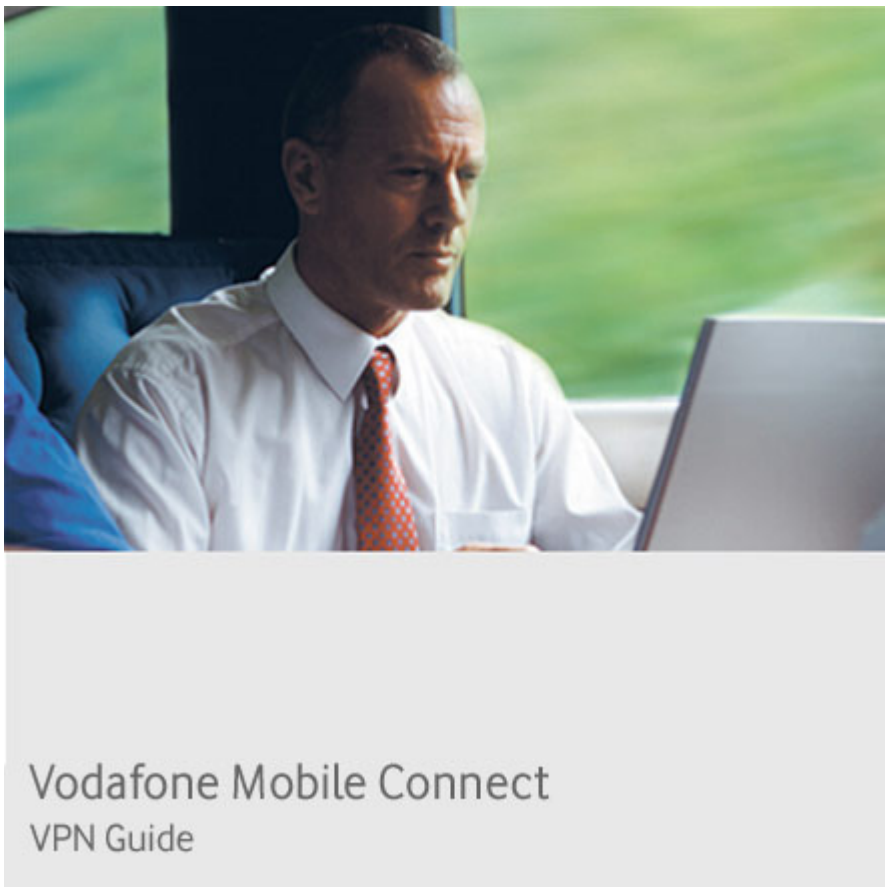
VPN End to End – Cisco PIX 501

Technical Notes for use with Vodafone Mobile Connect services

Date: **03 May 2007**

Revision No: **3.0**



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 changes
3.0	May 2007	Editorial changes + R9 Impact

File Reference

VPN - Cisco PIX501_v3.0.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

Contents

Tables & Figures

1 Executive Summary

This document provides an explanation of how to use a Cisco PIX VPN solution with Vodafone 3G and related services. Furthermore, this document describes how to diagnose problems and performance issues with the Cisco PIX VPN over Vodafone 3G and related services. A general overview of the Cisco PIX installation, update and configuration for both the concentrator 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 Cisco PIX VPN solution.

A single client software is provided by Cisco for all its VPN solutions. This software must be the only VPN software installed on the client laptop (and so will disable the native Microsoft Windows IPSec subsystem when installed to avoid conflicts).

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 <5% (60 bytes/packet, MTU size = 1380 bytes) 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 has a role for lower-speed connections
- 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.

2 Introduction

This chapter describes the Cisco PIX 501environment and prerequisites for use.

2.1 Test environment

The tests are based on a Cisco PIX 501 with software version 6.3 (5) with PDM version 3.0 (4).

As client software, version vpnclient-win-is-4.8.00.0440-k9 was used. This was installed on an IBM T20 notebook running Windows XP Professional with SP2.

2.2 Cisco PIX outline

The Cisco PIX is a widely used firewall platform with stateful packet inspection, VPN abilities for remote access and site-to-site VPNs. Higher level packet inspection is available depending on the firewall model.

Cisco offers the PIX as either an appliance or as plug-in cards for the Cisco Catalyst switches.

The PIX operating system is a purpose-built embedded operating system. The PIX 501 supports Version 6.1 and higher.

The configuration can be done via the web-based PIX Device Manager (PDM). A start up wizard supports the first-time configuration. Alternatively, a text-based interface (similar to Cisco IOS) is available.

2.3 Cisco VPN handling

The PIX supports connections through PPTP, L2TP, IPSec and tunnelled IPSec with either the Cisco Client (recommended) or other standard based IPSec Clients.

As an appliance the PIX is shipped ready-to-use: The PIX can assign an IP address to the configuration PC and all further configurations are done over a web browser (see Appendix).

The PIX supports local user data base and user verification via RADIUS or TACACS+. This allows using Token systems like RSA SecureID or other RADIUS-based authentication systems.

The Client software needs to be installed on the Client PC, MAC or Solaris system and needs some basic information to establish a connection to the PIX: VPN group name and password, target IP address and the form of IPSec encapsulation/tunnelling, if needed (e.g. NAT-Traversal), finally the user's name and password.

The user can define a “start before logon” option to deal with Windows Active Directory domain logon or roaming profiles.

2.4 VPN Client System requirements

Verify that your computer meets the requirements documented by Cisco documentation for “vpnclient-win-is-4.8.00.0440-k9”.

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.

3 Which Protocols are supported?

3.1 Control connection

Cisco uses Internet Key Exchange Protocol (IKE) to set up a VPN tunnel. Standard IKE uses UDP/500 as destination port, but this can be configured to support TCP also. 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

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 Cisco VPN Client complies with the IPSec protocol and is specifically designed to work with the VPN Concentrator. However, the VPN Concentrator can establish IPSec connections with many protocol-compliant Clients. Likewise, the VPN Concentrator can establish LAN-to-LAN connections with other 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) or Internet Key Exchange (IKE, UDP 500) cannot function, or can function only with modification to existing firewall rules. NAT-Traversal protocol encapsulates both the IKE and IPSec protocols within a UDP packet (Port 4500), and enables secure tunnelling through both NAT and PAT devices and firewalls.

The Cisco PIX 501 appliance can simultaneously support standard IPSec and 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 Cisco VPN environment and building a connection from Client to the concentrator (server).

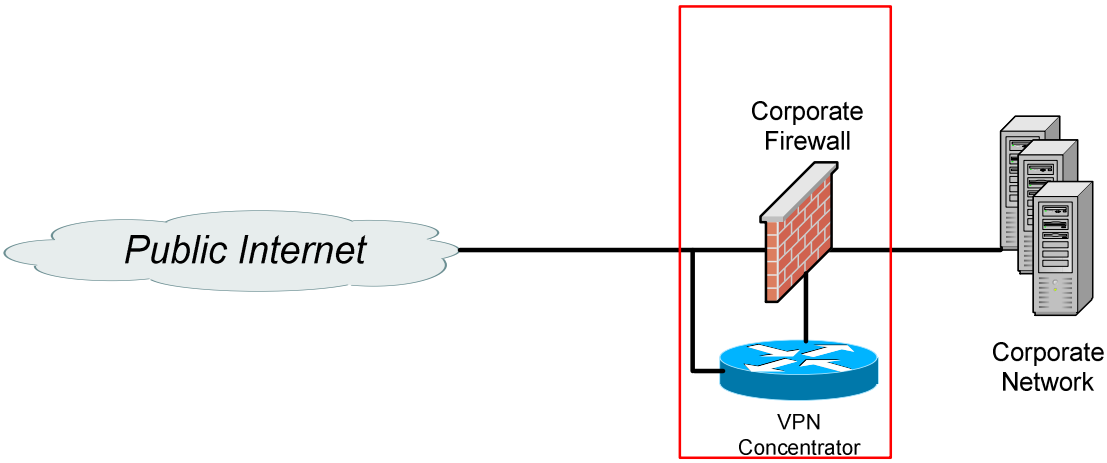


Table 1 – High Level Cisco PIX 501 environment

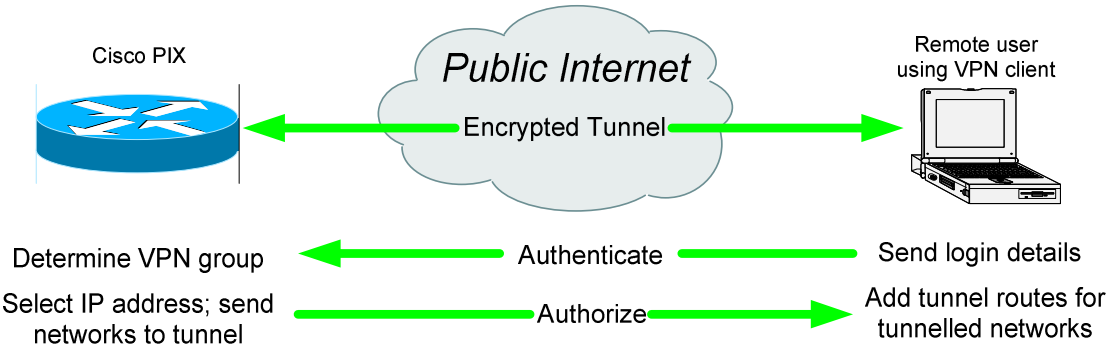


Table 2 – Logical Flow for Building Connection

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	
IPSec ESP	IP	50	50	Client → Server	
Encapsulated IPSec (for NAT-T)					
IPSec NAT-T	UDP	Arbitrary > 1024	4500	Client → Server	

Table 3 – Port Summary

3.5 IKE “keep alive” messages

IKE “keep-alive”, or “hello” packets, are a component of IPSec that tracks accessibility 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 24 hours and that of an IPSec SA is eight hours. There is no standards-based mechanism for either type of SA to detect the loss of a peer, except when the QM negotiation fails.

By implementing a “keep-alive” feature over the IKE SA in Cisco software, Cisco 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.

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: Increase the default interval from 10 to 15-30 seconds.

An interval of 10 seconds will cause unnecessarily high traffic. The interval can be increased to 15 to 30 seconds without loss of functionality. Users who use the VPN frequently from poor transmission areas may suffer frequent loss of VPN-connection. A longer interval for the detection of missing IKE “Dead Peer Detection” packets can be used to reduce the frequency of dropped connections. If the connection is lost permanently, 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.

4 VPN Performance

This chapter decribes 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 200 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 around 60 bytes/packet.

To avoid fragmentation, the default setup of the Cisco PIX reduces the maximum transfer unit (MTU) to 1380 Bytes per packet. The IPSec overhead is thus <5% for most applications generating well-filled packets.

4.3 IP compression

IP compression is not available in the current release.

5 Support of Split Tunnelling

The Client-server VPN connection does support split tunnelling and it is disabled by 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. Therefore the profile configuration of groups let you setup the tunnelling mode policy that will be pushed to the Client when connecting.

We recommend **not** using split tunnelling for security reasons, but document the configuration settings here for completeness.

5.1 Configuration of Split Tunnelling

Split tunnelling is supported and will be negotiated in the connection phase by server push. Split tunnelling is disabled by default. The user cannot override the server settings, but access to the internet is possible as long as the VPN connection is not enabled.

Enabling or disabling split tunnelling can be configured in the Group 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 enabled by choosing “Only tunnel networks in the list” a network list has to be created in the Policy Management / Traffic Management menu.

If split tunnelling is disabled by choosing the “Tunnel everything” option, a direct connection to the internet is not possible as long as the VPN connection is established. The connection to web pages can then be established using the corporate proxy server, or directly via the corporate network through the corporate firewall, if the routing is set up accordingly. The client can be used to modify the Internet Explorer proxy settings automatically when a VPN tunnel is established.

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 IPSec over UDP. Enter this in the main configuration in the base group, or the appropriate group for your users. Please check “IPSec over UDP” and enter a port number within the given range, for example 10000.

  For further help, please review the Cisco documentation and refer to Appendix A: “VPN Concentrator Installation and Configuration”

- We further recommend selecting the “Tunnel everything” split tunnelling option. Otherwise you open serious backdoors over your remote clients into your private LAN.

As an alternative, you can use the IETF draft NAT-T implementation. To enable this option go to the menu Configuration | Tunnelling and Security | IPSec | NAT Transparency screen and enable **IPSec over NAT-T.**

6 Additional Applications & Services

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

6.1 Client Firewall

Local Firewall is shipped with the Cisco VPN Client. The VPN Client configuration option "Stateful Firewall (Always on)" is disabled by default on the VPN Client. The VPN Client user enables this option on the VPN Client under the options menu. The policy is not controlled by the VPN Concentrator, but the concentrator can be configured to require an enabled personal firewall.

When enabled, this feature prohibits inbound sessions from all networks, whether or not a VPN connection is in effect. Also, the Firewall is active for both tunnelled and non-tunnelled traffic. There are two exceptions to allowing no inbound traffic:

1. The first is DHCP, which sends requests to the DHCP server out one port but receives responses from DHCP through a different port. For DHCP, the stateful Firewall allows inbound traffic.
2. The second is ESP (VPN data). The stateful Firewall allows ESP traffic from the secure gateway, because ESP rules are packet filters and not session-based filters.

6.2 Virus scanner support

No virus scanner service is available on the Cisco VPN Concentrator. A 3rd party virus scanner service should be used.

6.3 Timers

Cisco PIX offers the possibility to configure the idle timeout and the Maximum Connect Time (Configuration>VPN>Remote Access>Cisco VPN Client, Select Group and click "Edit").

Idle Timeout: If there is no communication activity on a user connection in this period, the system terminates the connection. The default value is 180 seconds.

Maximum Connect Time: After this period, the system terminates the connection automatically. The default value is never (No value in the field).

6.4 SNMP

SNMP requests and traps are supported and configurable
(System Properties>Administration>SNMP Server).
The SNMP management station list shows the SNMP network management systems that have been configured as destination for SNMP requests and / or event trap messages, and the PIX interface associated with each destination.

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 appropriate client applications for Flash Networks and for ByteMobile Macara are integrated with the 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 testing:

- IBM T20 Notebook running Windows XP Professional SP2
- DELL Inspirion 8600 Notebook, XP Professional SP 2
- Microsoft Outlook 2003 SP1
- 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 version 6.01.0001

The tests were performed using Vodafone Germany's network running Byte Mobile optimisation and using the Macara client integrated into VMC software version 6.01.

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.

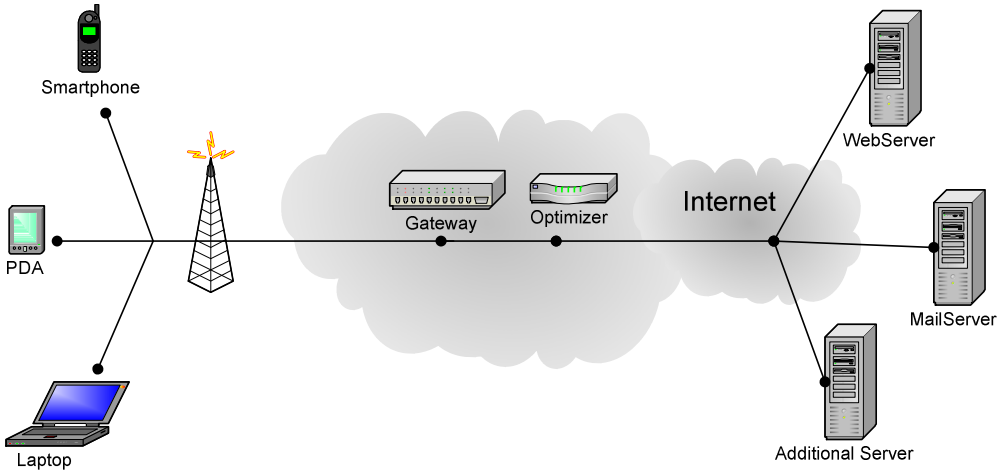


Table 4 – Schematic of Network Generic Optimisation in Mobile Network

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 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, if applicable:

- 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, the Cisco PIX is can only use UDP-encapsulation. Since the NGO is operating as a TCP proxy server, UDP packets pass unchanged without interaction. Therefore there is no issue when using a Cisco Client with a Cisco PIX firewall.

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.

Used reference files: Word Document = 300 KB; MP3 File = 3072 KB = 3MB[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	3.17	n/a[1]	n/a[1]	229	3.16
300KB / 3072KB	**http-internet**[4]	n/a[1]	n/a[1]	159	3.25	n/a[1]	n/a[1]	n/a[2]	n/a[2]
300KB / 3072KB	**ftp-internet**[5]	n/a[1]	n/a[1]	298	3.27	n/a[1]	n/a[1]	n/a[2]	n/a[2]
300KB / 3072KB	**http-intranet**	n/a[1]	n/a[1]	291	3.22	n/a[1]	n/a[1]	283	3.29
300KB / 3072KB	**ftp-intranet**	n/a[1]	n/a[1]	285	3.13	n/a[1]	n/a[1]	314	3.22

1. The Cisco PIX 501 does not support compression
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

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 (<10%) 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.

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).

8 Special Settings for 3G/HSDPA/GPRS

The main settings to be considered for VPN over a mobile network relate to address translation schemes.

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 allocating temporary IP addresses using 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. See an example setup of NAT traversal in the appendix.

We recommend avoiding NAT traversal methods involving TCP encapsulation to avoid possible interference with TCP optimisers like ByteMobile Macara or Flash Networks. Use either IPSec over UDP encapsulation or the NAT-T draft implementation (also UDP based).

We further recommend using the IPSec “keep alive” option in a dynamic NAT/NAPT environment 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 (server / concentrator) and B (client).

9 VPN Client Installation and Configuration (Cisco VPN Client 4.8.00.0440)

The Cisco VPN Client can be installed on a Windows 2000 or Windows XP Workstation. To install the Software a user need Administrator rights on the local machine. This client can be used to establish a VPN connection to the Cisco PIX, the Cisco VPN Concentrator or the Cisco PIX 501. Other VPN Clients have to be uninstalled prior to installing the Cisco client.

Run the installation program according to the directions given by the program and for further information review the Cisco client installation guide. Keep in mind that the integrated IPSec Subsystem of Windows 2000 and XP will be disabled by the CISCO VPN Client.

During the setup a Deterministic Network Enhancer will be installed on all available network adapters. Additionally Cisco VPN Client 4.0 creates a new network adapter.

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 Cisco documentation and refer to Appendix B: “VPN Client – chapters Installation and Configuration”

10 Configuration & Connection Using VMC Software

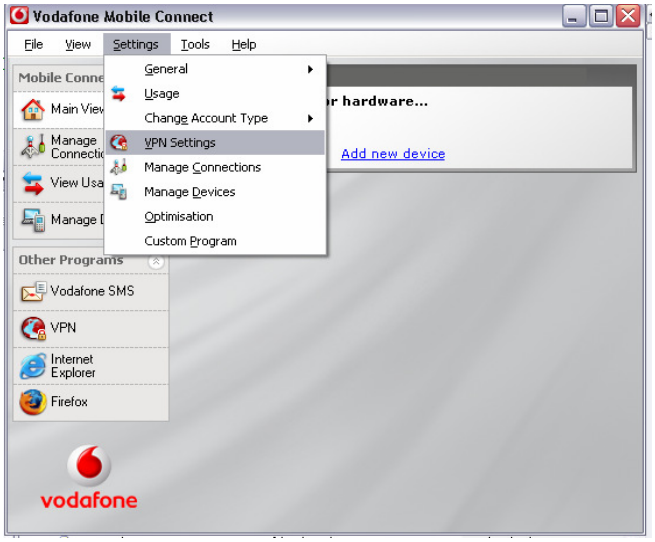
This chapter is used to describe possible configuration possibilities for using the VPN client in conjunction with the current released Vodafone Mobile Connect application. Furthermore we recognised a display issue within the VPN client which is reported (Section 10.5).

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:

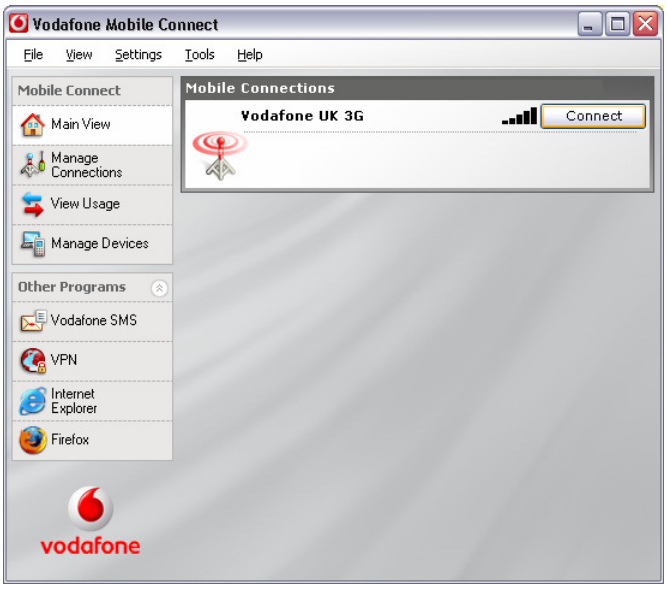
1. The '**Connect**' button is found in the 'Mobile Connections' window of the main screen.
2. The VPN button is found in the '**Other Programs**' section on the left side of the main view. If the Vodafone Mobile Connect software is not visible, it may need to be expanded from the mini view or from the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

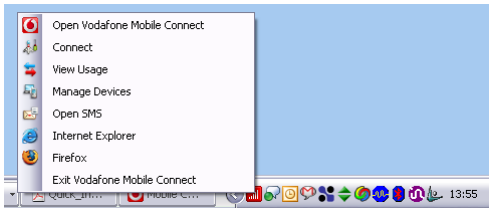
With a SIM card inserted into your datacard (or USB modem), to establish a connection:

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



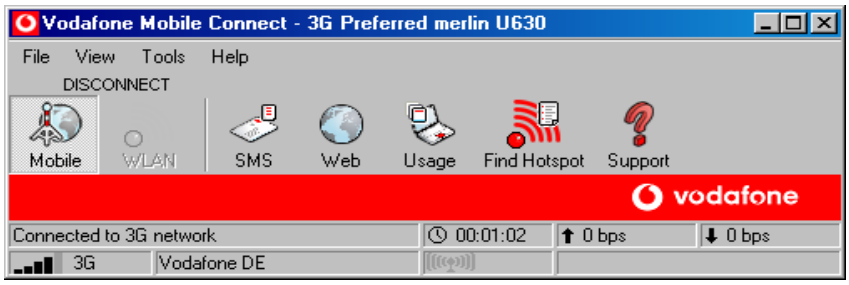
2. In the mini-view, use the **Connect** button, or

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:

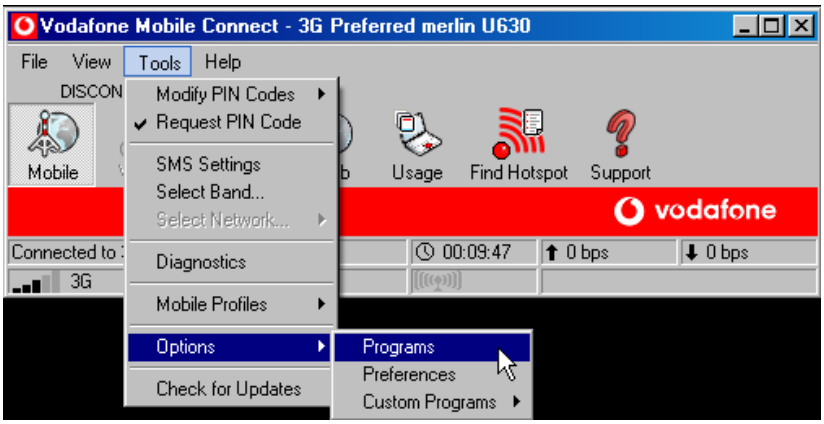


Press the **Mobile** button in the CONNECT/DISCONNECT area of the toolbar

10.3 Configure VMC for the VPN Client

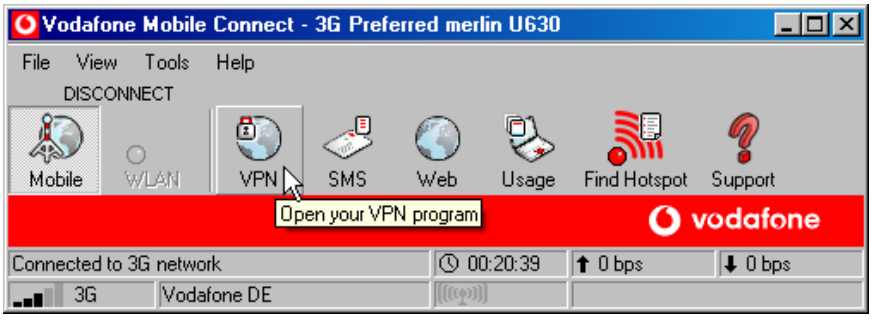
Note: The following steps apply to the legacy version of Vodafone Mobile Connect software R7 and earlier. See notes above on the process using the new R9 version.

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

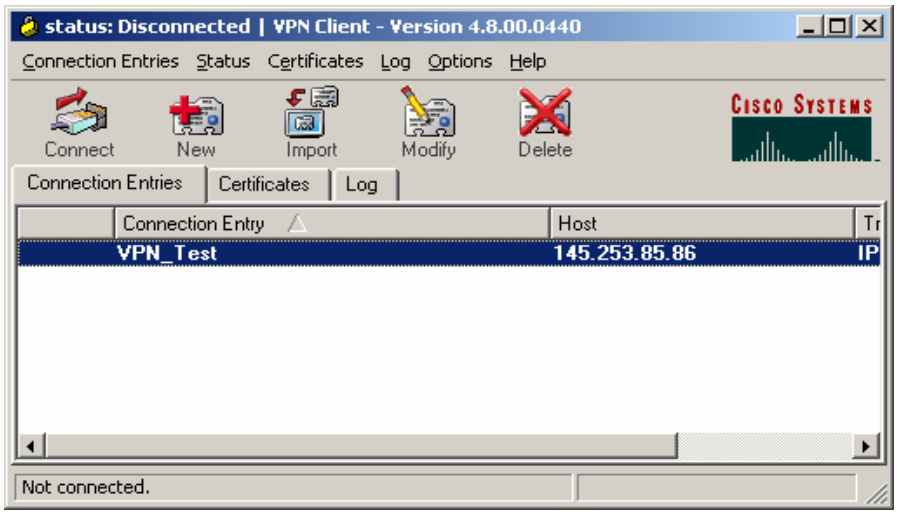


- Choose Tools | Mobile Profiles | Options | Programs
- Check the radio button “other” and select “Browse” to open your VPN client from the file system

- Select your Cisco VPN client here “vpngui.exe” and chose “Open”.
- Confirm your configuration with “OK”



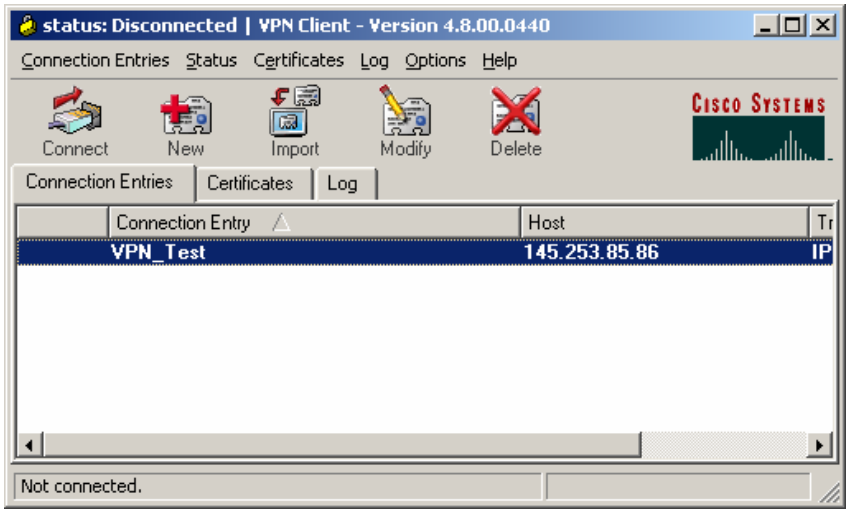
- Click the “Mobile” button on the main Dashboard screen.
  After you build up your preferred connection, click the “VPN” button to open your configured VPN Client



- Click “Connect” 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.

10.4 VPN Client Starting and Connection Option

By default, the Cisco VPN client has to be started manually. It is possible to change the starting option e.g. from the Run-Key of the Registry. Also the connection to the concentrator, by default, must be made manually by pressing the “Connect” button in the VPN client.



The connection establishment can be changed to connect automatically. The Cisco VPN client supports Auto-Initiation. To configure this, the vpnclient.ini file, located in the folder “C:\Program Files\Cisco Systems\VPN Client”, has to be modified. By using Auto-Initiation, auto reconnect is available with the option AutoInitiationRetryInterval.

Example taken from the Cisco documentation:

```
[Main]
ConnectOnOpen=1
AutoInitiationEnable=1
AutoInitiationRetryInterval=3
AutoInitiationList=RTC_VPN

[RTC_VPN]
Network=192.168.2.0
Mask=255.255.255.0
ConnectionEntry=RTC_VPN (points to a connection profile named RTC_VPN.pcf)
```

10.5 Display issue within the VPN client

During our tests we noticed that on the “Tunnel Details” tab within the statistics view, the “Local LAN:” setting is not displayed correctly. Regardless of the configuration of the client and its settings, there is no way to get the “Local LAN” field to update. This affects the Cisco VPN client version 4.6 as well. General functionality is not impaired, since this is only display behaviour on the Local LAN field used for the Statistics view.

This field is described as follows in the Cisco Help/feature description as follows:

Cisco client help / feature description:
Local LAN Access--Whether access to your local area network while the tunnel is active is enabled or disabled.

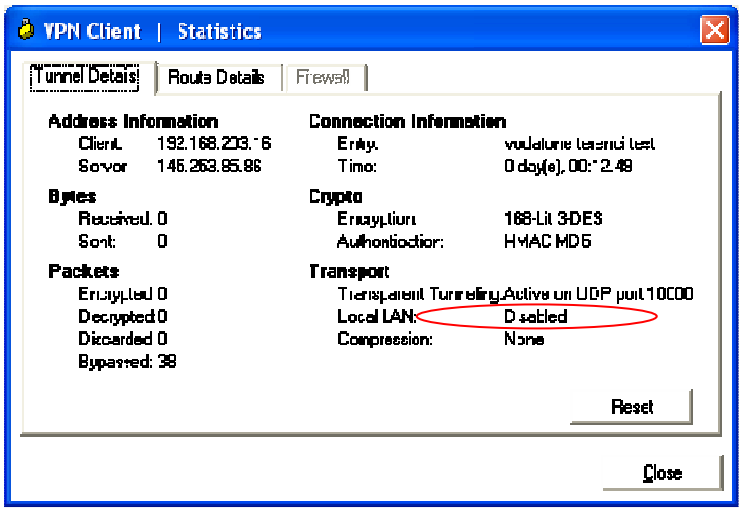


Table 6 – VPN Client Display for Local LAN settings

Furthermore the “Route Details” tab is not showing entries for the “Local LAN Routes”. This field is left empty, even the connected networks are not shown within this field.

This field is described as follows in the Cisco Help/feature description as follows:

Cisco client help / feature description:
Local LAN Routes
The Local LAN Routes box shows the network addresses of the networks you can access on your local LAN while you are connected to your organization's private network through an IPSec tunnel. You can access up to 10 networks on the client side of the connection. A network administrator at the central site must configure the networks you can access from the client side. For information on configuring Local LAN Access on the VPN 3000 Concentrator, refer to VPN Client Administrator Guide, Chapter
Network--The IP address of the excluded route.

Subnet Mask--The subnet mask of the IP address for this route.
Secured Routes

The Secured Routes box shows the following information:
Network-The IP address of the remote private network with which this VPN Client has a security association (SA).
Subnet Mask--The subnet mask of the IP address for this SA

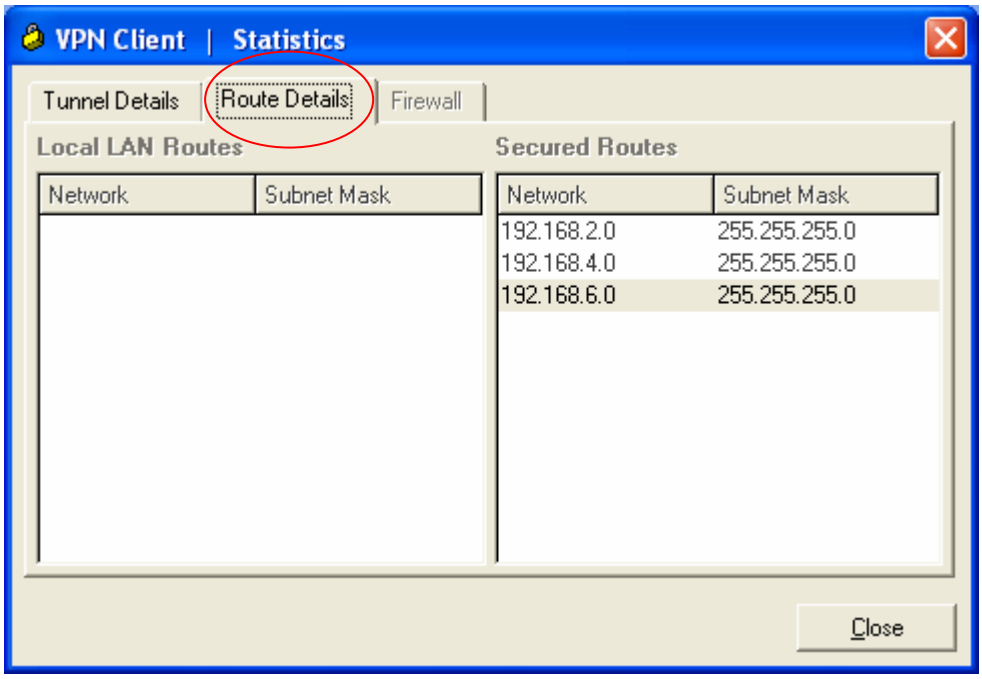


Table 7 – Route Details tab of VPN Client

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. Note that with Vodafone Mobile Connect software versions 3-7 with WLAN enabled, the WLAN features may be restricted to Vodafone-supported hotspots and other utilities must be used to control / configure the WLAN connection.
    - When using WLAN in a public hotspot, the customer has to authenticate via web browser (by browsing to a public IP address) before a connection to the internet is established. Did the customer authenticate successfully? Sometimes popup-blocker inhibits the correct functionality. *Hint: Just starting your email client will not initiate the authentication; use the web browser and attempt to reach a public address such as your favourite news site or www.cisco.com.*
    - 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”.

- Was the customer able to use the VPN-connection at least once before on the same computer? If so, possible changes to the client configuration (new firewall? Changes to internet connection preferences?) should be investigated.

11.2 Known Problems

- The connection to the internet works. Web servers in the internet are reachable. (E.g. Ping 198.133.219.25) A VPN connection does not work.

  Check: Double-click the Cisco-VPN-icon in the system tray, click the connection in question and select “Modify”. Select the register tab “Transport”. Is there a check mark at “Enable Transparent Tunnelling”?

  Reason: Pure IPSec VPN does not work over many networks, especially GPRS networks. The client has to use encapsulated IPSec, which Cisco calls “Transparent Tunnelling”.

  Solution: Set check mark.

- The IPSec connection does not work although the internet connection is OK. The transport tab in the Cisco client setup shows “IPSec over TCP” is selected. The customer uses an APN with optimiser support.

  Reason: The Cisco PIX does not support TCP encapsulation.

- The intranet web server just shows blank web pages after a timeout when accessed via the VPN. The customer may use a Cisco VPN client Version prior to 3.6.3.

  Reason: Data packets above 1400 Bytes need to be fragmented due to the additional VPN overhead. Cisco VPN-clients prior to 3.6.3 cannot set the fragmentation on WinXP correctly, since the wrong registry key is set.

  Alternative Reason: If the respective network card was installed after the VPN client was installed, the MTU value is not automatically corrected for this interface.

  Solution: In case of an old VPN client version, the customer’s system administrator should install a newer version of the Cisco client, e.g. Version 4.0. The clients are compatible to the older versions; there should be no changes necessary on the concentrator. It is also possible to correct the MTU value manually, e.g. using the setMTU tool supplied with newer versions (!) of the client. If a newer client is in use, set the MTU size of all network interfaces to 1300 Byte using the setMTU tool installed in the Cisco program group.

- The intranet web server just shows blank web pages after a timeout when accessed via the VPN.
  Mailing using Outlook/Exchange is not possible, although ping into the customer’s

intranet works fine. The Cisco-VPN-Client-version is 3.x or older.
The connection uses an optimised APN, e.g. Web-APN.

Reason: If “split tunnelling” is activated for the VPN and the optimiser in the dashboard is active (Menu Tools > Options > Applications > Compression), then the optimiser tries to optimise web and mail traffic. Cisco client version 3.x does not implement a virtual network interface, so that the optimiser may install over the VPN. Web data packets will be optimised first and then send to encryption. The encrypted packets pass the network generic optimiser since they are encrypted. When decrypted in the intranet, the packets are not usable by the web server.

Solution: Switch off compression in the dashboard (Menu Tools > Options > Applications > Compression) or deactivate an external optimiser.

11.3 Logging Concentrator (server side)

Event logging is available on the Monitoring / Filterable Event Logs screen. This screen shows the events in the current log file, lets you filter and display events by various criteria, and lets you manage the event log file.

The Log can be searched, printed, or exported to a file.

For further information please refer to the Cisco concentrator documentation.

11.4 Logging Client (client side)

On the client side, logging is also possible for at least the following components:

- IKE
- Connection Manager
- Daemon (cvpnd)
- User authentication
- Certificates
- IPSec
- Command Line
- GUI
- PPP
- Firewall

For all logs, the following Log Levels are available:

- Disabled - Inhibits event reporting for the chosen class.

- Low - Provides the least amount of information.
- Medium - Includes severity levels 1 through 4
- High - Includes severity levels 1 through 6

The log file may be searched, printed, and exported to a file.

For more information please refer to the VPN client's documentation.

*** End of Document ***