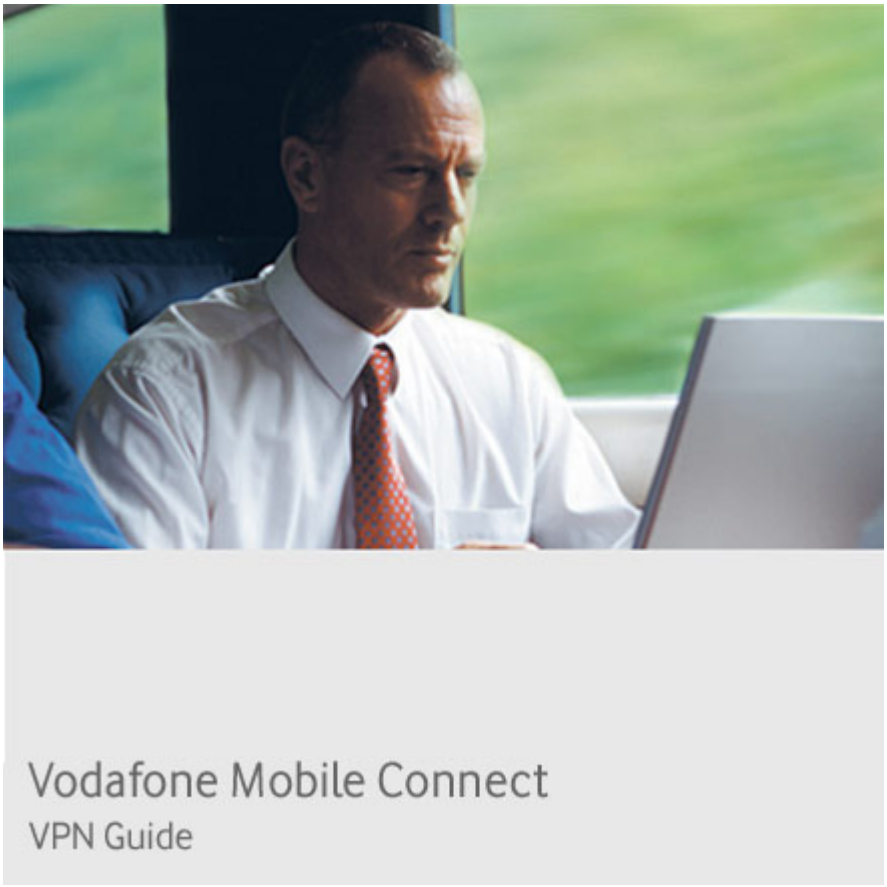
VPN End to End – VPN – MS 2003 L2TP IPSec

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
2.0	May 2006	Update to new versions of VPN software and focus on 3G network performance.
3.0	May 2007	Minor changes & R9 updates

File Reference

VPN - MS_2003_L2TP_IPSec_v3.0

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 5

2 Introduction 6
- 2.1 Test environment 6
- 2.2 Microsoft outline 6
- 2.3 Windows 2003 VPN handling 6
- 2.4 VPN Client System requirements 7
- 2.5 VPN Basics 7

3 Which Protocols are supported? 8
- 3.1 Control connection 8
- 3.2 Data transfer connection 8
- 3.3 Schematic diagram VPN connection 10
- 3.4 Port summary for firewall setup 11
- 3.5 NAT-T “keep alive” messages 11

4 VPN Performance 12
- 4.1 Keep alive messages 12
- 4.2 Overhead caused by IPSec encryption and encapsulation 12
- 4.3 IP compression 12

5 Support of Split Tunnelling 14
- 5.1 Configuration of Split Tunnelling 14
- 5.2 Recommendation 14

6 Additional Applications & Services 15
- 6.1 Client Firewall 15
- 6.2 Virus scanner support 15
- 6.3 Timers 15
- 6.4 SNMP 15

© VODAFONE GROUP 2007

7 Interoperability with Web Optimisers 16
7.1 Test Environment 16
7.2 Test Design 16
7.3 Results 19
7.4 Observations 19
7.5 Recommendations 20

8 Special Settings for 3G/HSDPA/GPRS 21

9 VPN Client Installation and Configuration (Windows XP SP2 integrated Client) 22

10 Configuration & Connection Using VMC Software 23
10.1 Establish the connection (VMC R9) 24
10.2 Establish the connection (VMC R7 and earlier) 24
10.3 Configure VMC for the VPN Client 25
10.4 VPN Client Starting and Connection Option 28

11 Troubleshooting 29
11.1 Logging Concentrator (server side) 29
11.2 Logging Client (client side) 29

Tables & Figures

Table 1 – High-level MS Windows 2003 VPN Environment 10
Table 2 – Logical Flow for Building Connection 10
Table 3 – Port Summary 11
Table 4 – Schematic of Network Generic Optimisation in Mobile Network 17
Table 5 – Test Results for NGO and VPN compression 19

© VODAFONE GROUP 2007

1 Executive Summary

This document provides an explanation using Microsoft Windows 2003 L2TP/IPSec VPN solution with Vodafone 3G related services. Furthermore this document describes diagnosing problems / performance issues with the Microsoft Windows 2003 L2TP/IPSec VPN over Vodafone 3G related services. A general overview regarding the Microsoft Windows 2003 L2TP/IPSec installation/update and configuration for both the Server and the client software is given in another document.

A schematic diagram reflects the usage of e.g. Network generic optimisers used within the Vodafone's 3G networks in conjunction with the VPN solution of Microsoft 2003 environment.

Standard usage scenarios are used to replicate daily usage within companies and their potential VPN users. Scenarios such as mail synchronisation, remote working and download are tested in combination with generated overhead and various factors such as VPN keep alive, compression etc. As a result of these test scenarios, recommended settings are highlighted for Vodafone 2.5G and 3G related services.

Key findings and recommendations are:

- VPN overhead was measured at ~10% (as is typical for VPN systems) and should not be a significant factor in either performance or total data volume
- IKE keep-alive packet counts may need to be increased for users in difficult transmission environments to reduce disconnections
- Data compression offers little benefit for most broadband users, but may have a role for lower-speed connections, although many of the benefits are already obtained from the network optimizers implemented in most mobile networks and integrated into the Vodafone Mobile Connect software
- By contrast, application-level compression (such as provided by Microsoft Outlook / Exchange 2003) DOES have a significant benefit and should be enabled
- Split-tunnelling is not recommended as it presents a security vulnerability
- Operations with network web optimizers was tested satisfactorily and shown to have the greatest impact on web (http:) traffic while transfers of already-compressed files (such as MP3) showed no benefit

No general performance or interoperability issues were identified using this VPN solution in the test environment.

© VODAFONE GROUP 2007

2 Introduction

This chapter describes the Microsoft Windows 2003 VPN environment and the needed prerequisites for usage.

2.1 Test environment

The tests are based on a Windows 2003 Server with Service Pack 1. Since the role of the server is to act as a VPN concentrator, this server does not need to be within an Active Directory Domain.

As Client software the integrated Windows XP SP2 client was used. This was installed on an IBM T20 notebook.

2.2 Microsoft outline

The Microsoft Windows VPN solution is based on the standard Windows 2003 installation. After basic installation there is a need to configure the server to act as a VPN concentrator. For both methods (PPTP and L2TP/IPSec) Routing and Remote Access must be configured.

2.3 Windows 2003 VPN handling

A VPN in servers running Windows Server 2003 is made up of a VPN server, a VPN client, a VPN connection (that portion of the connection in which the data is encrypted), and the tunnel (that portion of the connection in which the data is encapsulated). The tunnelling is completed through one of the tunnelling protocols included with servers running Windows Server 2003, both of which are installed with Routing and Remote Access. The Routing and Remote Access service is installed automatically during the installation of Windows Server 2003. By default, the Routing and Remote Access service is turned off. The two tunnelling protocols included with Windows are:

- Point-to-Point Tunnelling Protocol (PPTP): Provides data encryption using Microsoft Point-to-Point Encryption.
- Layer Two Tunnelling Protocol (L2TP): Provides data encryption, authentication, and integrity using IPSec.

Both Microsoft Windows Server 2003 and Windows XP support the Layer Two Tunnelling Protocol (L2TP) with Internet Protocol Security (IPSec) virtual private network (VPN) connection technology. The combination of L2TP and IPSec, known as L2TP/IPSec is supported by all current Microsoft 32 and 64-bit operating systems with the latest updates. Historically, one of the problems with L2TP/IPSec is that IPSec peers cannot be placed behind a network address translator (NAT) because Internet Key Exchange (IKE), the protocol used to negotiate SAs, and IPSec-protected traffic are not NAT-translatable.

© VODAFONE GROUP 2007

However, a new set of Internet drafts describe IPSec NAT traversal, in which IKE messages and processing are modified and IPSec-protected packets are encapsulated as User Datagram Protocol (UDP) messages. This allows L2TP/IPSec connections to be created for client and server computers that support IPSec NAT traversal that are located behind one or multiple NATs.

2.4 VPN Client System requirements

Since the Microsoft Windows VPN client is integrated in the operating system, the computer must meet the requirements for Windows XP described on following web pages:

http://www.microsoft.com/windowsxp/home/upgrading/sysreqs.mspx

http://www.microsoft.com/windowsxp/pro/upgrading/sysreqs.mspx

2.5 VPN Basics

A VPN is used to establish a secure method for access to the corporate LAN and resources while working remotely. The VPN solves the two fundamental security issues for remote access:

1. Restrict access to authorised users only
2. Prevent interception of communications

Previously these goals were accomplished by restricting remote access and using private network facilities. However, this is inconvenient for users (and reduces productivity for the company) and the private network can be expensive to set up and maintain. A VPN is used to accomplish the same goals while using the Internet as a network transport.

A VPN incorporates:

- Software on the remote (client) computer to control the VPN connection
- Software (and often hardware) at the corporate network (concentrator)

Many different VPN solutions are available from a range of vendors. The client software is designed to work with its matching concentrator component, but some mix-and-match solutions are possible. Each solution has a range of parameters to control setup, maintenance, monitoring, and operation of the VPN connection.

This document describes the configuration of the VPN and the selection of parameters to provide the optimal experience using mobile networks, particularly 3G and HSDPA. Appendices provide detailed description of the installation configuration of the client software and concentrator in this environment.

© VODAFONE GROUP 2007

3 Which Protocols are supported?

3.1 Control connection

Microsoft Windows 2003 L2TP/IPSec connection uses Internet Key Exchange Protocol (IKE) to set up a VPN tunnel. Standard IKE with UDP/500 as destination port will be used. The source port used is any arbitrary port number. Answers are sent back to the source port of the original message.

3.2 Data transfer connection

3.2.1 Standard connection

Microsoft uses a combination of Layer 2 Tunneling Protocol (L2TP) and IPSec to set up a VPN connection:

First, an IPSec control connection over Internet Key Exchange (IKE) is established. This is carried out over UDP port 500, and uses either a pre-shared key, public keys, or X.509 certificates on both ends for authentication.

Second, the Encapsulated Security Payload (ESP) connection in transport mode is negotiated. The IP Protocol number for ESP is 50. At this point, a secure channel has been established, but no tunneling is taking place.

Now, negotiation and establishment of L2TP tunnel between the IPSec endpoints takes place. The actual negotiation of parameters takes place over the secure channel, within the IPSec encryption.

The first data packet sent over a L2TP/IPSec connection is used to establish a PPP connection. Data packets are first encrypted and encapsulated with a PPP header. The resulting PPP frame is then encapsulated with the L2TP header, which uses the UDP port 1701. This data will then be encrypted with the IPSec Encapsulating Security Payload (ESP), which contains the source and destination IP addresses that correspond to the tunnel endpoints.

IP-Header	ESP-Header	L2TP-Header	PPP-Header	**Payload**

3.2.2 NAT-Traversal

Microsoft Windows L2TP/IPSec VPN connection does work in an environment where Network Address Translation (NAT) and Network Address and Port Translation (NAPT) are used, with the implementation of NAT traversal. No configuration for IPSec NAT traversal is required. Microsoft L2TP/IPSec VPN Client automatically determines whether there are any NATs in the path and whether the VPN server is capable of doing IPSec NAT traversal. If both of these conditions are true, Microsoft L2TP/IPSec VPN Client

© VODAFONE GROUP 2007

automatically uses IPSec NAT traversal, which is defined as UDP port 4500. Support for IPSec NAT traversal is integrated in the Windows Server 2003 family and in Microsoft Windows XP SP2 clients. For any other operating systems such as Windows 2000 or Windows XP SP1 Microsoft offers an update for L2TP/IPSec NAT-T.

IP-Header	UDP-Port 4500	IP-Header	ESP-Header	L2TP-Header	PPP-Header	**Payload**

For detailed information please refer to the following web page:
http://support.microsoft.com/kb/818043/en-us

3.3 Schematic diagram VPN connection

The following illustrates a high level diagram of the Implemented Microsoft Windows 2003 VPN environment and building a connection from Client to the concentrator (server).

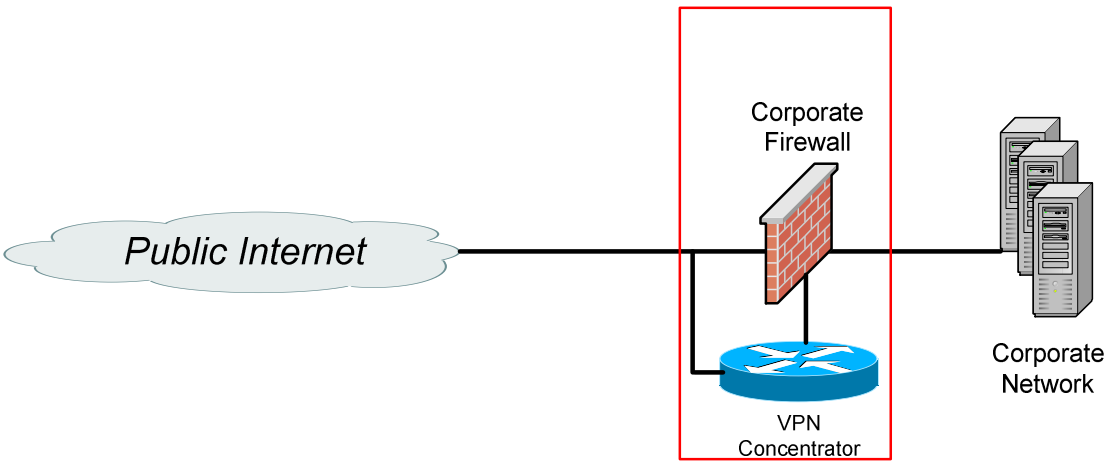


Table 1 – High-level MS Windows 2003 VPN Environment

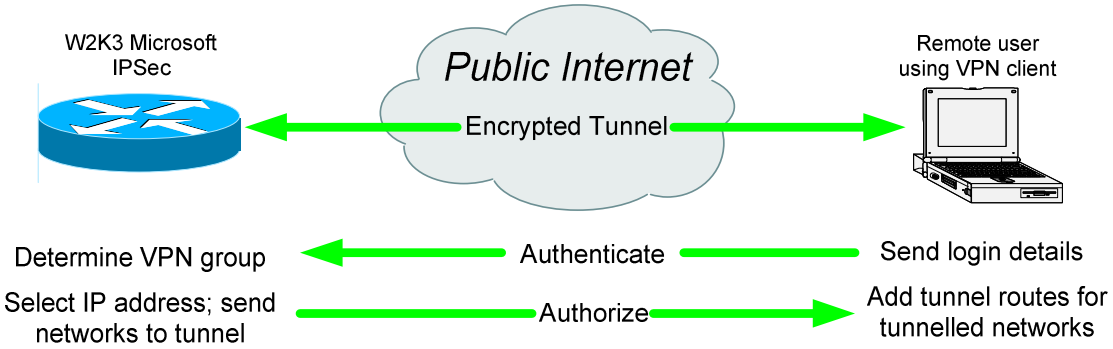


Table 2 – Logical Flow for Building Connection

3.4 Port summary for firewall setup

This table shows a summary of the ports used by the concentrator and has to be set up on the appropriate firewall.

Name	Protocol	Source Port/Service number	Destination Port/Service number	Connection Initiation	Comment
Standard IPSec					
IKE (Standard)	UDP	Arbitrary > 1024	500	Client → Server	
ESP	IP	50	50	Client → Server	
Encapsulated IPSec (for NAT-Traversal)					
IKE	UDP	Arbitrary > 1024	500	Client → Server	
NAT-T	UDP	Arbitrary > 1024	4500	Client → Server	

Table 3 – Port Summary

The internally used protocols, e.g. L2TP, Port UDP/1701, do not need to be opened on any firewalls passed, because they are hidden within the encrypted IPSec data.

3.5 NAT-T "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

4 VPN Performance

This chapter describes different types of performance settings and their meanings.

4.1 Keep alive messages

This feature lets the VPN Server monitor the continued presence of a remote peer and to report its own presence to that peer. If the peer becomes unresponsive, the VPN Server drops the connection.

L2TP/IPSec client, by default, sends "keep-alive" packet every 20 seconds to make sure the NAT table entry on IP provider side is kept updated and has a size of about 43 bytes.

The server sends out a keep-alive message every 40 seconds to verify the client is active and the tunnel still exists and has a packet size of about 102 bytes.

4.2 Overhead caused by IPSec encryption and encapsulation

IPSec overhead with the option IPSec over UDP and 3DES encryption was measured. The overhead was 118 bytes/packet. Sometimes there will be an additional overhead of some bytes to fill a packet to its optimal size. Given a default packet size > 1000 bytes, the IPSec overhead is thus <10% for most applications generating well-filled packets, although highly interactive applications (messaging, Telnet) will experience a higher % overhead (on a generally smaller traffic level).

4.3 IP compression

Data compression using LZS compression algorithm is available. 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.

<u>Notes and recommendations:</u>
Data compression increases the memory requirement and CPU utilization for each user session and consequently decreases the overall throughput of the VPN concentrator.

From our point of view there would be two recommendations for companies using only low bandwidth and companies using a broadband connection for the wireless VPN connection:

1) For this reason, enabling data compression is only recommended for users connecting with low bandwidth such as GPRS.
2) For broadband users the IP compression is not needed at the first place.

© VODAFONE GROUP 2007

Furthermore, it depends on the type of files which are usually transferred across the network. If users are transferring mostly highly-compressed files, such as MP3 or JPG, there is no reason to enable compression at all, as there is no further benefit.

In addition some current applications like Microsoft Outlook 2003 and Microsoft Exchange 2003 offer an internal compression as well and once the data is compressed it cannot be compressed again clearly. See chapter 7.2 for some results.

© VODAFONE GROUP 2007

5 Support of Split Tunnelling

The Client-server VPN connection does support split tunnelling and it is disabled by default on the client. In some scenarios it makes sense to have some local traffic on the Client network and even traffic to the public internet not passing the VPN tunnel and generating additional delay and overhead.

We recommend **not** using split tunnelling for security reasons.

5.1 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.

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

Note, in case split tunnelling is enabled and the corporate network is on another DMZ than the Windows 2003 Server, the user needs to have a static route on the client to the corporate network. This is the case in the network environment the tests were performed.

If split tunnelling is disabled by choosing the option “Use default gateway on remote network” the internet connection can be established using an internal proxy or directly from internal network through the Firewall.

For use with Mobile Connect Cards over the Vodafone 3G/HSDPA/GPRS infrastructure there are no special settings necessary except the compression in case a low-bandwidth like GPRS is used. The compression setting is described in section 4.3.

5.2 Recommendation

We recommend further having the split tunnelling disabled. Otherwise you open serious backdoors over your remote Clients into your private LAN.

© VODAFONE GROUP 2007

6 Additional Applications & Services

This chapter describes additional applications and services such as firewall, virus scanner etc.

6.1 Client Firewall

Local Firewall is an integral part of the Windows XP computer running SP2. The firewall is enabled by default. No changes from the default settings are needed for the VPN connection with L2TP/IPSec to work. When enabled, this feature prohibits inbound sessions from all networks, whether or not a VPN connection is in effect. The Firewall can be enabled or disabled for the whole system or for each network connection separately. Also the configuration of exceptions within this local firewall is possible. For more information of how to configure the Windows XP firewall see the online help and/or the Microsoft knowledge base articles.

6.2 Virus scanner support

No virus scanner service is available on the Microsoft Windows 2003 VPN concentrator. A 3rd party virus scanner service should be used.

6.3 Timers

Microsoft VPN Server offers the possibility to configure the idle-timeout and the maximum connect time (session-timeout). It is configurable in the remote access policies within the Routing and Remote Access service.

Idle Timeout: if there is no communication activity on a user connection in this period, the system terminates the connection.

Maximum Connect Time (session-timeout): at the end of this time, the system terminates the connection. For both timeouts, by default, this property is not set and there is no maximum session limit. The minimum is 1.

6.4 SNMP

A server running Routing and Remote Access can participate in a Simple Network Management Protocol (SNMP) environment as an SNMP agent. For this configuration, you need to install the SNMP service. The remote access server records management information in various object identifiers of the Internet MIB II that is installed with the SNMP service. For more information of how to configure the SNMP service on a Windows 2003 Server see the online help and/or the Microsoft knowledge base articles.

© VODAFONE GROUP 2007

7 Interoperability with Web Optimisers

As most Vodafone and partner networks are supporting Network Generic Optimisers (NGOs), the VPN system was tested under typical NGO conditions. These are the optimisers from Flash Networks, used in the French (SFR) and Italian networks and the ByteMobile Macara system used in most of the other networks.

Web Optimisers operate by compressing the data stream to reduce the volume of transmitted data thus decreasing the time needed for transmission. While some optimisation is performed for all traffic, the main impact is seen when the client software is used in conjunction with the network-based optimiser. The client applications for Flash Networks and for ByteMobile Macara are integrated with the appropriate national versions of VMC software to provide this benefit to the user. However, because of the encryption and integrity checks of the IPSec data packets, optimisation at the application layer is not possible and network optimisation is difficult.

Tests were conducted to determine:

- Does the combination of NGO and VPN work correctly?
- What is the impact of the NGO and VPN on performance?

Recommendations are made regarding VPN usage with NGO for common business applications.

7.1 Test Environment

The following environment was used for the test:

- IBM T20 Notebook running Windows XP Professional SP2
- DELL Inspirion 8600 Notebook, XP Professional SP 2
- Microsoft Outlook 2003 SP2
- DU Meter Version 3.07 Build 200 for measuring data transfer
- Vodafone Mobile Connect Card UMTS/GPRS Option Fusion, firmware 1.5.5
- Vodafone Mobile Connect software 7.01.0001

The tests were performed using Vodafone Germany's network running Byte Mobile optimisation and using the Macara client integrated into VMC software version 7.

7.2 Test Design

Relative performance was assessed by transferring files of known size and measuring the amount of data transmitted. In comparable network conditions, transferring less data will provide the user with better performance.

© VODAFONE GROUP 2007

Examples of two common files were used. A 300 KB Microsoft Word document was chosen to show the possible compression from the NGO systems, the VPN client and Outlook 2003. Additionally, a 3 MB file in MP3 format was used. As the MP3 is itself a compressed format, little further compression should be expected, and the transferred volume will reflect VPN and protocol overhead.

All the test cases were performed with Network Generic Optimisation in the Vodafone network. Even if the optimiser client is not installed, the optimiser server lies within the data flow. For unencrypted data, there is some optimisation possible in the direction from the internet to the client PC, e.g. size reduction in picture files embedded in HTML code.

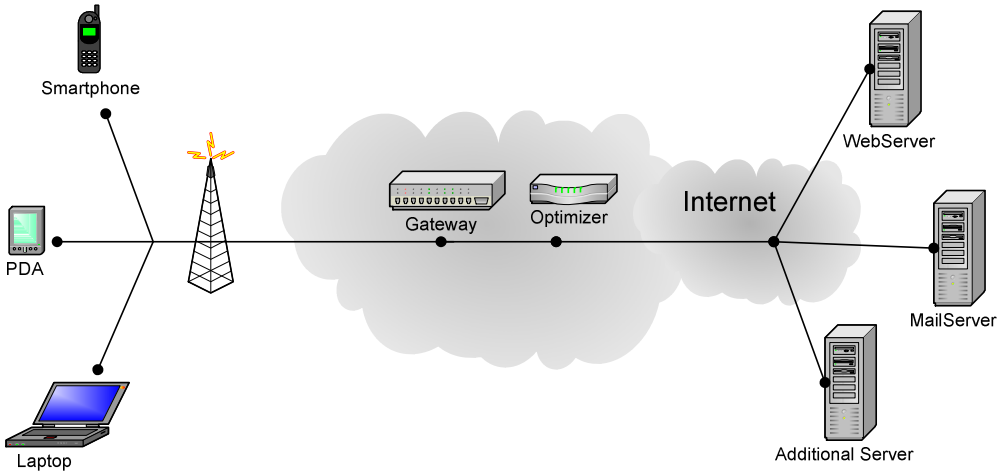


Table 4 – Schematic of Network Generic Optimisation in Mobile Network

7.2.1 Test Cases

The following test cases were considered:

- Split Tunnelling:
  Depending on the setup of the VPN client, unencrypted traffic over the internet can be allowed in addition to the encrypted VPN-traffic. This unencrypted traffic can be optimised by the mobile network, while encrypted traffic (including Internet or intranet access using the encrypted VPN tunnel via the corporate network gateway) is not compressible.

- VPN compression:
  In addition to the VPN functionality, some VPN solutions offer compression of the encrypted data. Because the VPN key length is quite big to ensure privacy, the encrypted data does not compress very well. Therefore, it makes sense to compress the data before encryption. For obvious reasons this can only be done by the VPN client itself.

© VODAFONE GROUP 2007

7.2.2 Use Cases

The following use cases were tested and the volume of data transferred measured for each case, both with / without split tunnelling and with / without VPN compression:

- Mail sending via Outlook / Exchange using VPN:

  The files were attached to an empty mail message and sent to a mail account residing on the Exchange server.

  We noticed that the data transfer to the Exchange server started as soon as the file was attached. To have comparable results, we waited until the data transfer (after adding the document to the mail) ebbed off and then pressed the send mail button.

  For Outlook / Exchange to work, it is important to be able to resolve the Exchange server name on the client PC. For this reason, the name either has to be declared in the local etc\hosts file or DNS name resolution must be possible.

- Access to a intranet HTTP server via VPN:

  The files were downloaded by selecting links on a web page consisting of fixed content (no database or dynamically generated contents) which was accessed via the VPN.

- Access to a internet HTTP server via VPN using split tunnelling:

  The same specially prepared web page was accessed via the internet. This measurement is only possible if split tunnelling is active, since there is no internet access otherwise.

- Access to an intranet FTP server via VPN:

  The files were downloaded from an FTP server.

- Access to a internet FTP server via VPN using split tunnelling:

  The documents were downloaded unencrypted via the internet. This measurement is only possible if split tunnelling is active, since there is no internet access otherwise.

7.2.3 Configuration Notes & Observations

When NAT or NAPT is used, Microsoft IPSec is using a standard NAT-Traversal for the UDP encapsulation. There is no support for TCP encapsulation.

The Macara server works as a proxy server for TCP connections and terminates incoming connections on the server and initiates new connections to the original destination. As the

© VODAFONE GROUP 2007

Juniper NetScreen 5GT uses only UDP encapsulation no problems with the Macara optimisation occurred.

7.3 Results

The results are shown in the table below. For each combination of test case and use case, the transferred data is shown in KB or MB.

Please refer to chapter **Error! Reference source not found.** for further discussion of compression configurations and the impact on VPN concentrator performance.

Used reference files: Word Document = 300 KB MP3 File = 3072 KB = 3 MB[5] Connection: 3G / UMTS		**web.vodafone.de (APN)**							
		Network Generic Optimiser (NGO)							
		Split Tunnelling				**No Split Tunnelling**			
		VPN Compr.		**No VPN Compr.**		**VPN Compr.**		**No VPN Compr.**	
Reference	**Type**	300KB	3MB	300KB	3MB	300KB	3MB	300KB	3MB
300KB / 3072KB	**Outlook[2]**	256	3,47	257	3,44	254	3,45	257	3,47
300KB / 3072KB	**http-internet[3]**	277	3,16	156	3,16	n/a[1]	n/a[1]	n/a[1]	n/a[1]
300KB / 3072KB	**ftp-internet[4]**	284	3,16	287	3,16	n/a[1]	n/a[1]	n/a[1]	n/a[1]
300KB / 3072KB	**http-intranet**	267	3,33	289	3,29	267	3,31	294	3.29
300KB / 3072KB	**ftp-intranet**	274	3,30	305	3,32	266	3,30	304	3,30

1. Direct Internet access is not possible due to the 'No Split Tunnelling' configuration
2. Outlook 2003 and Exchange 2003 are using an internal compression
3. Internet access without VPN tunnel showing the influence of the Macara optimisation
4. Internet access without VPN tunnel. FTP is not optimised by Macara
5. MP3 files are not compressible clearly, so the results of the MP3 file are showing the overhead of the used protocol and the VPN tunnel itself

Table 5 – Test Results for NGO and VPN compression

7.4 Observations

Little overall benefit was observed from enabling compression in the VPN system. Intranet transfers showed 5-15% reduction in data transfer, while FTP (Internet) and Outlook showed no significant benefit. Curiously, HTTP (Internet) showed markedly better performance without compression. A possible explanation is that the VPN compression interferes with that of the NGO.

Previously compressed file formats (MP3 in our example) are not compressed further either by the NGO or the VPN systems. In fact, a slight increase in data transfer (5-15%) is observed reflecting the overhead of encryption and encapsulation of a VPN solution.

© VODAFONE GROUP 2007

For email usage, most of the compression benefit is provided by Outlook 2003 / Exchange 2003, with little further benefit from adding VPN compression to the mix.

Note:
Although the transfer time was not measured, the amount of data volume can be used to get an idea of transfer times as both are related. Nevertheless the transfer time is also depending on the wireless network speed (the bearer in use, network congestion, radio conditions), on the bandwidth of the company network (into the VPN concentrator, across the company network, and out to the internet) and even laptop performance.

7.5 Recommendations

Application-level compression (as illustrated by the Outlook use case) delivers significant benefits and should be enabled where possible.

Companies whose primary remote access applications involve FTP and/or compressed file formats (MP3, JPG, etc) are unlikely to see further benefit from either NGO or VPN compression.

For common download applications using HTTP, the NGO provides a benefit by reducing data transfer volumes leading to better performance. Further compression by the VPN system is not beneficial (and has other negative implications noted below).

In addition, earlier chapters presented important considerations for VPN usage and configuration:

- The CPU impact of compression on VPN concentrators may outweigh the benefits (Section 4.3), particularly for high-bandwidth (3G/UMTS, HSDPA) connections.
- Split-tunnelling is insecure and it was recommended NOT to implement this feature (Section 5.2).

© VODAFONE GROUP 2007

8 Special Settings for 3G/HSDPA/GPRS

For most 3G/HSDPA/GPRS scenarios, there are not enough official IP addresses available for the network operator to supply each device with an official IP address. Therefore, the devices are assigned private IP addresses, which need to be translated into official IP addresses to pass the internet. This is done by the use of Network Address and Port Translation (NAPT) or dynamic Network Address Translation (NAT). Both procedures involve data tables in which the entries are erased after a timeout. This timeout is configurable by the network operator. To achieve traversal of NAT/NAPT, both the concentrator and the client have to be configured to support it.

In the Vodafone Germany 3G/HSDPA/GPRS environment the Microsoft L2TP/IPSec VPN client works without using special settings regardless of using Network Address Translation (NAT) or Network Address and Port Translation (NAPT). The NAT-T implementation in Windows Server 2003 and Windows XP SP2 uses UDP-encapsulation, thus there is no interference with TCP optimisers like ByteMobile Macara or Flash Networks expected.

For an example configuration please refer to the appendix.

© VODAFONE GROUP 2007

9 VPN Client Installation and Configuration (Windows XP SP2 integrated Client)

The Microsoft Windows L2TP/IPSec client does not need to be installed separately. It is by default integrated in the Windows XP operating system. The user only needs to create a new connection from the “Network Connections” window using VPN as the connection type. In addition to this an IPSec policy has to be created on the client and depending on the authentication method a certificate must be installed or a pre shared key has to be configured.

The VPN client can be integrated into the Vodafone Mobile Connect application (for more information refer to chapter 10 “Configuration & Connection Using VMC Software”)

For further help please review the Microsoft documentation and refer to Appendix B: “VPN Client Installation and Configuration”

© VODAFONE GROUP 2007

10 Configuration & Connection Using VMC Software

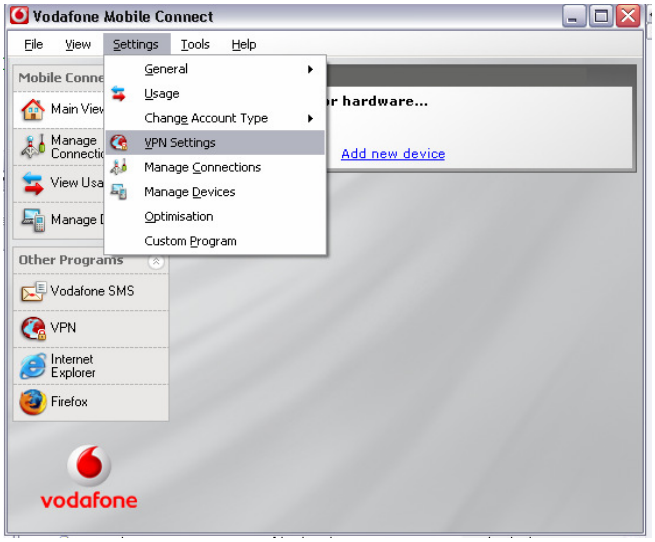
This chapter is used to describe possible configuration possibilities for using the VPN client in conjunction with the current released Vodafone Mobile Connect application.

First you need to build up a connection using your VMC. Insert the SIM into your datacard (or USB modem) and open the Vodafone Mobile Connect application.

Note: The new R9 of Vodafone Mobile Connect software offers the same features but with a different user interface. This document will be updated in due course with full demonstration of the steps using R9.

In short, the differences are:

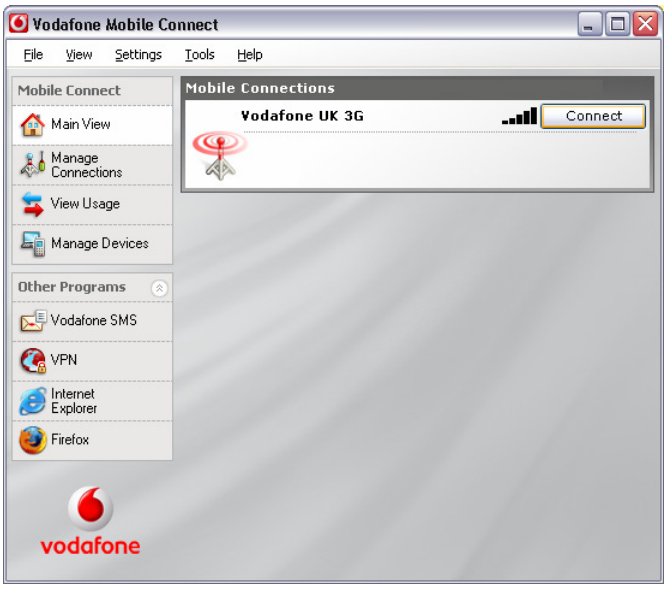
1. The '**Connect**' button is found in the 'Mobile Connections' window of the main screen.
2. The VPN button is found in the '**Other Programs**' section on the left side of the main view. If the Vodafone Mobile Connect software is not visible, it may need to be expanded from the mini view or from the icon in the Windows Notification Area (system tray).
3. The VPN settings can be modified using the **Settings | VPN Settings** commands from the main menu. This dialog will be initiated automatically the first time the VPN button is selected for the user to associate the button with the correct VPN software.



10.1 Establish the connection (VMC R9)

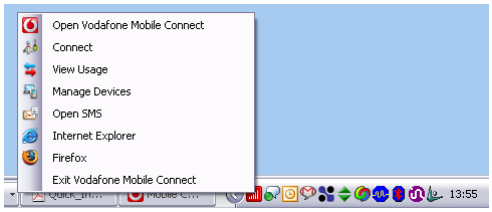
With a SIM card inserted into your datacard (or USB modem), to establish a connection:

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



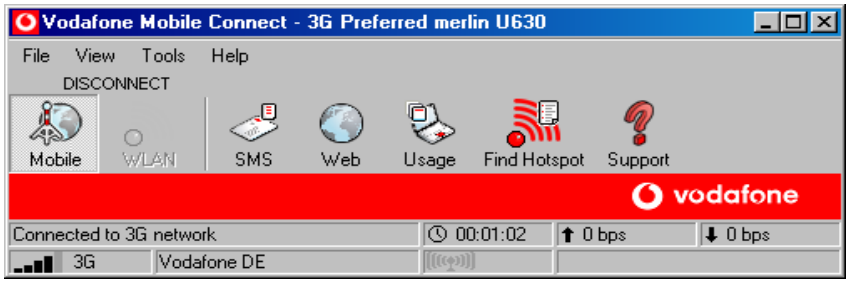
2. In the mini-view, use the **Connect** button, or

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



10.2 Establish the connection (VMC R7 and earlier)

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

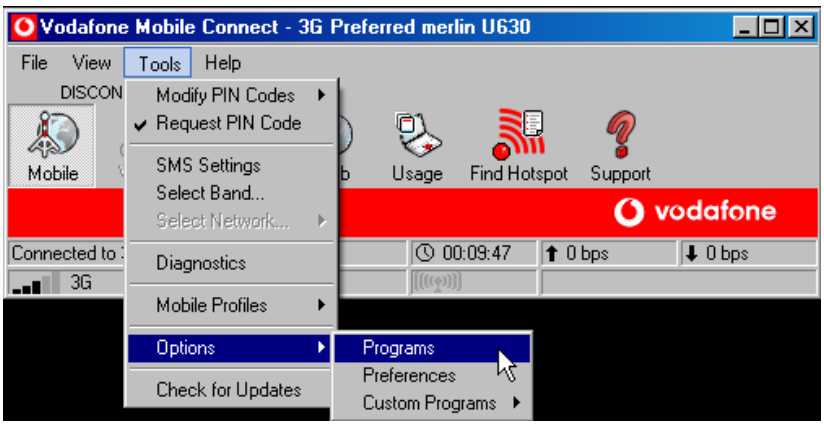


Press the **Mobile** button in the CONNECT/DISCONNECT area of the toolbar

10.3 Configure VMC for the VPN Client

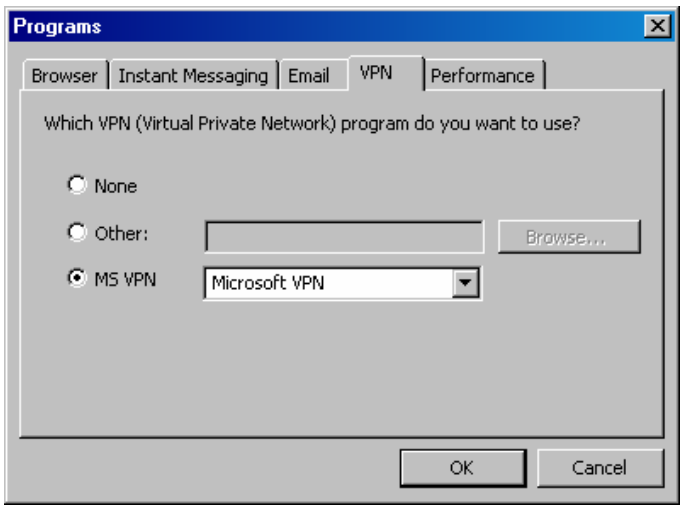
Note: The following steps apply to the legacy version of Vodafone Mobile Connect software R7 and earlier. See notes above on the process using the new R9 version.

- Configure your VPN client as follows to start it from within the VMC software.

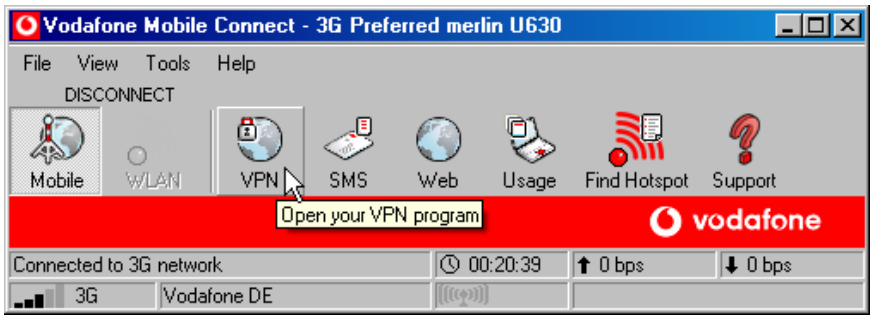


- Choose Tools | Mobile Profiles | Options | Programs

- Check the radio button “MS VPN” and select the profile for the Microsoft Windows L2TP/IPSec connection.



- Confirm your configuration with “OK”



- Click the “Mobile” button on the main Dashboard screen. After you build up your preferred connection, click the “VPN” button to open the VPN Client with your configured profile

© VODAFONE GROUP 2007

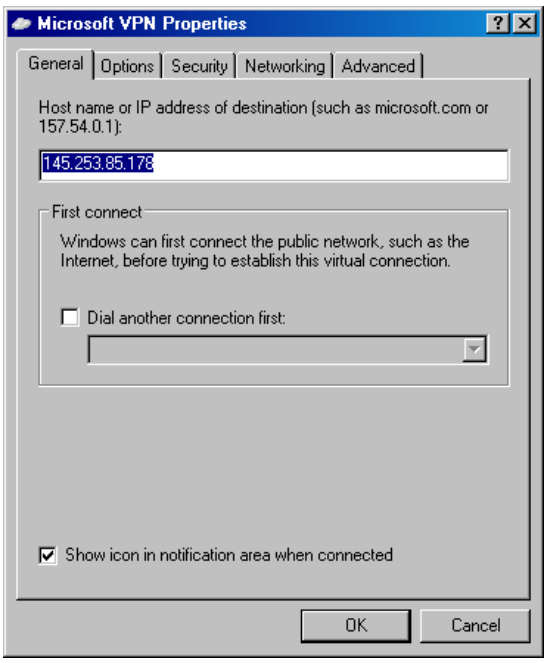
- Click Enter the username and password and click “Connect” in the main dialog and the Client will establish a VPN connection to the Server.

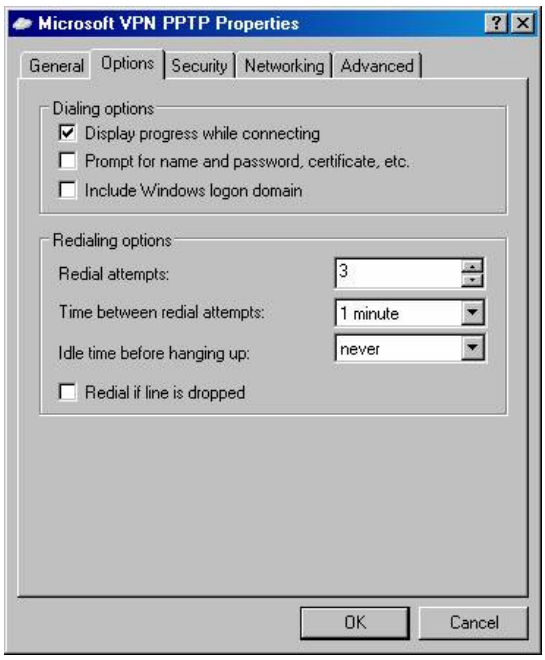
10.4 VPN Client Starting and Connection Option

By default Microsoft L2TP/IPSec VPN Client has to be started manually. It is possible to change the starting option to start automatically e.g. from the “Startup” Windows menu. Also the connection to the Server, by default, must be made manually by pressing the “Connect” button in the VPN Client. This can also be changed to connect automatically. In order to achieve this, the user has to change the following settings:

- Make sure the VPN profile is configured properly
- On the connection window select “Save this username and password for the following users:”
- Click on the “Properties” button on the connection window
- On the “general” tab check the box for “Dial another connection first” and select the profile for the Vodafone Mobile connection
- On the “Options” tab deselect the check box for “Prompt for name and password…”
- Using the Windows drag and drop feature you can now copy a shortcut of the VPN connection to the “Start up” Windows menu

The precondition for establishing a connection automatically using the Vodafone Mobile Connect card is an inserted SIM without a PIN or a scenario where the PIN is already entered.





11 Troubleshooting

In this section general possibilities are explained to troubleshoot issues with the delivered functionality of the components used for the VPN usage.
In fact enabling of logging is a first choice to analyse issues and errors during the usage of building connections or any other mal function of the service provided by the VPN environment.

As the Microsoft IPSec Client is part of the operating system there are only limited testing tools available, but in case of any VPN problem it should be checked, if any Internet connection is possible. Furthermore the Windows Firewall could be disabled to check, if the Firewall configuration may block the needed ports.

11.1 Logging Concentrator (server side)

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.

The log files on the server can be enabled in the Routing and Remote Access snap-in. There are logging options in the properties of the server and in the “Remote Access Logging” section.

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

For further information please refer to the Microsoft documentation.

11.2 Logging Client (client side)

On client side connection and disconnection is logged in the Event Viewer. In order to generate a log file for the IPSec connection, a registry key has to be added. If not present create a new key named “Oakley” in the following location:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\PolicyAgent\
Within this key create a DWORD entry named “EnableLogging” and set the value to “1”.
After a reboot and new IPSec connection establishment, this will create a log file for the IPSec connection in the following directory “C:\Windows\Debug\Oakley.log”

**** End of Document ****

© VODAFONE GROUP 2007