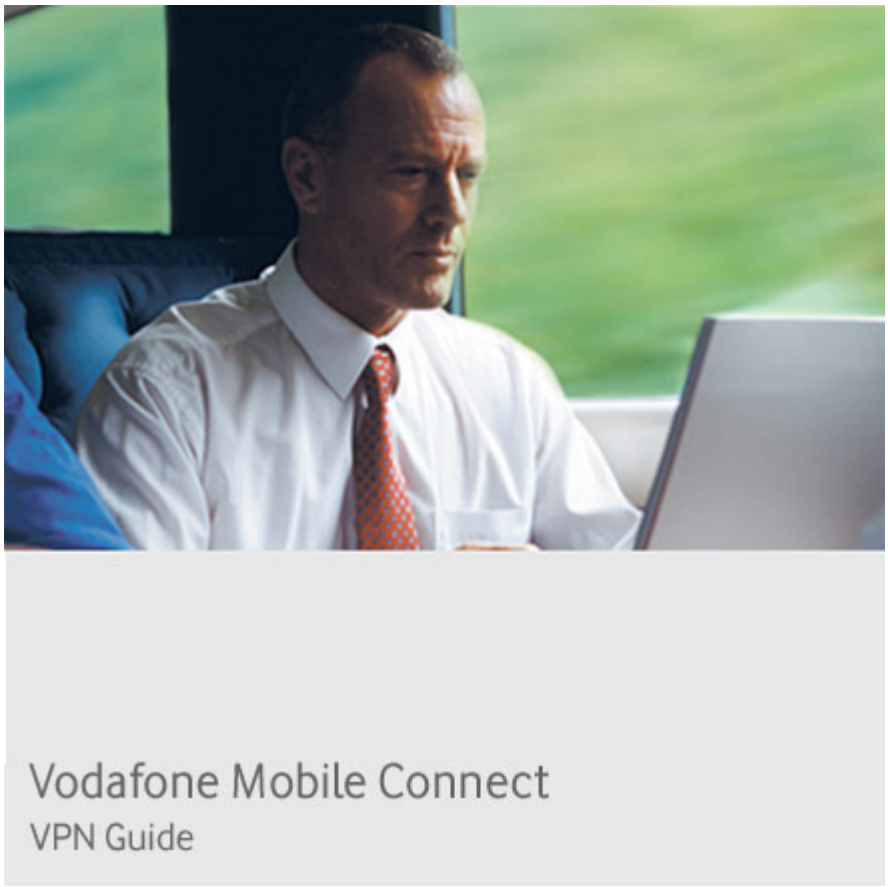
VPN End to End – Checkpoint FW-1/ VPN-1 NGX VPN

Technical Notes for use with Vodafone Mobile Connect services

Date: **30 May 2007**
Revision No: **3.1**



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	June 2006	Update to new versions of VPN software and focus on 3G network performance.
2.1	June 2006	Minor corrections
2.2	November 2006	Redraft of NGO chapter 7; minor edits
3.0	December 2006	Issued on website
3.1	May 2007	Updated for R9; Issued on website

File Reference

VPN_Checkpoint_NGX_v2.2

Document Authors

Marcus Hasenbeck, TECON Terenci
Peter Jaeger, TECON Terenci
Miroslaw Grzesica, TECON Terenci
Stefan Wozny, 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 Checkpoint FW-1/VPN-1 NGX VPN solution with Vodafone 3G and related services. Furthermore, this document describes how to diagnose problems and performance issues with the Checkpoint FW-1/VPN-1 NGX VPN over Vodafone 3G and related services. A general overview of the CHECKPOINT NGX installation, update and configuration for both the 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 Checkpoint FW-1/VPN-1 NGX 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% (60 bytes/packet) for applications with well-filled packets (>1000 bytes/packet). This overhead is one of the lowest of the products tested.
- IKE keep-alive packet intervals 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
- 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.

2 Introduction

This chapter describes the Checkpoint FW-1/VPN-1 NGX environment and prerequisites for use.

2.1 Test environment

The tests are based on a Nokia IP350 appliance with Checkpoint NGX R61 software in connection with the Checkpoint NGX Management Center.

As client software, version NGX R60 was used. At the time of writing, no R61 client was available.

This was installed on an IBM T20 notebook running Windows XP Professional SP2, a Gericom XEBGINE XL with Windows XP Professional SP2 and a DELL Inspiron 8600 Notebook with XP Professional SP2.

2.2 Checkpoint NGX outline

Checkpoint NGX is firewall and VPN software made by Checkpoint. Together with Cisco PIX, FW-1/VPN-1 is the most common security software within the Vodafone footprint.

It is available for several platforms, e.g.:

- Sun Solaris
- Microsoft Windows (WIN32 Platform)
- LINUX (“SecurePlatform”)
- Nokia IPSO

The Firewall system is divided into 3 main modules. The firewalling and VPN support is handled on the enforcement point, which is a gateway or routing device. This enforcement point obtains a compiled policy from a management system, which can support one to several enforcement points. Policy and object information is stored on the management and generation of the compiled policies is done on this module. The user interface is handled by a GUI-client called SmartConsole. The GUI-client can be installed on a different machine than the management and handle the configuration tasks via a secure connection.

Apart from firewalling and basic VPN functionality, Checkpoint FW-1/VPN-1 supports scanning of higher networking protocols up to the application layer. Virus- and content-scanners can be integrated in the data flow. (OPSEC-protocol)

2.3 Checkpoint NGX VPN handling

The appliance supports IPSec based site to site VPNs as well as client based VPN connections.

Checkpoint supports two Checkpoint VPN clients. SecuRemote is licensed free of charge if you licensed VPN-1. Unfortunately, there is no personal firewall policy possible and the client cannot use a virtual network interface. SecureClient does contain a personal firewall which can be configured in detail similar to the standard enforcement points via GUI-client and management server. The software features a virtual network interface. Unfortunately, this client needs to be licensed separately.

Additionally, Windows L2TP VPN clients are supported.

The Checkpoint NGX VPN clients support IPSec encryption. The information about the networks to encrypt has to be obtained via a “Topology-Download” in the initialisation and configuration of the client software. If the SecureClient is used, additionally, a Security Policy is downloaded when the user authenticates.

2.4 VPN Client System requirements

Verify that your computer meets the requirements documented by Checkpoint. At the time being, the client is supported on Microsoft Windows (Windows 2000/XP/2003 and Pocket PC 2003 2nd Edition and Handheld PC 2000). Further, Versions for Macintosh and LINUX are available also.

For the Windows (WIN32) versions, a minimum of 20 MB disk space and 64 MB RAM is needed.

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.

3 Which Protocols are Supported?

3.1 Control connection

Checkpoint uses Internet Key Exchange Protocol (IKE) to set up a VPN tunnel. Standard IKE uses UDP/500. The source port used can be any port number. Answers are sent back to the source port of the original message.

Optionally, IKE over TCP is supported. This can be useful, if big IKE packets are fragmented and one of the devices in the network path will drop fragmented UDP packets.

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 Checkpoint NGX firewall/VPN gateway can function as initiator or responder. In IPSec client-to-LAN connections, the Checkpoint NGX appliance 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 Checkpoint VPN client complies with the IPSec protocol and is specifically designed to work with the Checkpoint NGX appliance. Likewise, the Checkpoint NGX appliance can establish LAN-to-LAN connections with other protocol-compliant VPN devices (often called “secure gateways”).

3.2.2 NAT-Traversal

IPSec encapsulation 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 encapsulates both the IKE and IPSec protocols within a UDP packet, and enables secure tunnelling through both NAT and PAT devices and firewalls (Note: This feature does not work with proxy-based devices in between).

Checkpoint NGX can simultaneously support standard IPSec and NAT-Traversal, depending on the client with which it is exchanging data.

Checkpoint does not use the standard UDP port but uses UDP/2746.

3.3 Schematic diagram VPN connection

The following illustrates a high level diagram of the Implemented Checkpoint VPN environment and building a connection from client to the appliance (server).

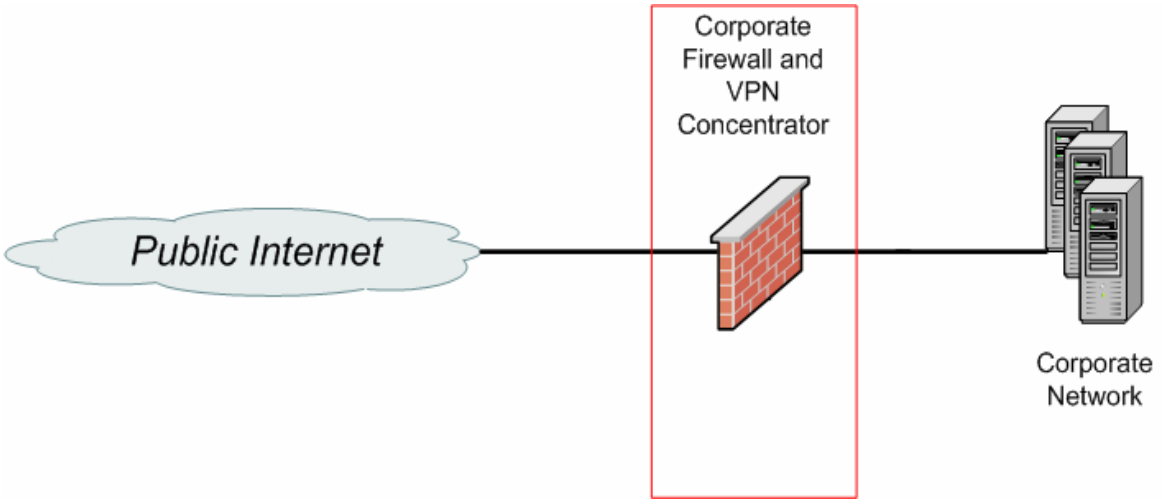


Table 1 – High-level Checkpoint VPN Environment

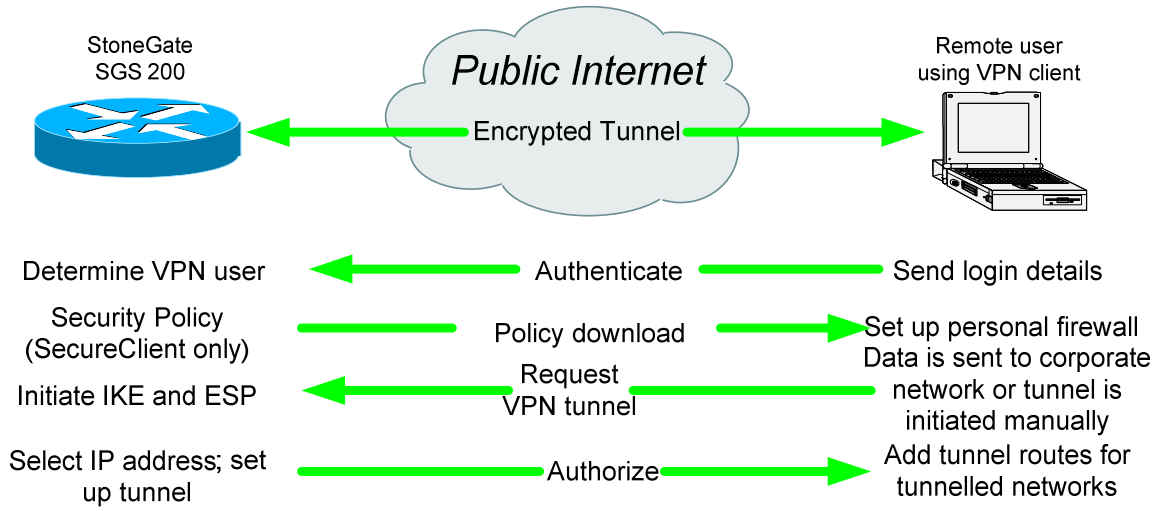


Table 2 – Logical Flow for Building Connection

3.4 Port summary for firewall setup

This table shows a summary of the ports used by the appliance 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	
IKE over TCP	TCP	Arbitrary > 1024	500	Client → Server	Optionally supported
IPSec ESP	IP	50	50	Client → Server	
Topology Information Transfer (Initiated from Client after basic configuration)					
Topology Download	TCP	Arbitrary > 1024	264	Client → Server	
Encapsulated IPSec (for NAT-Transparency)					
IKE (Standard)	UDP	Arbitrary > 1024	500	Client → Server	
IKE over TCP	TCP	Arbitrary > 1024	500	Client → Server	Optionally supported
IPSec NAT-Traversal	UDP	Arbitrary > 1024	2746	Client → Server	Proprietary, destination port is configurable

Table 3 – Port Summary

3.5 IKE “keep alive” messages

In a network environment using Network Address Translation, IPSec keep alive messages help to keep the connection entries on the NAT device up to date.

Without keep alive messages, the table entries on the NAT device “age” and the connection data is deleted eventually. This leads to a loss of connection when the gateway wants to reach the client after an interval without data transfer.

Keep alive messages are initiated on the client and may be answered by the gateway. Some VPN systems also feature IKE dead peer detection (DPD) to keep the IKE connection alive.

NAT keep alive can be activated on the VPN gateway, DPD is not configurable. See appendix A for the detailed configuration.

Recommendation:
Enable “Keep NAT-Traversal alive” if you are planning to use 3G or GPRS connections.

4 VPN Performance

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

4.1 Keep alive messages

This feature lets Checkpoint NGX monitor the continued presence of a remote peer and to report its own presence to that peer. If the peer becomes unresponsive, the Checkpoint NGX appliance removes the connection. Enabling IKE keep alive prevents hung connections when the IKE peer loses connectivity.

By default, keep alive messages are sent every 20 seconds and have a size of about 98 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 60 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 using LZS compression algorithm (“Deflate”) is available and can be enabled in the Global Properties>Remote Access>VPN-Basic. Enabling data compression might speed up the data transmission rate of VPN users. Compression is only available when using SecureClient; for SecuRemote no compression is available.

Notes and recommendations:
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 if every member of the group is a remote user connecting with low bandwidth such as GPRS.
2) If any member of the group connects via broadband, divide the group into two groups and enable compression only for the group of low-bandwidth users. For the broadband users the IP compression is not needed at the first place.

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 7.3 for some results.

5 Support of Split Tunnelling

The client-server VPN connection supports split tunnelling, and this needs to be configured on the gateway. 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. The VPN configuration therefore lets you set up the tunnelling mode policy that will be pushed to the client when connecting.

We recommend **not** using split tunnelling for security reasons. To block Split Tunnelling, SecureClient must be used.

5.1 Configuration of Split Tunnelling

Split Tunnelling abilities depend on the VPN Client type.

When using the SecuRemote VPN Client, Split Tunnelling is the default behaviour and cannot be switched off. There is no personal firewall which would inhibit access to the internet.

When using SecureClient, a full featured personal firewall is activated. This firewall can be configured on a rule by rule basis, so that unencrypted access to certain networks or all unencrypted access can be prohibited. The security policy is updated when the VPN connection is established.

5.2 Recommendation

To use with Vodafone Mobile Connect Cards over the Vodafone 3G/HSDPA/GPRS infrastructure, the following settings are recommended:

- NAT traversal should be supported on the VPN gateway (Checkpoint gateway properties>VPN>VPN Advanced, industry standard NAT Traversal)
- Checkpoint proprietary NAT Traversal must be supported on the gateway (Checkpoint gateway properties>Remote Access, “Support NAT traversal mechanism (UDP encapsulation”)
- Refrain from using SecuRemote and rather use SecureClient to provide client protection.
- When using SecureClient, configure a security policy which blocks unencrypted traffic from the internet to the client. If possible, block unencrypted traffic to the Internet also to disable Split Tunnelling.

6 Additional Applications & Services

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

6.1 Client Firewall

A local firewall is shipped with the Checkpoint SecureClient. The firewall is able to filter packets according to the security policy downloaded from the “policy server”, normally residing on the enforcement point (security gateway).

6.2 Virus scanner support

There is no built-in virus scanner, but 3rd party products can be spliced into the data flow by using the OPSEC protocol, which was disclosed by Checkpoint.

6.3 Timers

Apart from the IKE and IPSec rekey intervals and the keep-alive interval, no timers can be changed.

6.4 SNMP

Support for SNMP traps depend on the device running the Checkpoint software. E.g. Nokia IP Security Platforms support SNMP. In this case, SNMP is configured via the Nokia Network Voyager web based configuration.

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 to test the NGO:

- IBM T20 Notebook running Windows XP Professional SP2
- DELL Inspiron 8600 Notebook, Windows XP Professional SP2
- Gericom WebgineXL, Windows XP Professional SP2
- Microsoft Outlook 2003 SP2 and Exchange 2003 Server
- Internet Explorer (Version 6)
- DU Meter Version 3.07 Build 200 for measuring data transfer
- Vodafone Mobile Connect Card UMTS/GPRS Option Fusion, firmware 1.5.5
- VMC software R7.00.0005

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.

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.

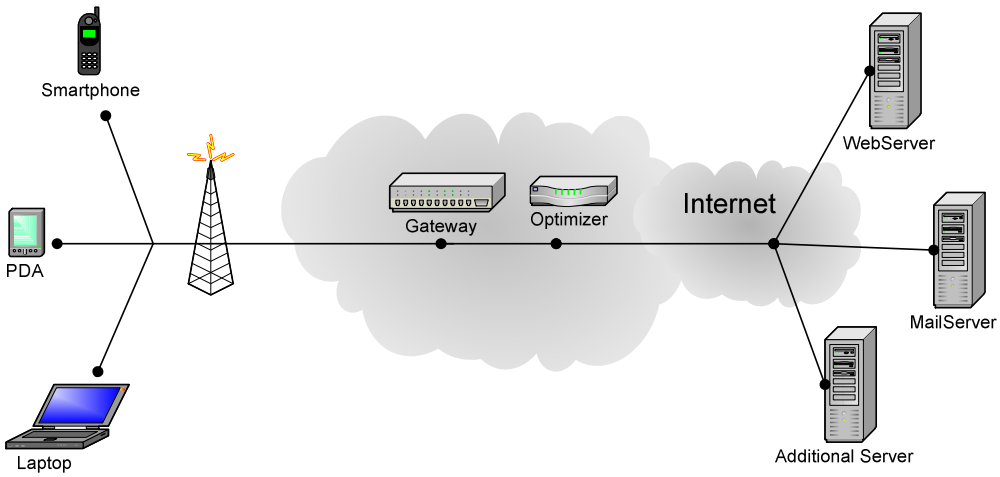


Table 4 – Schematic of Network Generic Optimisation in Mobile Network

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:

- 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, Checkpoint FW-1/VPN-1 NGX is using a non-standard UDP port for NAT-Traversal. 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 Checkpoint FW-1/VPN-1 NGX VPN uses only UDP encapsulation, no problems with the Macara optimisation occurred.

7.3 Results

The results are shown in the tables below for both SecureClient and SecuRemote.
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..

7.3.1 SecureClient

Used reference files: Word Document = 300 KB; MP3 File = 3072 KB= 3 MB[5]; 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**[2]	245,67	3,21	251,00	3,13	258,33	3,18	235,00	3,19
300KB / 3072KB	**http-internet**[3]	167,17	3,05	141,00	3,05	n/a[1]	n/a[1]	n/a[1]	n/a[1]
300KB / 3072KB	**ftp-internet**[4]	289,70	3,10	301,67	3,07	n/a[1]	n/a[1]	n/a[1]	n/a[1]
300KB / 3072KB	**http-intranet**	283,67	3,18	301,33	3,11	281,33	3,10	249,67	3,07
300KB / 3072KB	**ftp-intranet**	301,33	3,18	304,37	3,14	298,67	3,12	299,00	3,14

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 – SecureClient

7.3.2 SecuRemote

Used reference files: Word Document = 300 KB, MP3 File = 3072 KB = 3 MB[5], 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[2]**	218,5	3,03	217,1	3,01	n/a[1]	n/a[1]	n/a[1]	n/a[1]
300KB / 3072KB	**http-internet[3]**	154,6	3,04	153,1	3,04	n/a[1]	n/a[1]	n/a[1]	n/a[1]
300KB / 3072KB	**ftp-internet[4]**	310,7	3,05	310,8	3,05	n/a[1]	n/a[1]	n/a[1]	n/a[1]
300KB / 3072KB	**http-intranet**	279,1	3,03	279,1	3,03	n/a[1]	n/a[1]	n/a[1]	n/a[1]
300KB / 3072KB	**ftp-intranet**	312,1	3,06	312,0	3,07	n/a[1]	n/a[1]	n/a[1]	n/a[1]

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 6 – Test Results for NGO and VPN compression - SecuRemote

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 either by the NGO or the VPN systems. In fact, a slight increase in data transfer (<5%) is observed reflecting the overhead of encryption and encapsulation of a VPN solution.

The compression provided by the VPN system provides little benefit in the NGO environment:

- The SecuRemote client showed no meaningful benefit from compression.
- The SecuClient configuration showed improvement of <5% from using compression, and even showed an increase in one case (http-internet).

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 (5.2).

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 appliance and the client have 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.

9 VPN Client Installation and Configuration (Checkpoint SecureClient NGX)

The Checkpoint VPN clients can be installed on most Windows platforms (WIN32) and some Windows mobile, LINUX and Macintosh platforms. To install the software, a user needs administrator rights on the local computer. Also older versions of SecureClient or SecuRemote down to version 4.1 can be used to establish a VPN connection to the Checkpoint NGX gateway. Other VPN clients must be de-installed before installing Checkpoint clients.

Run the installation program according to the directions given by the program. For further information, review the Checkpoint client installation guide.

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 Checkpoint documentation and refer to Appendix B: “VPN Client - chapter Installation and Configuration”.

10 Configuration & Connection Using VMC Software

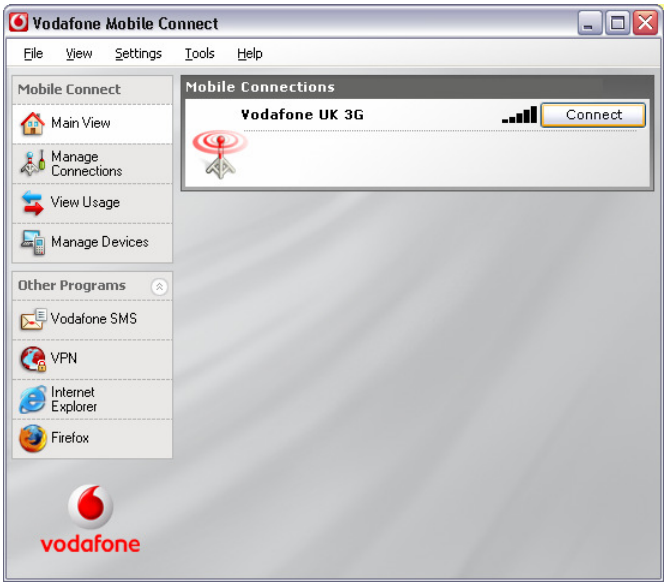
The Checkpoint VPN client is installed as a system utility and runs transparently whenever the computer is started. The client is accessed via the icon in the Windows Notification Area (System Tray). As the client is always running, there is no need (and it is not possible) to configure the VPN button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

10.1 Establish the connection (VMC R9)

The new R9 of Vodafone Mobile Connect software offers the same features as earlier versions but with a different user interface.

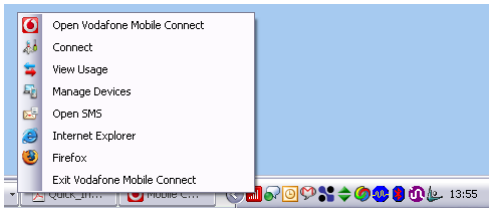
With a SIM card inserted into your datacard (or USB modem), to establish a connection:

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



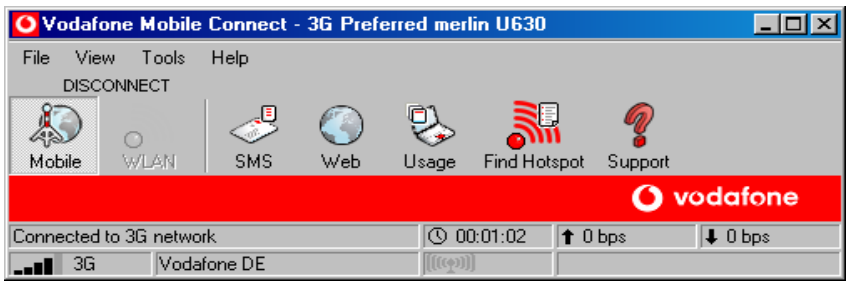
2. In the mini-view, use the **Connect** button, or

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



10.2 Establish the connection (VMC R7 and earlier)

Note: The following steps apply to the legacy version of Vodafone Mobile Connect software R7 and earlier.



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

10.3 Establish the VPN

- As the Checkpoint NGX VPN clients are placed into the system tray by default, there is no need to configure the current Dashboard for the VPN, furthermore the Checkpoint NGX VPN clients run as a service and start the VPN establishment when triggered by a network packet intended for the protected network.

10.4 VPN Client Starting and Connection Option

To initiate the VPN tunnel, either start the application that needs access to the corporate network to initiate the VPN client or start the VPN manually from the system tray icon of the VPN client. Use the right mouse button to obtain the context menu and select connect.

Then enter the user credentials and click OK.

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. Is the VPN-system configured for NAT/NAPT-Traversal? 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.Checkpoint.com in the web browser or just “ping www.Checkpoint.com” or “ping 84.34.144.5”.

- Does the network access to the internet allow the ports necessary for IKE and NAT-Traversal?

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

11.2 Known Problems

- When the Checkpoint VPN client is installed after the Vodafone Dashboard, the Dashboard configuration may be lost. There is no known measure to prevent this, just reconfigure the Dashboard profile.
- The Checkpoint VPN clients older than Version NGX do not reduce the Medium Transfer Unit (MTU) on the client computer. This results in IP packet fragmentation in case big data packets (e.g. over 1400 Bytes) are encrypted and the network is not able to route fragmented packets. This was observed e.g. in the Vodafone networks of Vodafone UK and Spain.
  To avoid this problem, reduce the MTU-size by setting the appropriate registry setting on the Windows client computer. The NGX Version of the client automatically reduces the MTU to 1350 Bytes. For older Versions, this can be established either by using one of the freeware tools available or setting up the entries using regedit as described in the Microsoft Knowledgebase article http://www.microsoft.com/technet/community/columns/cableguy/cg0704.mspx .
- If SecuRemote is used, no virtual network interface is created and split tunnelling is active. This leads to the possibility, that the optimiser built into the Vodafone Dashboard is going into active state and depending on the sequence of operation of optimiser and VPN client, packets may be “optimised” before encryption. Since the encrypted packet passes the optimisation server in the network, the data reaching the protected networks is garbled. To avoid this, switch off the optimisation in the Dashboard.

11.3 Logging Appliance (server side)

Event logging is available on the Checkpoint NGX SmartDashboard. The firewall logs can be filtered and exported in several ways.

For further information please refer to the Checkpoint appliance documentation.

11.4 Logging Client (client side)

On the client side, a VPN status can be displayed via the log viewer. The program can be started from the Windows “start menu>Programs>Checkpoint SecuRemote>logviewer”.

**** End of Document ****