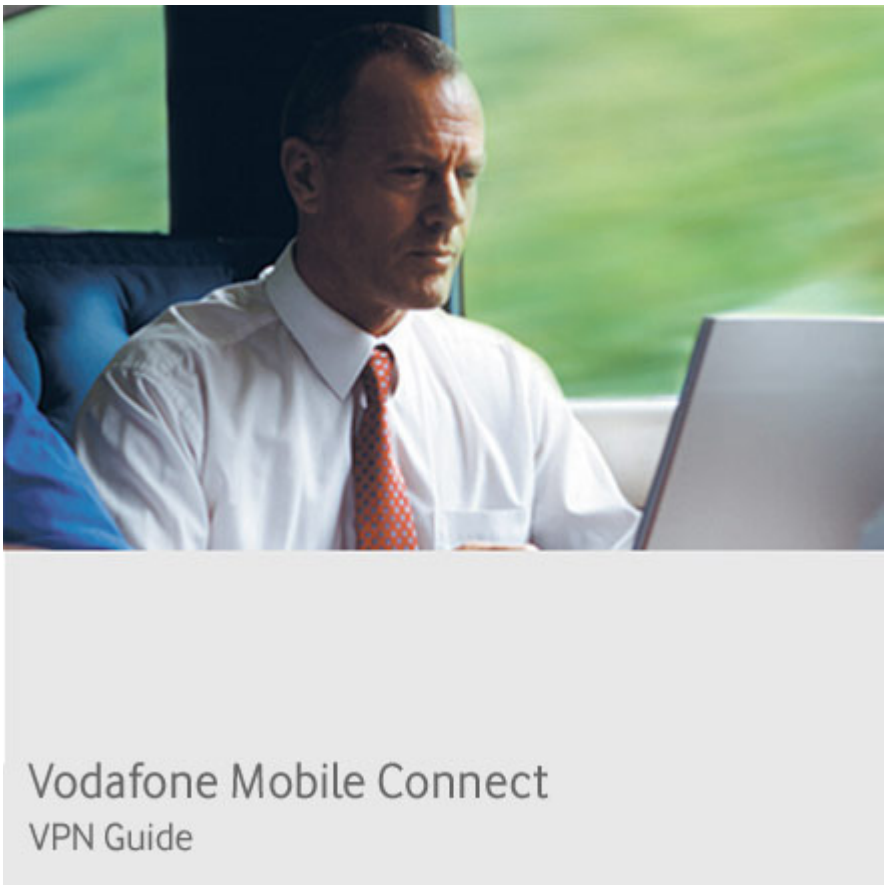
VPN End to End – SonicWALL TZ 170 Wireless VPN

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.
2.1	June 2006	Minor corrections
3.0	May 2007	Minor Changes

File Reference

VPN_SonicWall_TZ_170W_v3.0.doc

Document Authors

Peter Jaeger, TECON Terenci
Miroslaw Grzesica, TECON Terenci
Marcus Hasenbeck, 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 6

2 Introduction 7
- 2.1 Test environment 7
- 2.2 SonicWALL TZ 170 W outline 7
- 2.3 SonicWALL TZ 170 W VPN handling 7
- 2.4 VPN Client System requirements 8
- 2.5 VPN Basics 8

3 Which Protocols are Supported? 9
- 3.1 Control connection 9
- 3.2 Data transfer connection 9
- 3.3 Schematic diagram VPN connection 10
- 3.4 Port summary for firewall setup 11
- 3.5 IKE “keep alive” messages 12

4 VPN Performance 13
- 4.1 Keep alive messages 13
- 4.2 Overhead caused by IPSec encryption and encapsulation 13
- 4.3 IP compression 13

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 Value-added Services, Virus scanner support 15
- 6.3 Timers 15
- 6.4 Reporting, SNMP 15

© VODAFONE GROUP 2007

7 Interoperability with Web Optimisers 16
7.1 Test Environment 16
7.2 Test Design 17
7.3 Results 19
7.4 Observations 20
7.5 Recommendations 20

8 Special Settings for 3G/HSDPA/GPRS 21

9 VPN Client Installation and Configuration 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

11 Troubleshooting 28
11.1 General 28
11.2 Logging Concentrator (server side) 29
11.3 Logging Client (client side) 29

Tables & Figures

Table 1 – High-level SonicWall 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 of how to use a SonicWALL TZ 170 W VPN solution with Vodafone 3G and related services. Furthermore, this document describes how to diagnose problems and performance issues with the SonicWALL TZ 170 W VPN over Vodafone 3G and related services. A general overview of the SonicWALL TZ 170 W installation, update and configuration for both the firewall/VPN appliance and the client software is given in another document.

A schematic diagram shows the use of network generic optimisers within Vodafone 3G networks in conjunction with the SonicWALL TZ 170 W VPN solution.

Standard usage scenarios are used to depict normal use by companies and their potential VPN users. Scenarios such as mail synchronisation, remote working and download are tested in combination with generated overhead, plus various other factors, such as VPN keep-alive and compression. 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% of data traffic which is a typical result for this application
- IKE keep-alive packet counts may need to be increased for users in difficult transmission environments to reduce disconnections
- 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; it is recommended to disable this feature (default is enabled)
- Operation 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 SonicWALL TZ 170 W environment and prerequisites for use.

2.1 Test environment

The tests are based on a SonicWALL TZ 170 Wireless with SonicOS 3.1.0 (Firewall+VPN).

As client software, the Global VPN Client v. 3.1 was used. This was installed on an IBM T20 notebook running Windows XP professional with SP2, a DELL Inspirion 8600 Notebook running XP Professional SP 2 and a Gericom Webgine XL running Windows XP SP2.

2.2 SonicWALL TZ 170 W outline

Firewall with VPN functionality can be used for site-to-site and site-to-client connection capabilities. The W model has WLAN capabilities so is also usable as Access point and guest internet gateway.

The SonicWALL TZ 170 Wireless is a Firewall and Virtual Private Network (VPN) platform designed for small businesses or branch offices that require up to 90 Mbps inspection and 30 Mbps maximum 3DES Encryption performance. It supports up to 50 simultaneous IP security (IPSec) VPN Client sessions (1 session included, up to 50 with upgrade) and up to 10 site-to-site tunnels. L2TP is also supported.

The SonicWALL TZ 170 W offers the firewall/VPN device as an appliance with ready-to-use installed software. There is no need to install and maintain any operating system or additional VPN software. This leads to reduced total cost of ownership, and reduced maintenance downtime. The WLAN interface is 802.11b and g capable and supports WEP and WPA encryption standards.

2.3 SonicWALL TZ 170 W VPN handling

The appliance supports connections through IPSec with other sites or the SonicWALL Global VPN Client.

The client software needs to be installed on the client PC with a Windows operating system. After an initial configuration of the VPN gateway parameters, the policy is downloaded from the gateway when the connection is established.

The client supports preshared secrets or certificates for authentication.

© VODAFONE GROUP 2007

2.4 VPN Client System requirements

Verify that your computer meets the requirements documented by SonicWALL TZ 170 W documentation for “Sonicwall_GVC_3[1].1_Administrators_Guide.pdf” and “Sonicwall_GVC_3[1].1_Getting_Started_Guide.pdf”.

- IBM compatible computer with a Pentium (or equivalent) processor Microsoft Windows 95/98, ME, Windows NT 4.0 SP6, Windows 2000 Professional SP3, Windows XP operating system
- SonicWALL gateway version 6.4.2.0 or higher or SonicOS 1.0 Standard or 2.0 Enhanced or higher, configured for SonicWALL GroupVPN.

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, restricting access 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

SonicWALL TZ 170 W uses Internet Key Exchange Protocol (IKE) to set up a VPN tunnel. Standard IKE uses UDP/500 as destination port. In case NAT-Traversal protocol is used, UDP/500 is used.

The source port used can be any port number. Answers are sent back to the source port of the original message.

3.2 Data transfer connection

3.2.1 Standard connection

IPSec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. Both LAN-to-LAN connections and client-to-LAN connections can use IPSec. In IPSec terminology, a “peer” is a remote-access client or another secure gateway. During tunnel establishment under IPSec, the two peers negotiate Security Associations (SA) that governs authentication, encryption, encapsulation, key management, etc. These negotiations involve two phases: first, to establish the tunnel (the IKE SA, IKE: Port UDP/500); and second, to govern traffic within the tunnel (the IPSec SA).

In IPSec LAN-to-LAN connections, the VPN concentrator can function as initiator or responder. In IPSec client-to-LAN connections, the VPN concentrator functions only as responder. Initiators propose SAs; responders accept, reject, or make counter-proposals - all in accordance with configured SA parameters. To establish a connection, both entities must agree on the SAs.

The SonicWALL Global VPN client complies with the IPSec protocol and is specifically designed to work with the SonicWALL TZ 170 W appliance. Likewise, the SonicWALL TZ 170 W appliance can establish LAN-to-LAN connections with other IPSec protocol-compliant VPN devices (often called “secure gateways”).

3.2.2 NAT-Traversal

NAT-Traversal protocol enables a VPN client to operate in an environment in which standard Encapsulating Security Protocol (ESP, Protocol 50) cannot function, or can function only with modification to existing firewall rules. NAT-Traversal protocol encapsulates the ESP protocol within a UDP packet, and enables secure tunnelling through both NAT and PAT devices and firewalls. SonicWALL uses a proprietary protocol based on port UDP/500 for data transfer also.

© VODAFONE GROUP 2007

The TZ 170 W appliance can simultaneously support standard IPSec, IPSec with NAT-Traversal, depending on the client with which it is exchanging data. The use of NAT-T is automatically determined when the connection is negotiated between client and appliance.

3.3 Schematic diagram VPN connection

The following illustrates a high level diagram of the Implemented SonicWALL TZ 170 W VPN environment and building a connection from client to the concentrator (server).

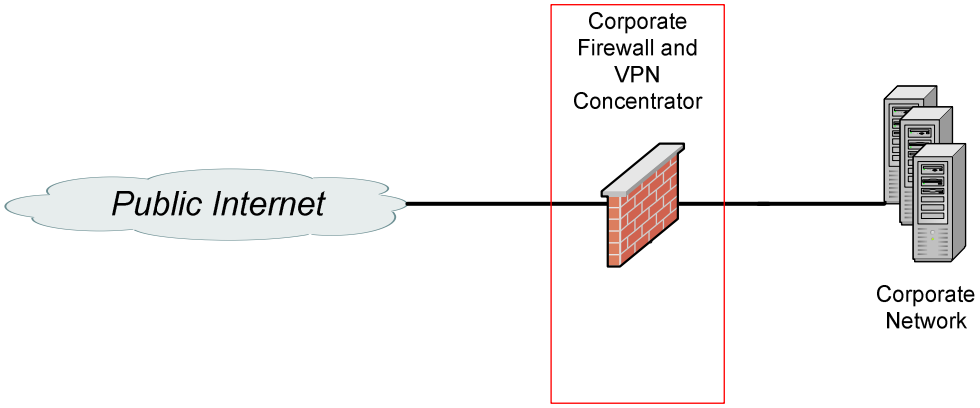


Table 1 – High-level SonicWall VPN Environment

The SonicWALL TZ 170 W VPN can be used as the corporate Firewall and VPN concentrator simultaneously.

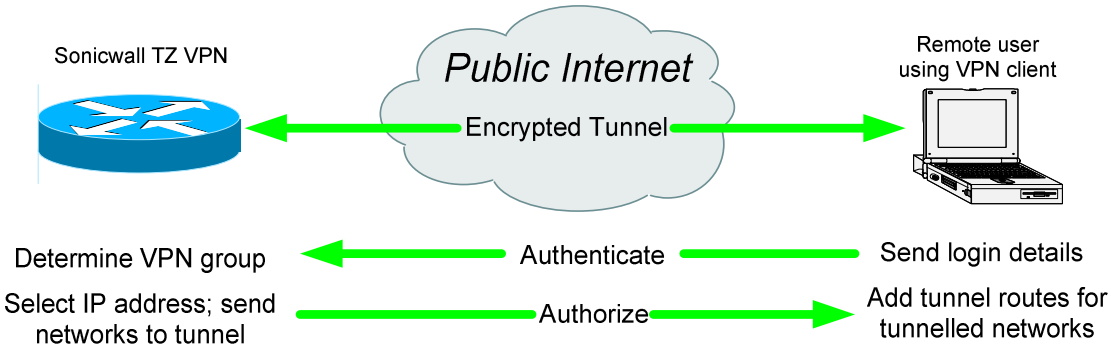


Table 2 – Logical Flow for Building Connection

3.4 Port summary for firewall setup

This chapter shows a port matrix for the different protocols used with the particular configurations.

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

Table 3 – Port Summary

3.5 IKE “keep alive” messages

3.5.1 Background

IKE “keep alive”, or “hello” packets, are a component of IPSec that tracks availability of peers by sending hello packets between peers. This feature lets the VPN concentrator monitor the continued presence of a remote peer and to report its own presence to that peer. If the peer becomes unresponsive, the VPN concentrator removes the connection. Enabling IKE keep alive prevents hung connections when the IKE peer looses connectivity.

During the typical life of the IKE Security Association (SA), as defined by the RFCs, packets are only exchanged over this SA when an IPSec quick mode (QM) negotiation is required at the expiration of the IPSec SAs. For this device, the default lifetime of an IKE SA is eight hours and that of an IPSec SA is one hours. Both VPN client and appliance support IKE Dead Peer Detection (DPD), which can be enabled on the appliance.

By implementing a “Dead Peer Detection” feature over the IKE SA in the SonicWALL TZ 170 W appliance, SonicWALL has provided network designers with a simple and non-intrusive mechanism for detecting loss of connectivity between two IPSec peers. Once three packets are missed, an IPSec termination point concludes that it has lost connectivity with its peer.

3.5.2 Configuration and Recommendation

Using the default interval of 10 seconds between IKE packets, an interruption of 30 seconds (3 missed packets) will be reported as a lost connection.

Recommendation:
An interval of 10 seconds will cause an unnecessary high traffic. The interval can be increased to 20 to 40 seconds without loss of functionality. In cases, where the connection is lost, this may cause a longer period until the dropped connection is detected. Since the connection can be reset manually, this poses no risk, if the interval is increased sensibly, e.g. doubled.

Please see the document “VPN - SonicWall_TZ_170W_Appendix_A_Concentrator.doc” for details.

© 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 concentrator monitor the continued presence of a remote peer and to report its own presence to that peer. If the peer becomes unresponsive, the VPN concentrator removes the connection. Enabling IKE keep alive prevents hung connections when the IKE peer loses connectivity.

By default, keep alive messages are sent every 10 seconds and have a size of about 43 bytes. In the tested software version, the interval did not change, in spite of the setup in the appliance.

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 110 bytes/packet. Sometimes there will be an additional overhead of some bytes to fill a packet to its optimal size.

As the default packet size is >1000 bytes, this overhead represents ~10% of traffic for applications that generate well-loaded packets. Highly interactive applications, such as messaging or Telnet, will have smaller packets and hence higher % overhead albeit with lower traffic volumes.

4.3 IP compression

Data compression is not supported by the SonicWALL TZ 170 Wireless.

© VODAFONE GROUP 2007

5 Support of Split Tunnelling

The client-server VPN connection supports split tunnelling. Split tunnelling is configured on the TZ 170 W appliance and is the default.

In some scenarios it makes sense to have some local traffic on the client network, or even traffic to the public internet, not passing the VPN tunnel and generating additional delay and overhead. On the other hand, Split Tunnelling opens a door for malware like Trojans to get access from the internet to the secured networks.

The client can therefore be configured to block all unencrypted traffic. If the policy is pre-configured, it is possible to inhibit the user to change this setting in the policy.

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

5.1 Configuration of Split Tunnelling

Split tunnelling is supported and will be negotiated in the connection phase by server push. Split tunnelling is enabled by default. The user cannot override the server settings.

Enabling or disabling split tunnelling can be configured in the GroupVPN properties. All users assigned to this group will use this setting and it is not possible to change the configuration from within the client.

If split tunnelling is disabled by choosing the “Allow Connections to This Gateway Only” option, the internet connection can be established using an internal proxy, or directly from the internal network through the firewall.

5.2 Recommendation

To use with Vodafone Mobile Connect Cards over the Vodafone 3G/HSDPA/GPRS infrastructure, advanced settings are required, which are specified as follows:

- Since we are doing IPSec over an address translation, we need to enable NAT-Traversal. This will encapsulate the standard IPSec into UDP packets. The configuration has to be done on the TZ 170 W appliance.

  For further help, please review the SonicWALL TZ 170 W documentation and refer to Appendix A: “VPN Concentrator Installation and Configuration” and Appendix B: “VPN - SonicWALL_TZ 170 W_5GT_Appendix_B_Client”.

- We further recommend disable split tunnelling by configuring the “GroupVPN > Client” entry “Allow Connections to” to “This Gateway Only”. Otherwise you open serious backdoors over your remote clients into your private LAN. Please refer to Appendix A: “VPN - SonicWALL_TZ 170 W_5GT_Appendix_A_Concentrator”.

© VODAFONE GROUP 2007

6 Additional Applications & Services

6.1 Client Firewall

There is no full personal firewall delivered with the client. The only possibility to secure the client against attacks from the internet is to configure the policy to block non-encrypted connections as described above. Since the client can be started with the PC, this may block all internet access.

A problem caused by this could be, that the user cannot log into public hotspots as long as the policy is active. It may be necessary to disable the connection until authentication to an ISP is done.

6.2 Value-added Services, Virus scanner support

The SonicWALL TZ 170 W appliance has a built in network and gateway anti virus scan engine which can scan certain protocols like http and mail. Content filtering and intrusion detection features are integrated. The use of these features needs additional licenses.

6.3 Timers

The SonicWALL TZ 170 W VPN appliance offers the possibility to configure several timers relevant for a GPRS or 3G connection. The following values are configurable:

Keep Alive Interval: If NAT-Traversal is selected, a regular telegram can be sent to keep the NAT table from being deleted. The default value is 10 seconds, but this will cause high traffic. A value between 30 and 60 seconds will always be sufficient. Unfortunately, in the tested software version, the interval did not change, in spite of the setup in the appliance.

See appendix A for the configuration.

IKE DPD: Dead Peer Detection, checks if the VPN connection is still operational. This is not needed when NAT-Traversal is used because of the Keepalive Telegram used there. Without NAT-T, this ensures that an inoperable VPN connection is detected after a maximum time which can be configured on the appliance.

See appendix A for the configuration.

6.4 Reporting, SNMP

SNMP traps and requests are supported and configurable. Logs can also be written to a standard Syslog server or email.

Report facilities are available on the appliance and on the client.

© 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
- Dashboard 7.00.0005

The tests were performed using Vodafone Germany's network running Byte Mobile optimisation and using the Macara client integrated into VMC software version 7.00.

© VODAFONE GROUP 2007

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.

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.

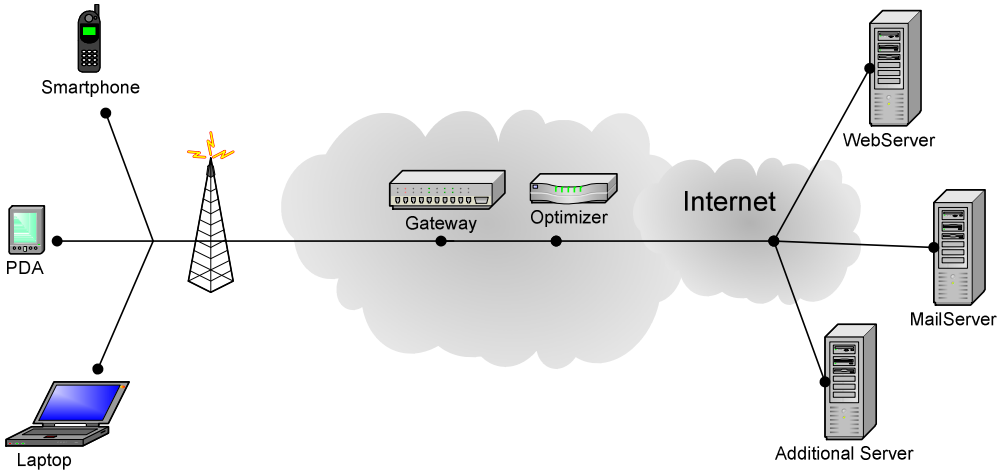


Table 4 – Schematic of Network Generic Optimisation in Mobile Network

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

© VODAFONE GROUP 2007

compress the data before encryption. For obvious reasons this can only be done by the VPN client itself.

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.

© VODAFONE GROUP 2007

7.2.3 Configuration Notes & Observations

When NAT or NAPT is used, the SonicWALL TZ 170 W VPN is using a proprietary 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 SonicWALL TZ 170 W VPN 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 4.3 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[6] 3G connection used		**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[3]**	n/a[1]	n/a[1]	229	3.18	n/a[1]	n/a[1]	232	3.17
300KB / 3072KB	**http-internet[4]**	n/a[1]	n/a[1]	181	3.13	n/a[1]	n/a[1]	n/a[2]	n/a[2]
300KB / 3072KB	**ftp-internet[5]**	n/a[1]	n/a[1]	314	3.13	n/a[1]	n/a[1]	n/a[2]	n/a[2]
300KB / 3072KB	**http-intranet**	n/a[1]	n/a[1]	315	3.12	n/a[1]	n/a[1]	317	3.13
300KB / 3072KB	**ftp-intranet**	n/a[1]	n/a[1]	312	3.14	n/a[1]	n/a[1]	311	3.13

1. SonicWALL does not support VPN compression, therefore nothing could be tested
2. Direct Internet access is not possible due to the 'No Split Tunnelling' configuration
3. Outlook 2003 and Exchange 2003 are using an internal compression
4. Internet access without VPN tunnel showing the influence of the Macara optimisation
5. Internet access without VPN tunnel. FTP is not optimised by Macara
6. 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

© VODAFONE GROUP 2007

7.4 Observations

The greatest impact is seen in web access (http-internet), which is the primary target of NGO compression.

Previously compressed file formats (MP3 in our example) are not compressed further. In fact, a slight increase in data transfer (<6%) is observed reflecting the overhead of encryption and encapsulation of a VPN solution.

For email usage, most of the compression benefit is provided by Outlook 2003 / Exchange 2003 (based on evaluation of similar products with integrated compression features).

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 NGO compression.

For common download applications using HTTP, the NGO provides a benefit by reducing data transfer volumes leading to better performance.

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

- Split-tunnelling is insecure and it was recommended NOT to implement this feature (Section 5.2**Error! Reference source not found.**).

© 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, the concentrator has to be configured to support it. See an example setup of NAT traversal in the appendix.

In a dynamic NAT/NAPT environment we recommend using the IPSec “keep alive” option in order to prevent an early timeout of NAT/NAPT table entries in the network and to get an early indication of lost VPN connections.

For an example configuration please refer to the appendix A and B.

© VODAFONE GROUP 2007

9 VPN Client Installation and Configuration

The SonicWALL TZ 170 W VPN client can be installed on a Windows Workstation. To install the software, a user needs administrator rights on the local computer. This client can be used to establish a VPN connection to the SonicWALL TZ 170 W firewall / VPN appliance. Other VPN clients must be uninstalled.

Run the installation program according to the directions given by the program. For further information, review the SonicWALL Global VPN client installation guide or Appendix B.

The VPN client can be integrated into the Vodafone Mobile Connect application (for more information refer to chapter **Error! Reference source not found.** “Hints & Tips”)

For further help please review the SonicWALL TZ 170 W documentation and refer to Appendix B: “VPN Client Installation and Configuration”

© VODAFONE GROUP 2007

10 Configuration & Connection Using VMC Software

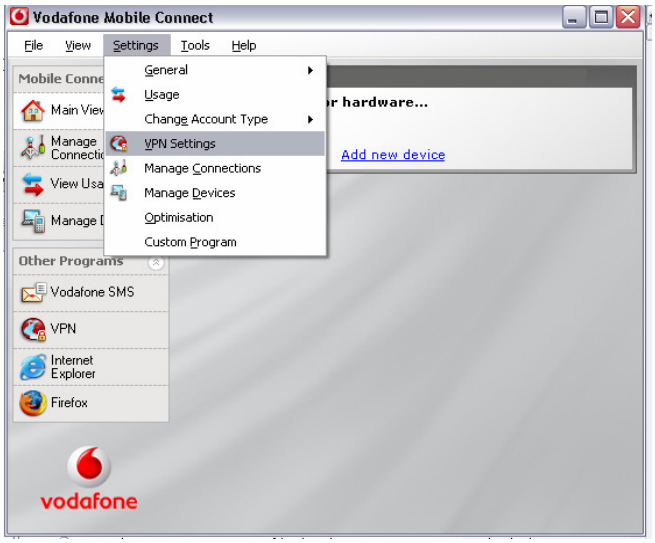
This chapter is used to describe possible configuration possibilities for using the VPN client in conjunction with the current released Vodafone Mobile Connect application.

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:

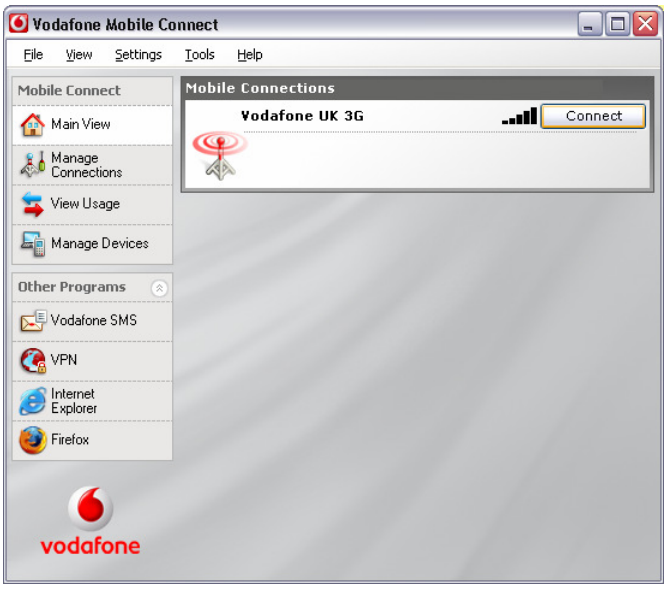
1. The '**Connect**' button is found in the 'Mobile Connections' window of the main screen.
2. The VPN button is found in the '**Other Programs**' section on the left side of the main view. If the Vodafone Mobile Connect software is not visible, it may need to be expanded from the mini view or from the 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)

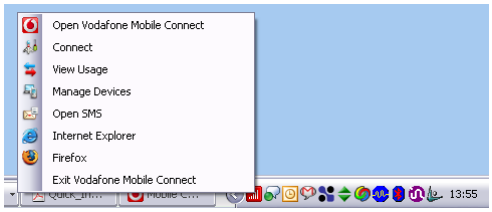
With a SIM card inserted into your datacard (or USB modem), to establish a connection:

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



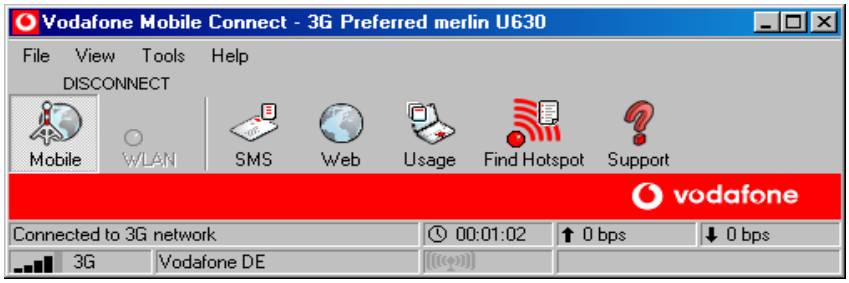
2. In the mini-view, use the **Connect** button, or

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:

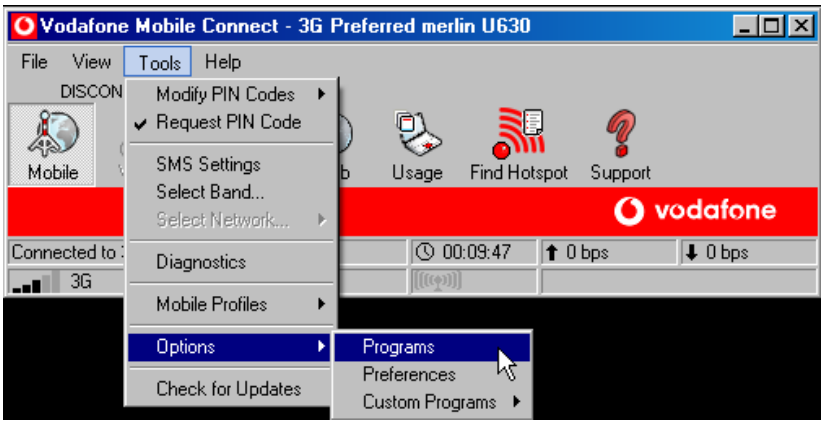


Press the **Mobile** button in the CONNECT/DISCONNECT area of the toolbar

10.3 Configure VMC for the VPN Client

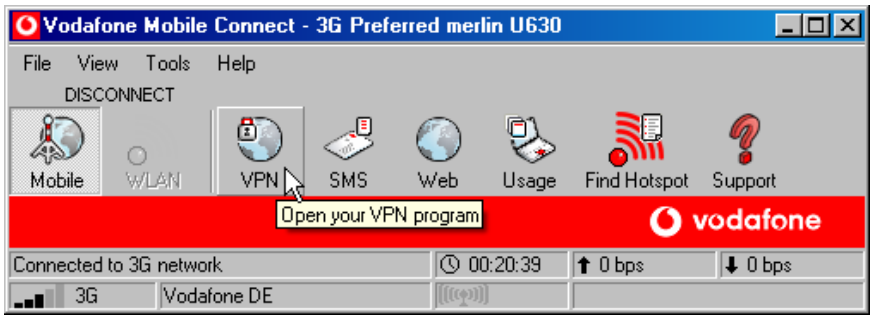
Note: The following steps apply to the legacy version of Vodafone Mobile Connect software R7 and earlier. See notes above on the process using the new R9 version.

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

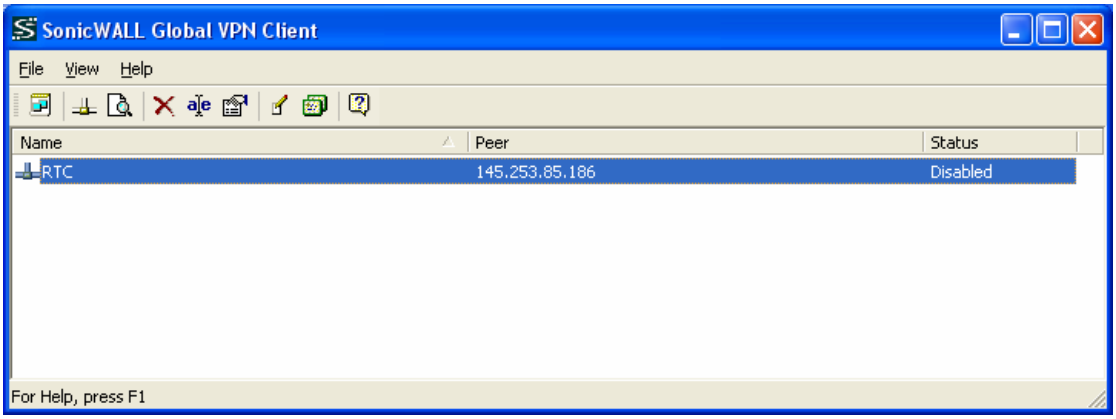


- Choose Tools | Mobile Profiles | Options | Programs
- Check the radio button “other” and select “Browse” to open your VPN client from the file system
- Select your SonicWALL Global VPN Client “SWGVpnClient.exe” and chose “Open”.
- Confirm your configuration with “OK”

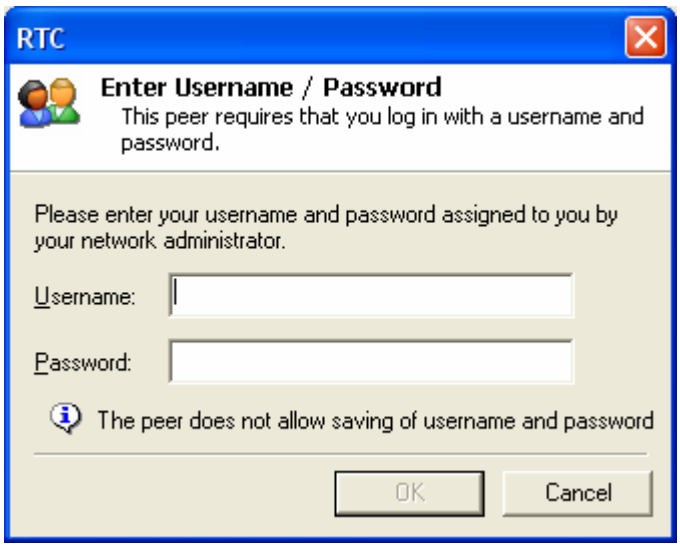
© VODAFONE GROUP 2007



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



- Click “Enable” in the main dialog and the client will open the connection to the concentrator, ask for user name and password and establish the IPSec session.



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 connections, or any other malfunction of the service provided by the VPN environment.

11.1 General

- Before starting to find a solution to a given problem, make sure you have all facts you can get from the corporate customer. What VPN-System is in use? Is the VPN-system configured for NAT/NAPT-Traversal? What type of encapsulation is configured? Is a network topology drawing available or at least try to obtain the internal IP address ranges.
- On the client side, check if the internet connection is functional. Depending on the VPN-client, access to the internet is disabled when the VPN-client is active. Therefore let the customer disable the VPN client and check if hosts in the internet are reachable at all.
    - If the dashboard is used, is the connection started at all? (Close and restart if necessary)
    - Did the client get an IP address from the provider (ipconfig)? Is the right APN in use?
    - If WLAN is used, did the WLAN card associate to an Access Point? Is the WLAN card set to the correct SSID? Depending on the operating system, the SSID has to be set up in the network (WinXP) or in the card-specific driver. Please note that in Windows XP there must be a check mark at “Allow me to connect to the wireless network even though it is not secure“, if the WLAN network is not encrypted.This is the case with most WISPs. If the Vodafone Dashboard 3.0 or higher is used and is WLAN-enabled, it takes over control over the card setup and it may not be possible to use the WinXP controls.
    - When using WLAN in a public hotspot, the customer has to authenticate via web browser before a connection to the internet is established. Did the customer authenticate successfully? Sometimes popup-blocker inhibits the correct functionality.
    - When you check the internet connectivity by using the web browser, make sure that there is no proxy server set up in the internet options.
    - Try to open the URL http://www.cisco.com in the web browser or just “ping www.cisco.com” or “ping 198.133.219.25”.

© VODAFONE GROUP 2007

- Was the customer able to use the VPN-connection at least once before on the same computer?

11.2 Logging Concentrator (server side)

Event logging is available via the web interface, path “Log > View”. This screen shows the events in the current log file.

The details to be logged can be adapted in the “Log > Categories” screen.

For further information please refer to the SonicWALL TZ 170 W appliance documentation.

11.3 Logging Client (client side)

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

“View > Log Viewer”. The log can be cleared, filtered and saved to a file. The log display can be stopped and restarted.

For more information please refer to the TZ 170 W Remote client’s documentation.

**** End of Document ****

© VODAFONE GROUP 2007