Firewall. We recommend placing it behind the Firewall and opening the appropriate ports for VPN connection to the Server. See the chapter “Which protocols are supported” above for port description.

Now there is a need to configure the server to act as a VPN concentrator. In order to achieve this Routing and Remote Access must be configured. Afterwards an IPSec policy has to be created and depending on the authentication method a certificate must be implemented or the server must be prepared for using “Pre shared Key” authentication. For the tests we use “Pre shared Key” authentication.

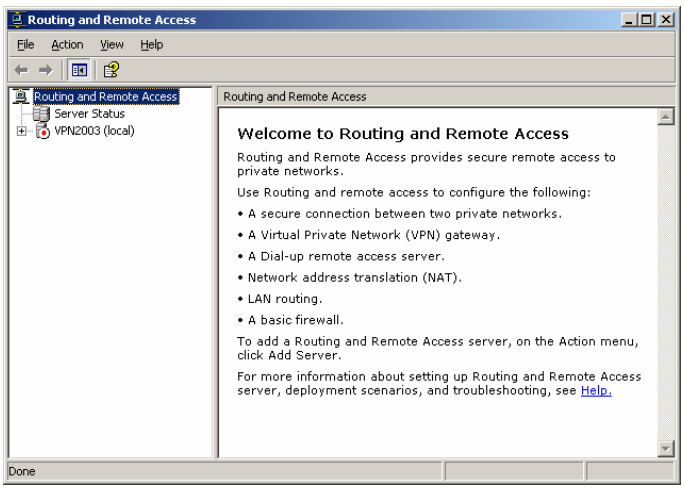
© VODAFONE GROUP 2007

2.2 Routing and Remote Access configuration

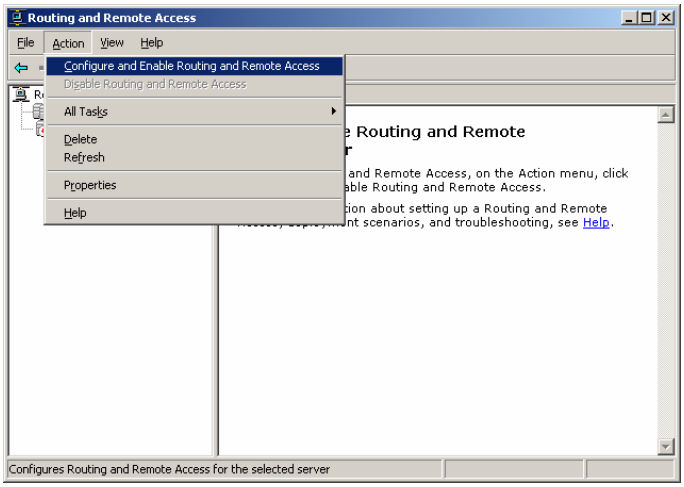
- Open “Routing and Remote Access” from the Administrative Tools.



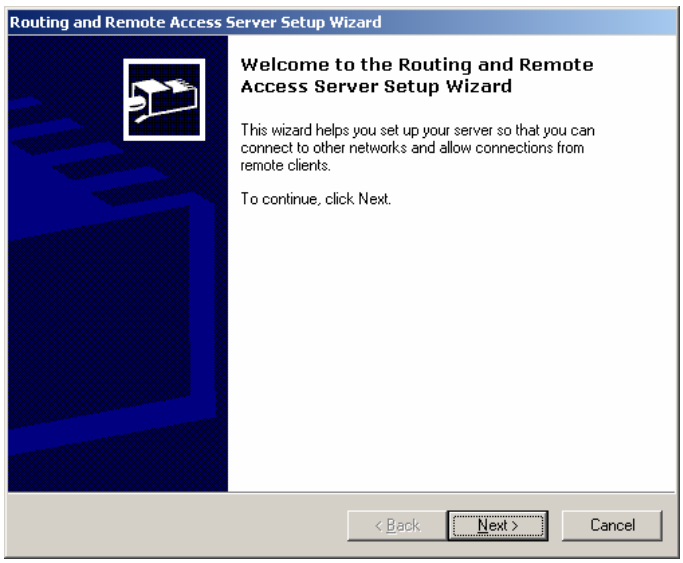
- The following screen shows that “Routing and Remote Access” is by default installed but not configured on a Microsoft Windows 2003 Server.



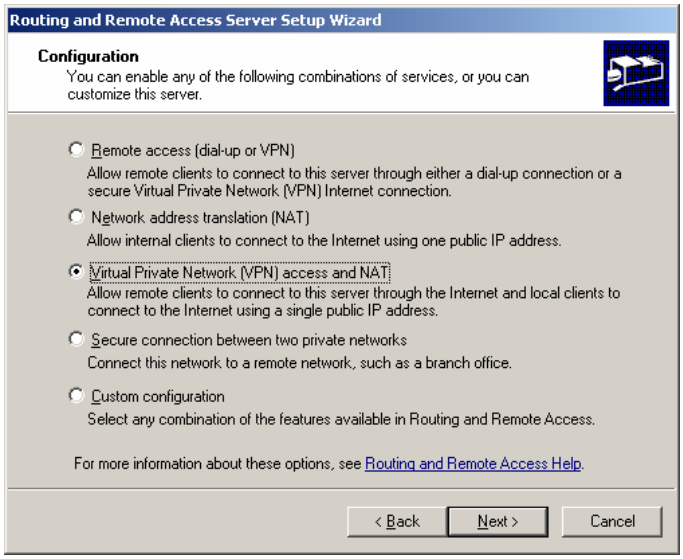
- From the “Action” menu entry select “Configure and Enable Routing and Remote Access”



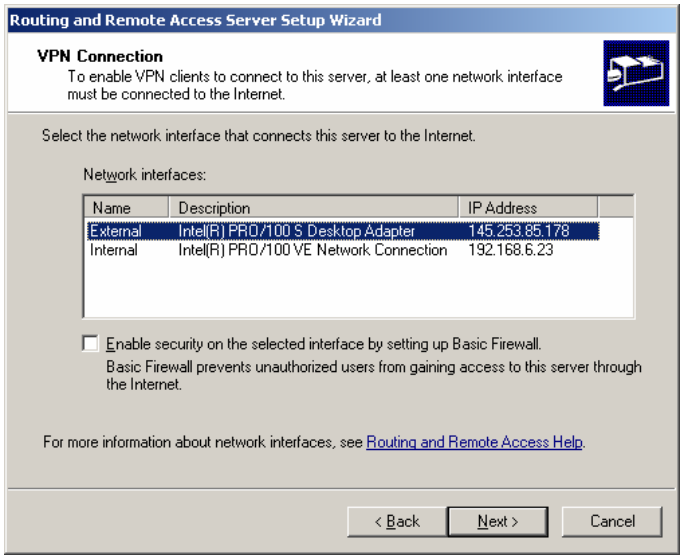
- On the “Welcome” window click on “Next”.



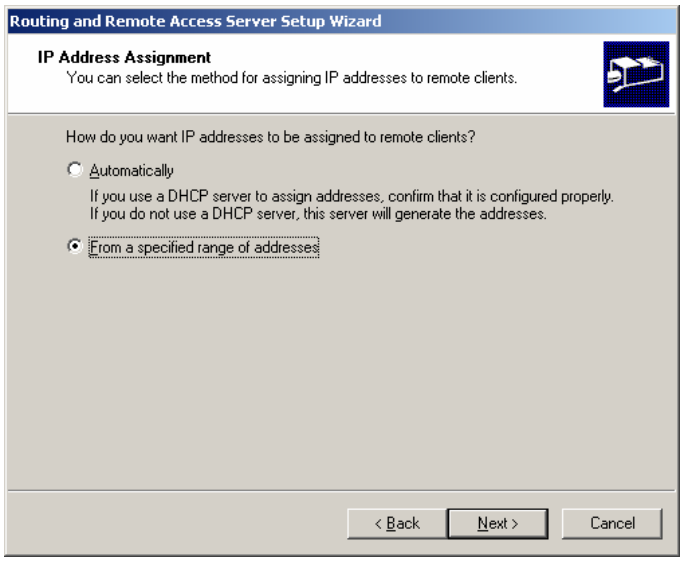
- On the next window select “Virtual Private network (VPN)” as the service to be enabled with Routing and Remote Access.



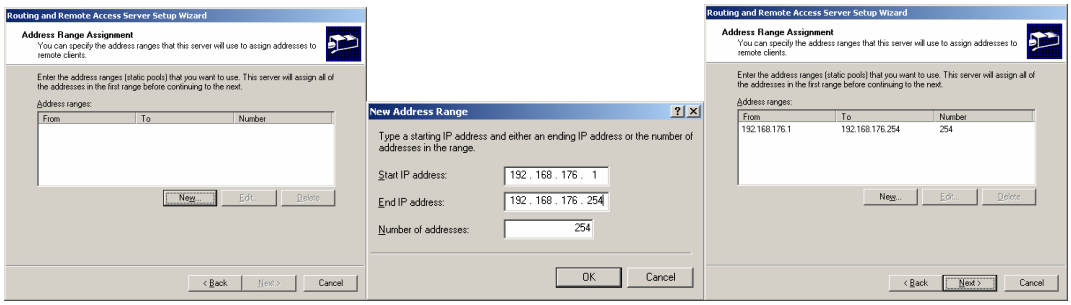
- On the “VPN Connection” window verify the interface settings. In case the VPN server is behind the corporate firewall, which is the recommended scenario, there is no need to enable a Basic Firewall on the VPN server.



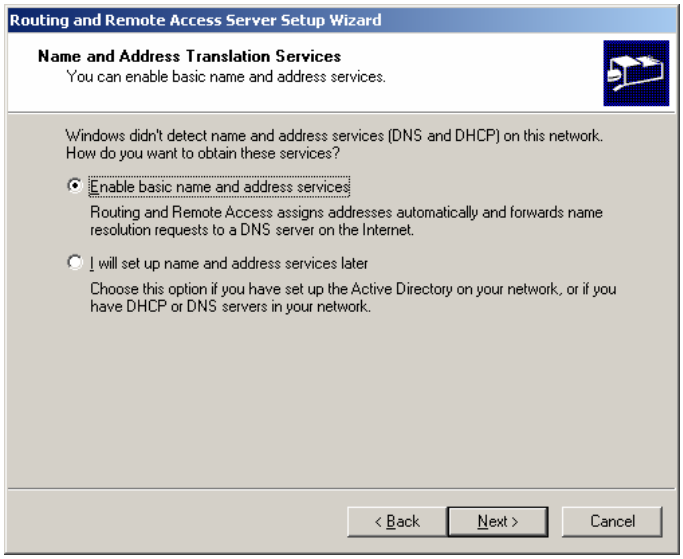
- After selecting “Next” you can configure either the clients will receive an IP-address automatically from a DHCP server in the internal LAN or from a specified range of addresses configured within the Routing and Remote Access service.



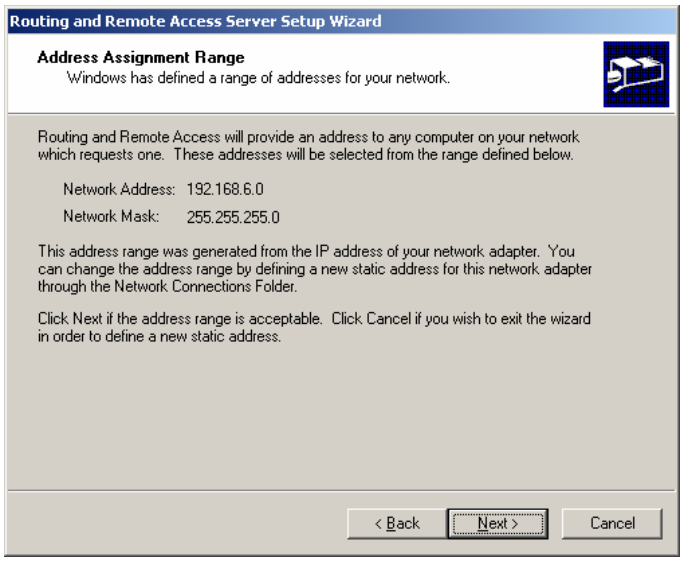
- In case a specified range of addresses was selected, this range must be defined on the following window.



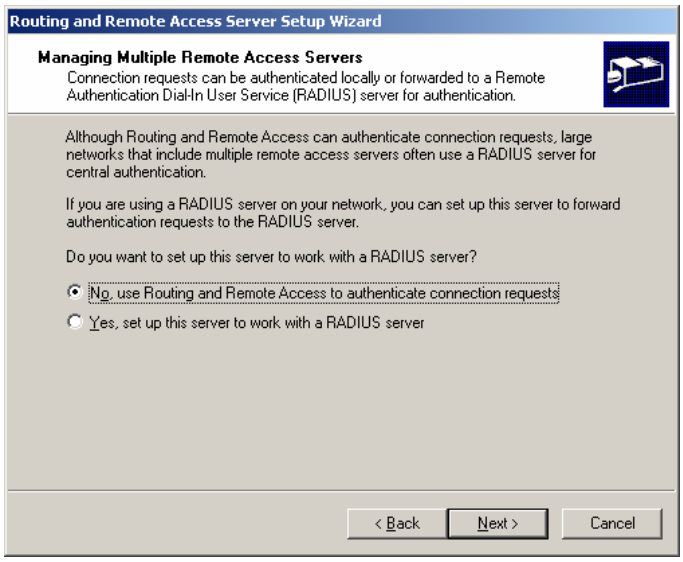
- Since the role of the server is to act as a VPN concentrator DHCP and DNS do not need to be configured. In this case basic name and address services should be selected.



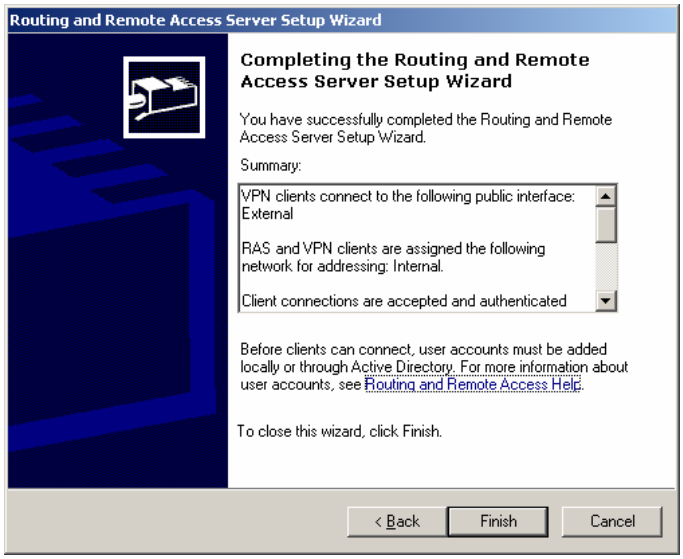
- On the next screen verify the address assignment range based on the IP address from the private interface and click on “Next”.



- On the following screen you can choose how to authenticate users. You can select the VPN Server internal users or using a RADIUS server. We used the default setting " Use Routing and Remote Access to authenticate connection requests"



- The last window of the "Routing and Remote Access" configuration shows a summary of the settings. Click on "Finish".



- After done, verify that the service is started automatically (green point on the server icon is visible). Otherwise it is also possible to start "Routing and Remote Access" manually. Use right-click on the server entry and select "All Tasks" -> "Start". Now you've finished the base configuration.

2.3 Configure Server to use preshared key authentication

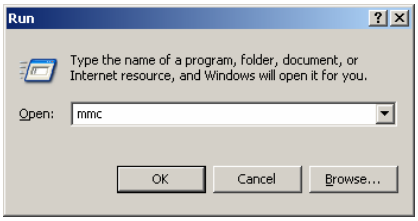
To implement the preshared Key authentication method for use with a L2TP/IPSec connection you must add the ProhibitIpSec registry value to the Server and configure an IPSec policy before a L2TP/IPSec connection can be established. This must be done on both endpoints, Server and Client.

To add the ProhibitIpSec registry value to the server follow these steps:

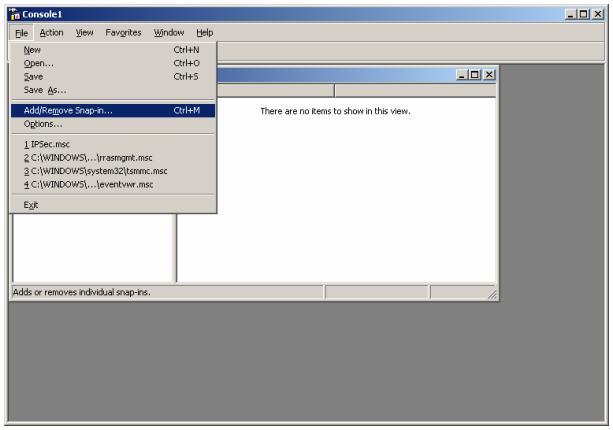
- Click Start, click Run, type regedt32, and then click OK.
- Locate, and then click the following registry sub key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
- On the Edit menu, click Add Value.
- In the Value Name box, type ProhibitIpSec.
- In the Data Type list, click REG_DWORD, and then click OK.
- In the Data box, type 1, and then click OK.
- Quit Registry Editor, and then restart your computer.

To create an IPSec policy, follow these steps:

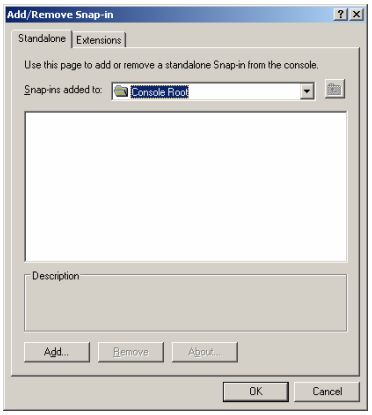
- Click Start, click Run, type mmc, and then click OK.

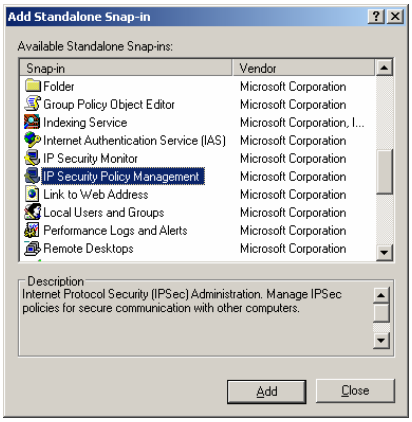


- In the Console window click Add/Remove Snap-in

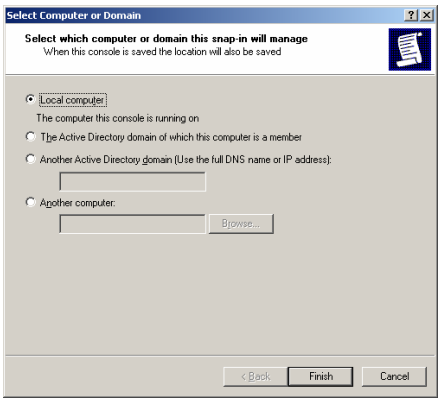


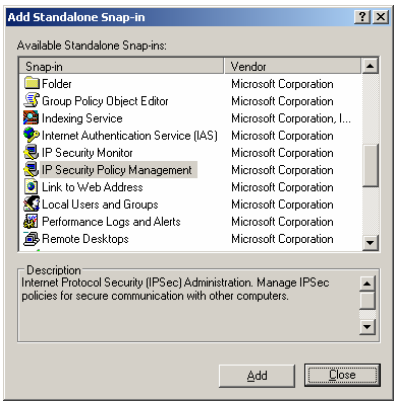
- In the “Add/Remove Snap-in” window click on the “Add…” button, select “IP Security Policy Management” and click on “Add…”



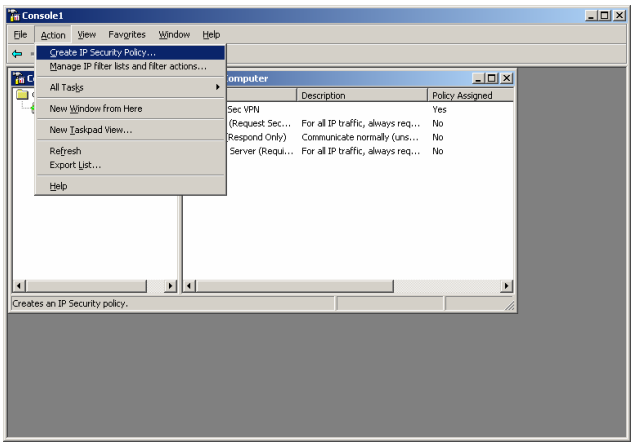


- Keep the default value “Local computer” and click on “Finish”. Back on the Snap-in window click “Close” and “OK”

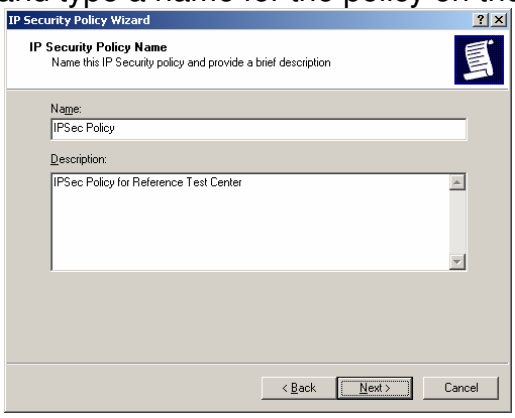




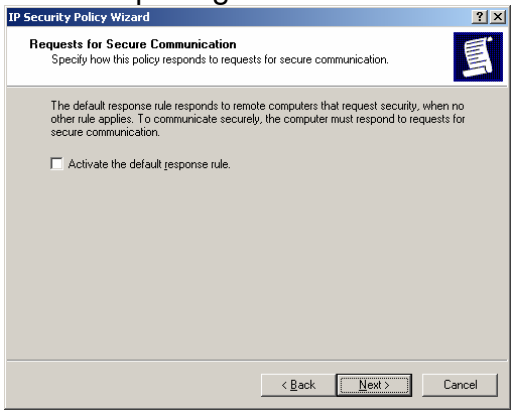
- In the “IPSec policies” window select to create a new IP security policy



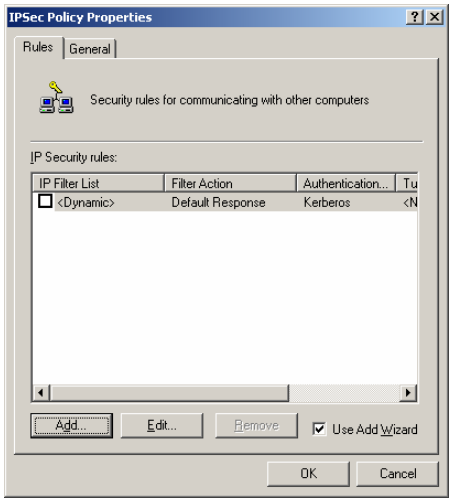
- Click “Next” on the welcome screen and type a name for the policy on the next window



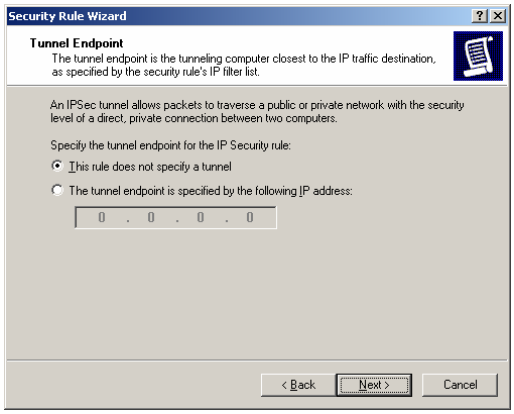
- Deactivate the checkbox for “Activate the default response rule” and click on “Next”. In the “Completing” window check the box for “Edit properties” and click on “Finish”.

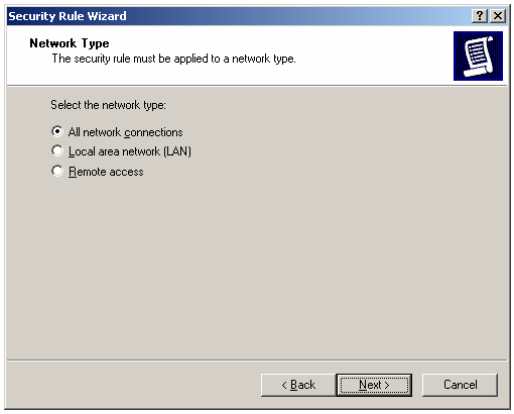


- In the created policy click on “Add…” in order to create a security rule. In the Welcome window click on “Next”.

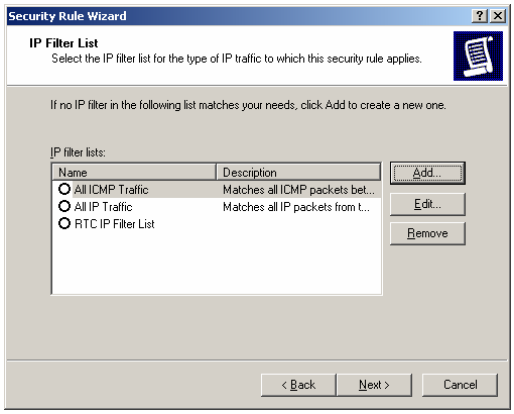


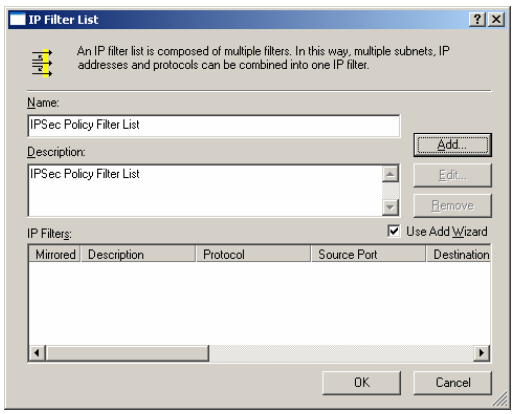
- Keep the default values in the “Tunnel Endpoint” and “Network Type” windows as shown below and click on “Next”



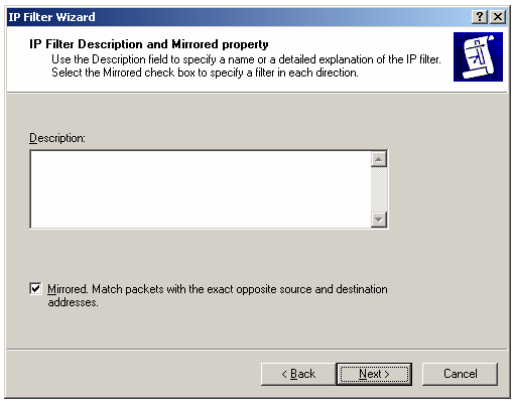


- Now an IP filter list must be created. Select “Add…” on the next window and type a name for the filter list



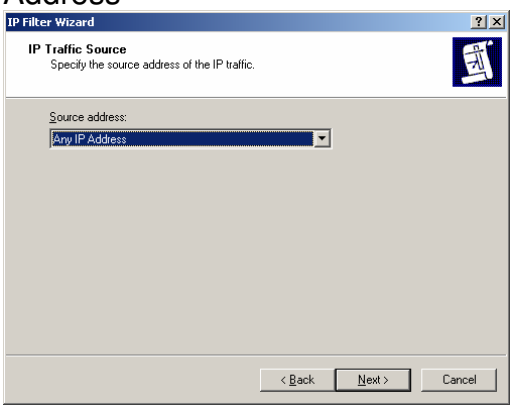


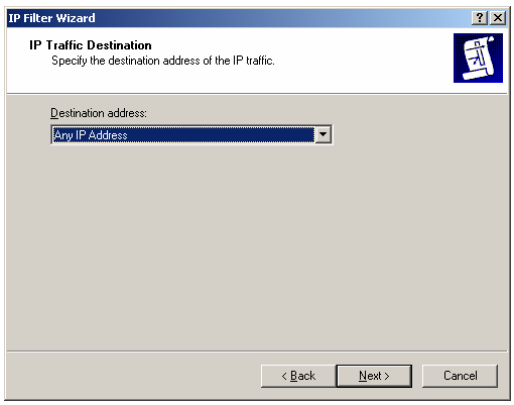
- On the “Welcome” window click “Next” and verify the checkbox for “Mirrored…” is activated. Click then on the “Next” button.



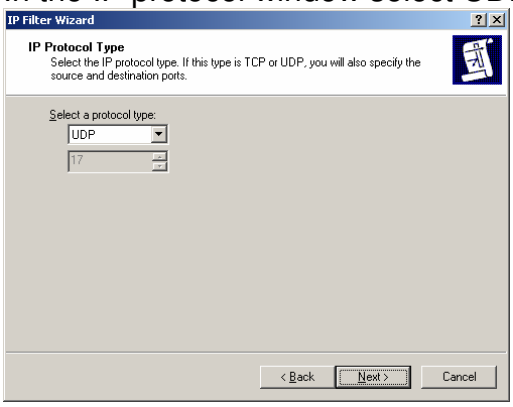
© VODAFONE GROUP 2007

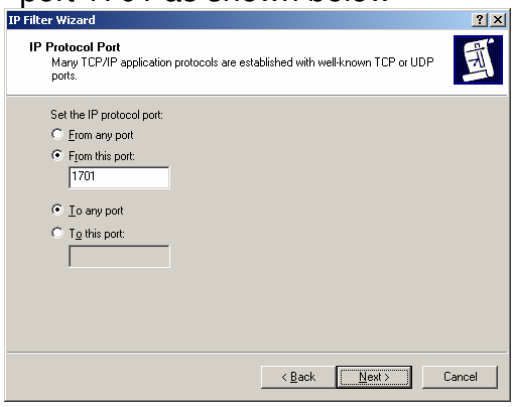
- For the client remote access set the source and destination address to “Any IP Address”



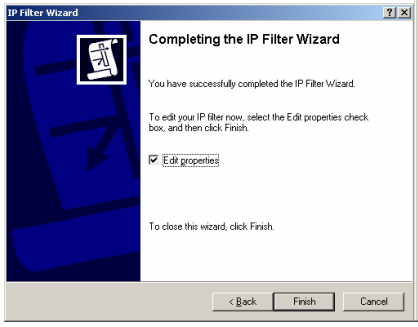


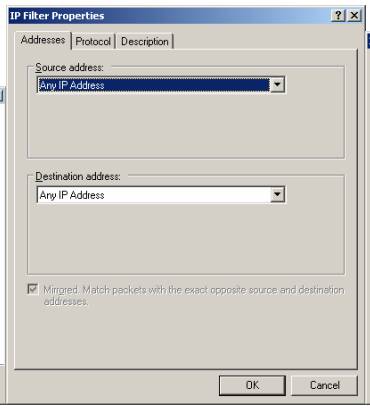
- In the IP protocol window select UDP port 1701 as shown below

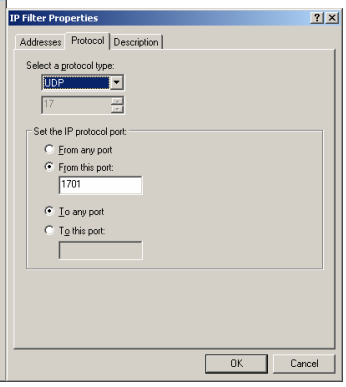




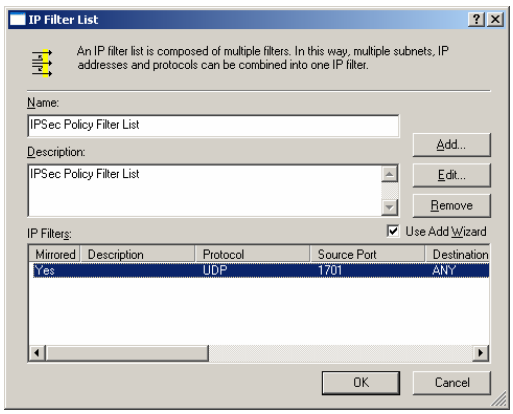
- In the “Completing IP Filter” window click on “Finish”. You can also check the box “Edit properties” in order to change or verify the settings.

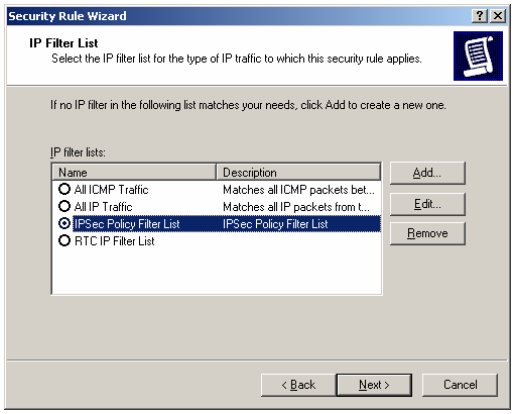




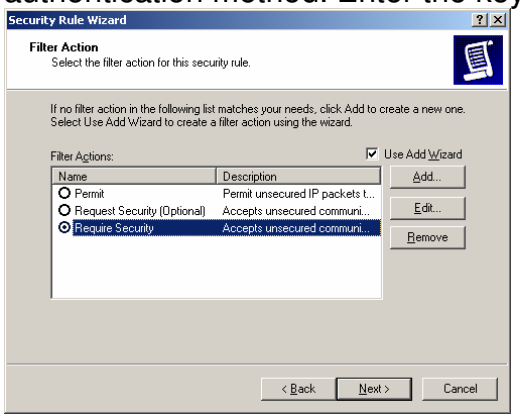


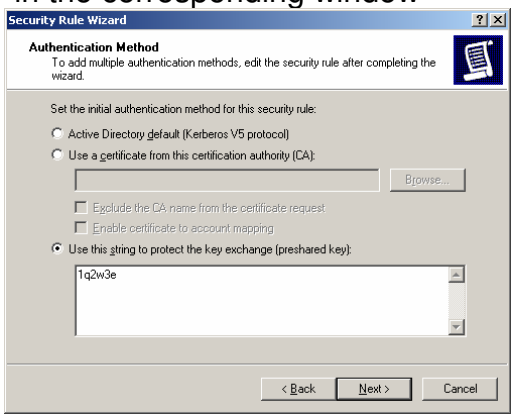
- Click on “OK” for the filter list and select the created filter list in the “Security Rule Wizard”





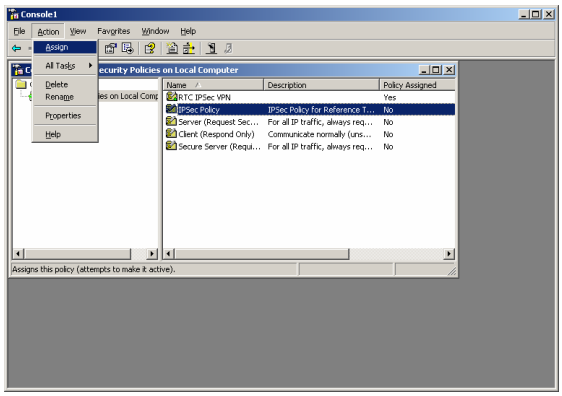
- As an action for the filter select “Require security” and preshared key as the authentication method. Enter the key in the corresponding window





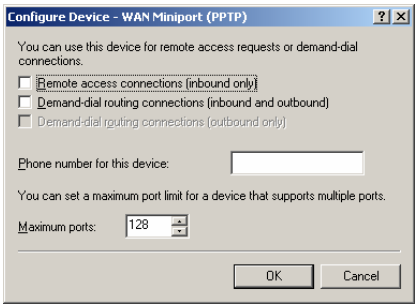
- On the “Completing Security Rule Wizard” window click on “Finish”. In order to change or verify the settings check the box “Edit properties”

- Back in the Management Console, you must assign the created IPSec policy by using the menu entry. Highlight the correct policy and select “Action” -> “Assign” from the menu.

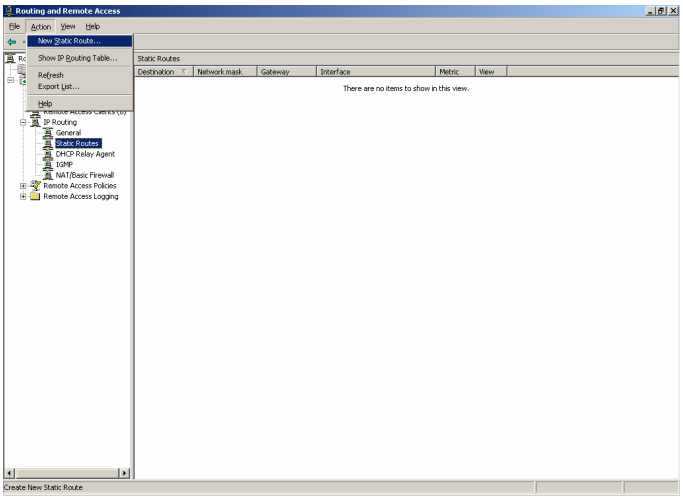


2.4 Advanced settings

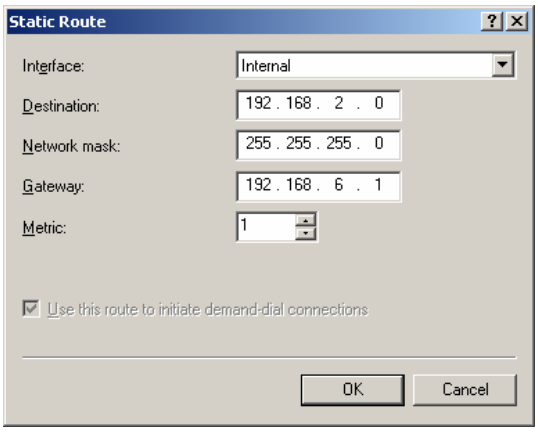
- Since in this configuration we use only L2TP/IPSec, all other protocols which are by default added to the Routing and Remote Access service can be disabled. In the Routing and Remote Access select “Ports” and open the properties. PPTP and L2TP are enabled with 128 ports for each protocol. Also the number of connections (ports) can be limited in this window. Select “PPTP”, click on “Configure” and uncheck the setting “Remote access connections”.



- In case the VPN server is not directly connected with the private interface to the corporate LAN, a static route must be defined within the “Routing and Remote Access” service. Navigate to “IP routing” -> “Static Routes” and select “New Static Route”.



- Insert the corresponding route entries.



2.5 Keep alive messages

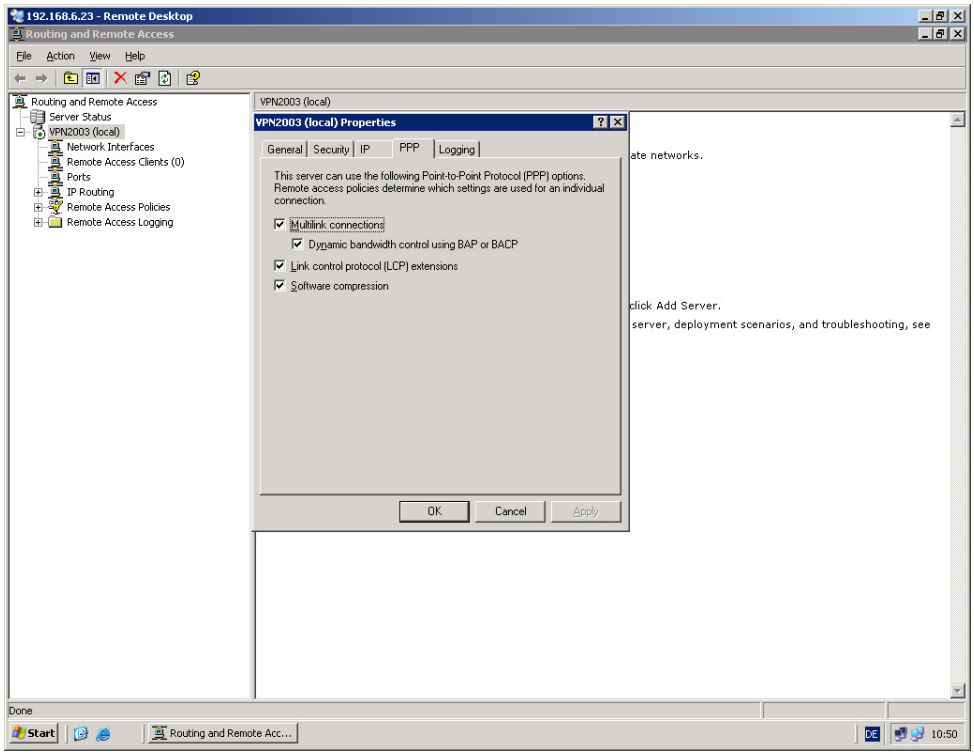
The Microsoft Windows L2TP/IPSec VPN connection supports NAT-T keep alive messages. A UDP message that uses the same ports as IKE traffic, contains a single byte (0xFF), and is used to refresh the UDP port mapping in a NAT for IKE and UDP-encapsulated ESP traffic to a private network host.

© VODAFONE GROUP 2007

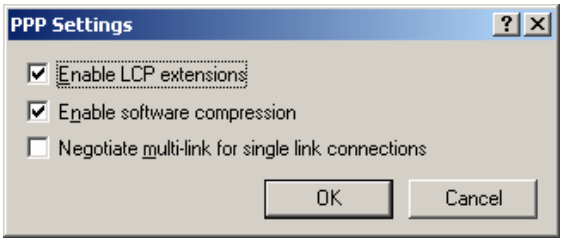
2.6 Data compression

Data compression using LZS compression algorithm is available and can be enabled on the server as well as on the client. On the server this setting is located in the “PPP” tab of the server properties within the Routing and Remote Access configuration. On the client this setting is located in the properties of the VPN type within the “Network” tab. Enabling data compression might speed up the data transmission rate of VPN users.

Server:



Client:



Note that software compression was shown to have little benefit for most environments. The benefit of compression should be reviewed in light of the cost of processor load for both the client and server.

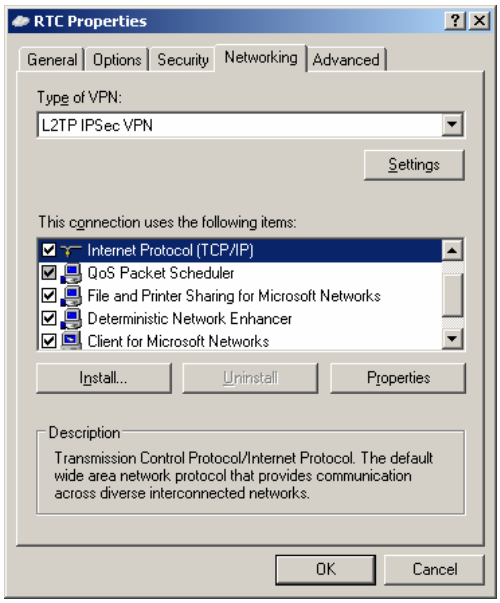
3 Configuration of Split Tunnelling

Split Tunnelling is supported and will be configured on the client. This feature is disabled by default. There is no possibility to allow or disallow this functionality on the server.

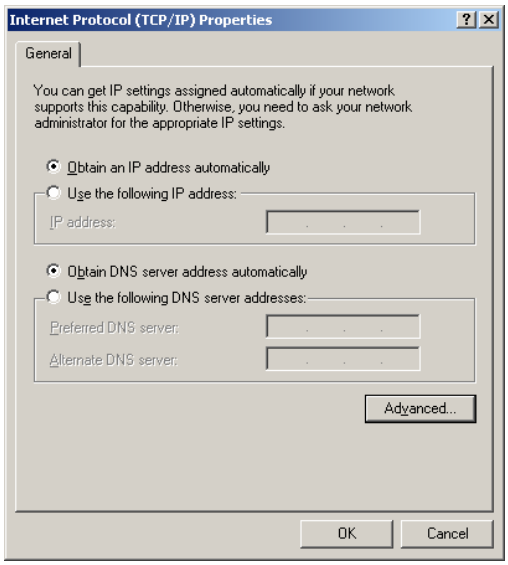
Recommendation: Split tunnelling should be disabled as it creates a security vulnerability at the client end. It is illustrated here for completeness.

Enabling or disabling split tunnelling can be configured on the client, This setting is located in the following window:

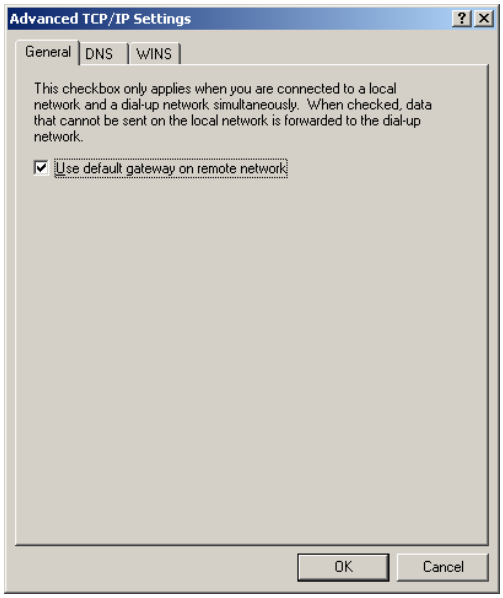
- open the properties of the VPN connection
- select the networking tab
- Highlight the “Internet Protocol (TCP/IP)” and click on the “Properties” button.



- On the “General” tab of the TCP/IP properties click on the “Advanced” button

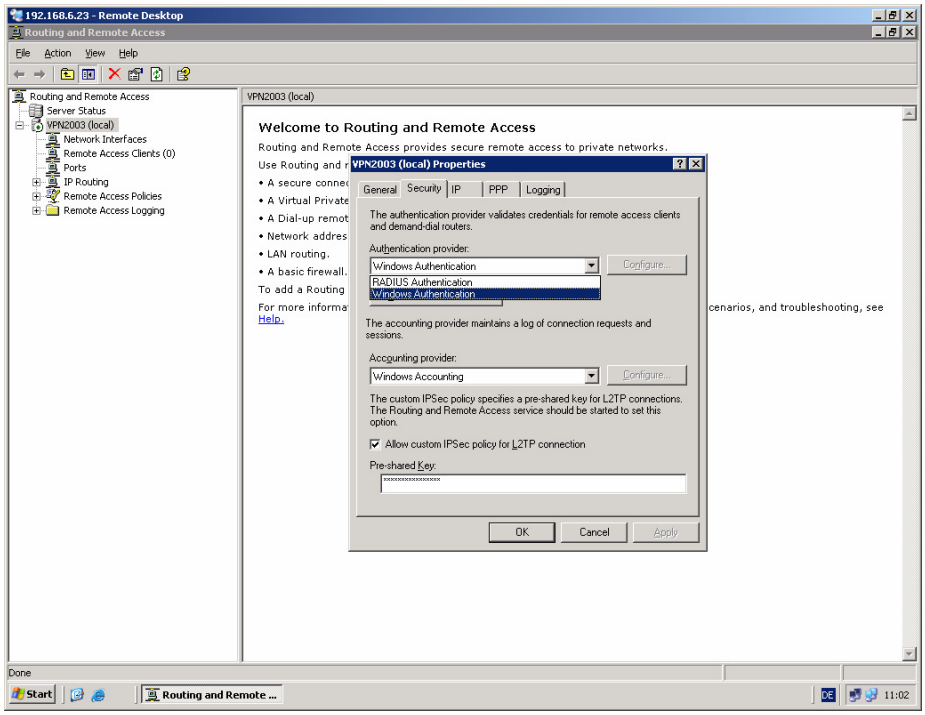


- In the Advanced TCP/IP window check the “Use default gateway on remote network” setting in order to disable split tunnelling or uncheck this setting in case split tunnelling should be enabled.

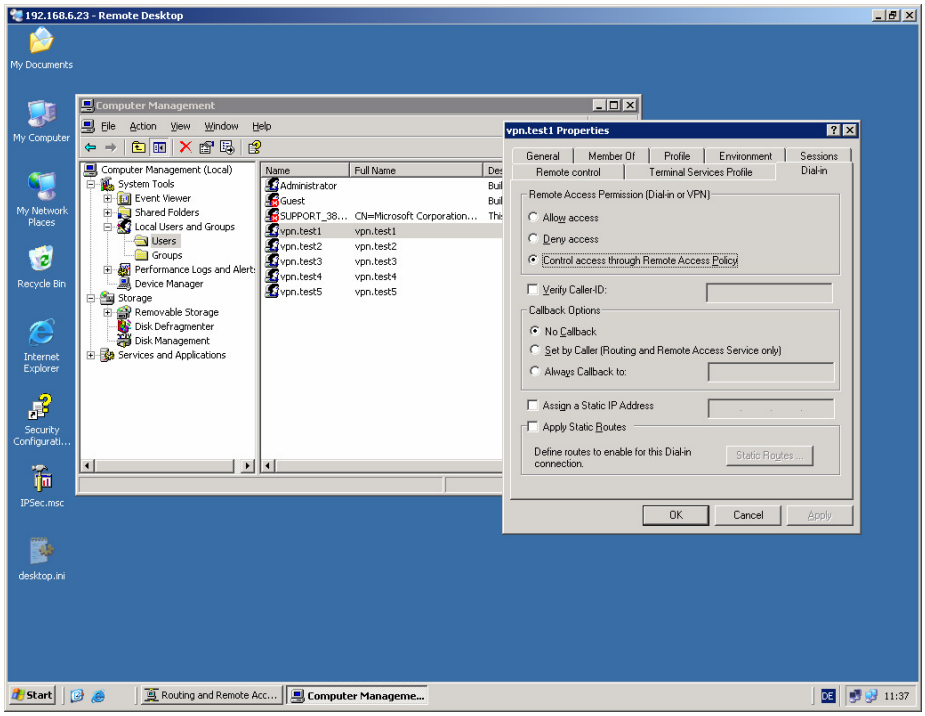


4 User Management and Profile Handling

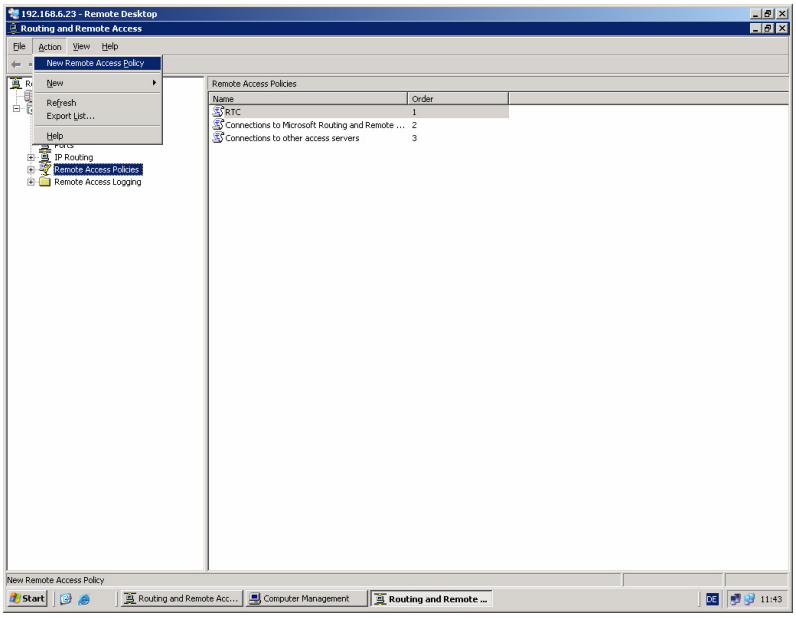
Integrated user management and external authentication using a RADIUS server are supported. You can choose it in the Security tab of the Server properties.



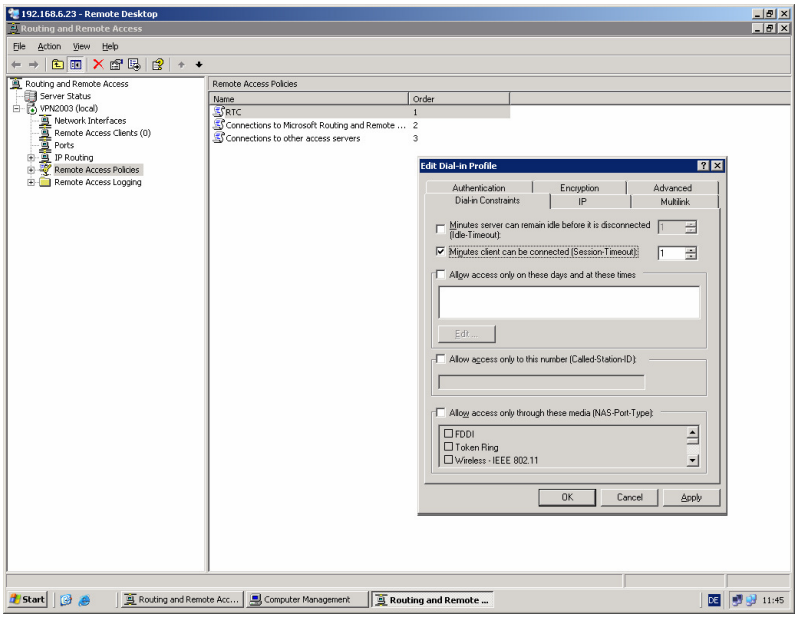
- For the Windows Authentication method local users must be created. In the “Dial-In” tab of the user properties, permissions can be established. There is the possibility to set it either to “Allow access” or “Control access through Remote Access Policy”.



- In case the control is managed through a “Remote Access Policy” this policy has to be created within the “Routing and Remote Access” service on the Server. Navigate to “Remote Access Policies” and select “New” -> “Remote Access Policy” from the right-click contextual menu or from the “Action” menu entry



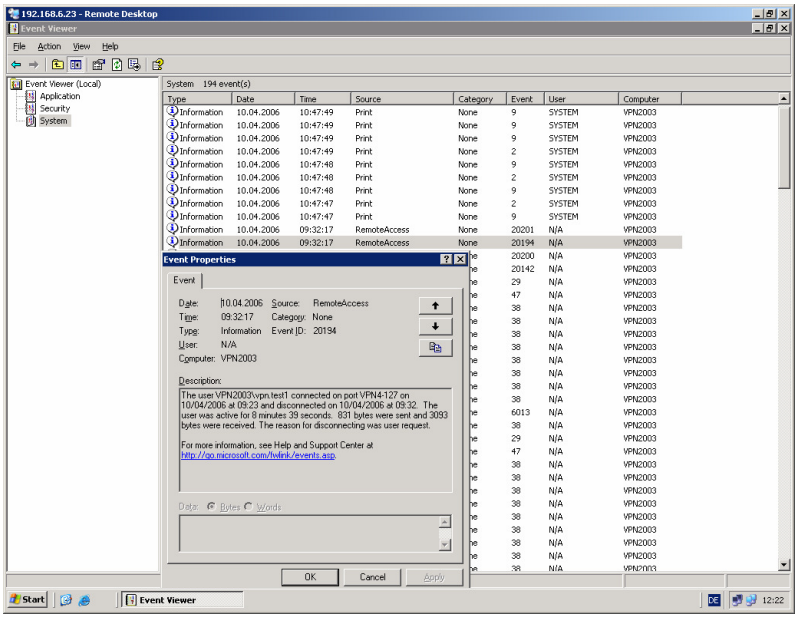
- All Profile settings can be changed from the policy properties using the button “Edit Profile”

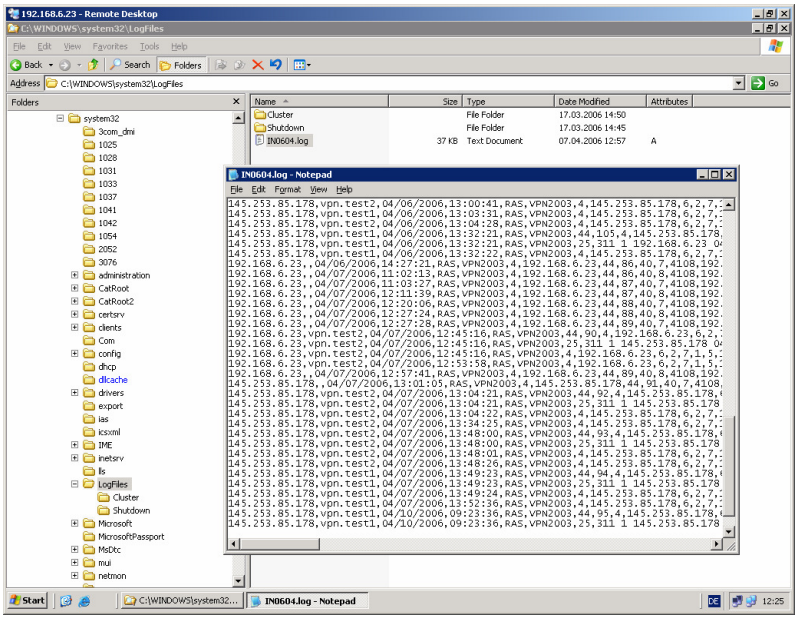


© VODAFONE GROUP 2007

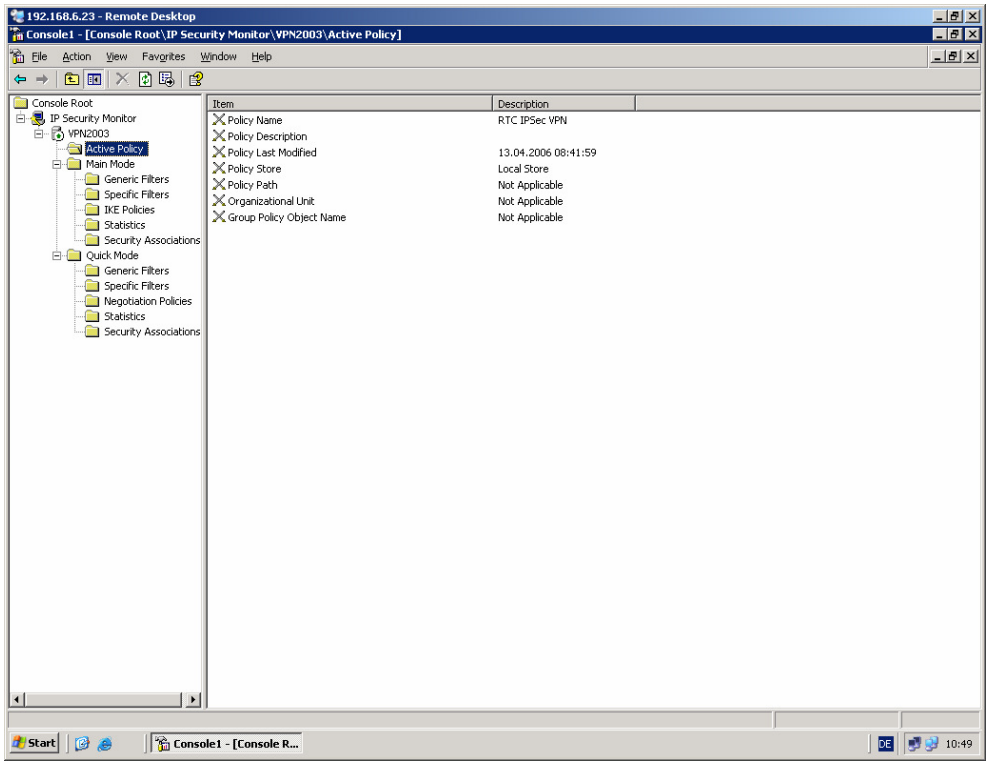
5 Logging

Event logging is available in the Microsoft Windows Event Viewer as well as in logging files created in the “%windir%\tracing” and “%windir%\system32\logfiles” directories. The Event Viewer shows events for connection and disconnection as well as the time and transferred amount of data during this connection.



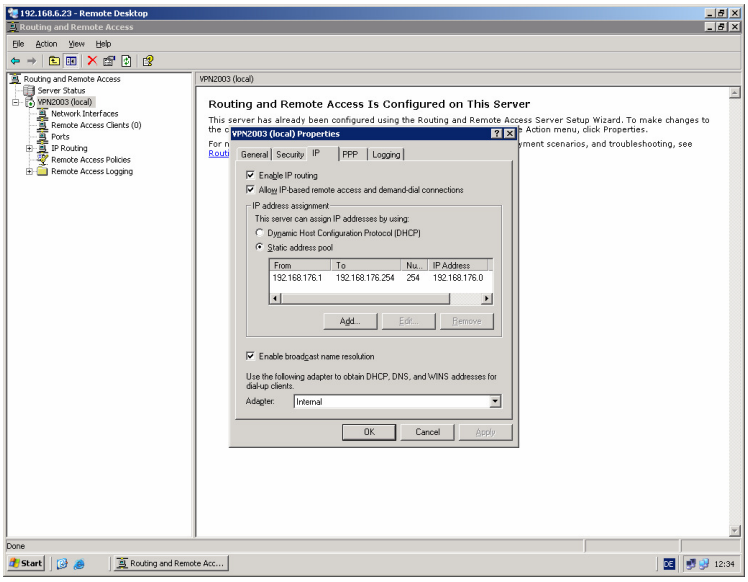


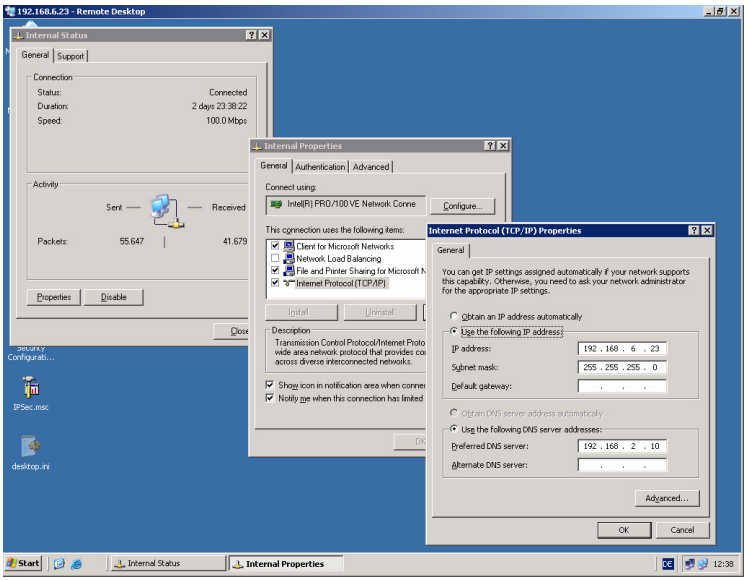
Useful statistics for L2TP/IPSec connections are also included within the “IP Security Monitor” Snap-in.



6 Name Resolution

DNS and WINS configuration is integrated in the “Routing and Remote Access” configuration. In the Server properties navigate to the “IP” tab and select the interface to obtain DNS and WINS addresses for the clients. Make sure the selected interface through which the clients contain the DNS or WINS addresses. After connection establishment DNS server IP address is assigned by the Server to the Client as primary/secondary DNS server for resolving host names.





**** End of Document ****