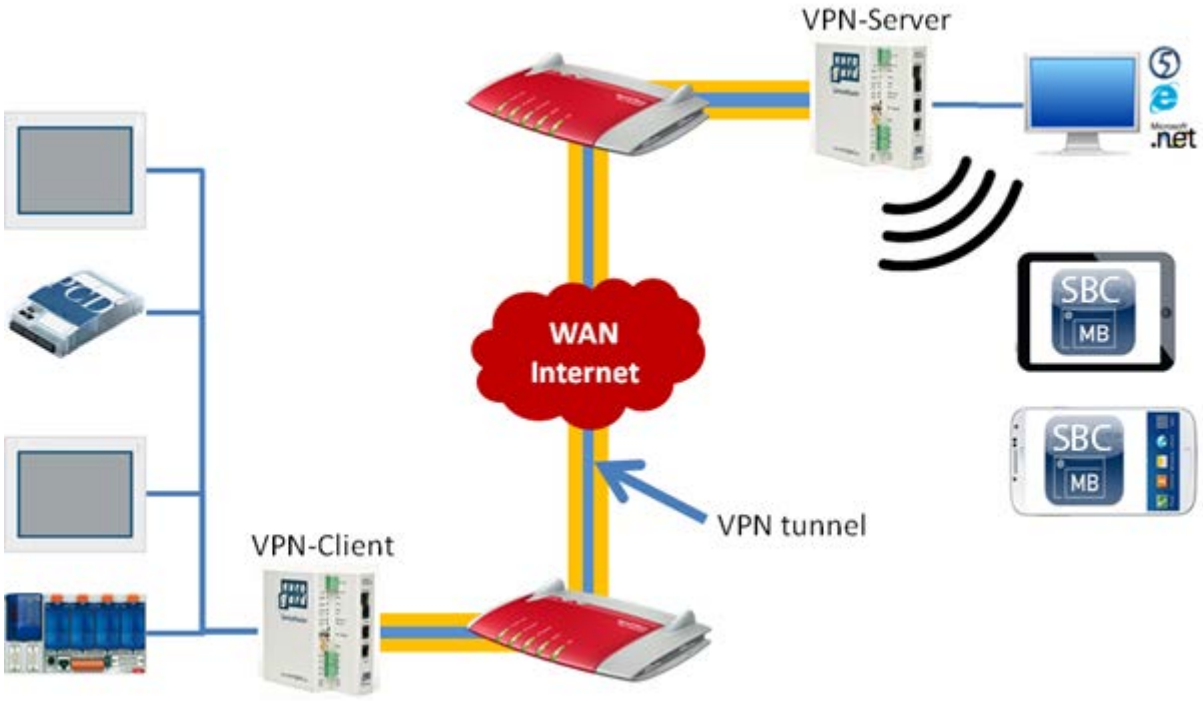
Saia-Burgess Controls AG
Bahnhofstrasse 18 I CH-3280 Murten I Switzerland
T +41 (0)26 672 72 72 I F +41 (0)26 672 74 99 I www.saia-pcd.com

VPN Router



Document History

Version	Revision	Publication	Notes
EN01	25/07/2013	26/07/2013	
EN02	30/09/2013	15/10/2013	New tested Routers: ➔ Net Module NB 1600 ➔ Vigor 2920 same configuration but no ADSL/VDSL Modem included
EN03	2014-02-20	2014-02-20	New company logo

Saia-Burgess Controls AG
Bahnhofstrasse 18 I CH-3280 Murten I Switzerland
T +41 (0)26 672 72 72 I F +41 (0)26 672 74 99 I www.saia-pcd.com

Contents

Information on this document:
Safe operation of the PCD controllers on the internet can only be guaranteed with additional external IT components offering integrated protection functions such as VPN, firewall, proxy servers, etc.

To that end, we have evaluated several VPN routers and tested them with our PCD controllers. This document lists the devices successfully tested and their suppliers. In this document the configuration and initial operation is

Tested devices:

- DreyTek Vigor 2850Vn
- DreyTek Vigor 2920Vn
- EuroGard Service Router V2 (WLan)
- EuroGard Service Router V2 (UMTS)
- Net Module NB 1600Net Module NB 1600-U

1 Technical information: Vigor 2850Vn, 2920, EuroGard Service Router V2 and Net Module NT 1600-U

The DrayTek Vigor 2850 is a business router for establishing VPN connections and managing small to medium-sized business/home networks. Its functionality and user interface are easy to use.

The EuroGard Service Router V2 is an industrial router for establishing secure connections on industrial installations. The configuration menu is available in several languages. The user guidance is simple to follow and establishing the VPN connection is easily achieved.

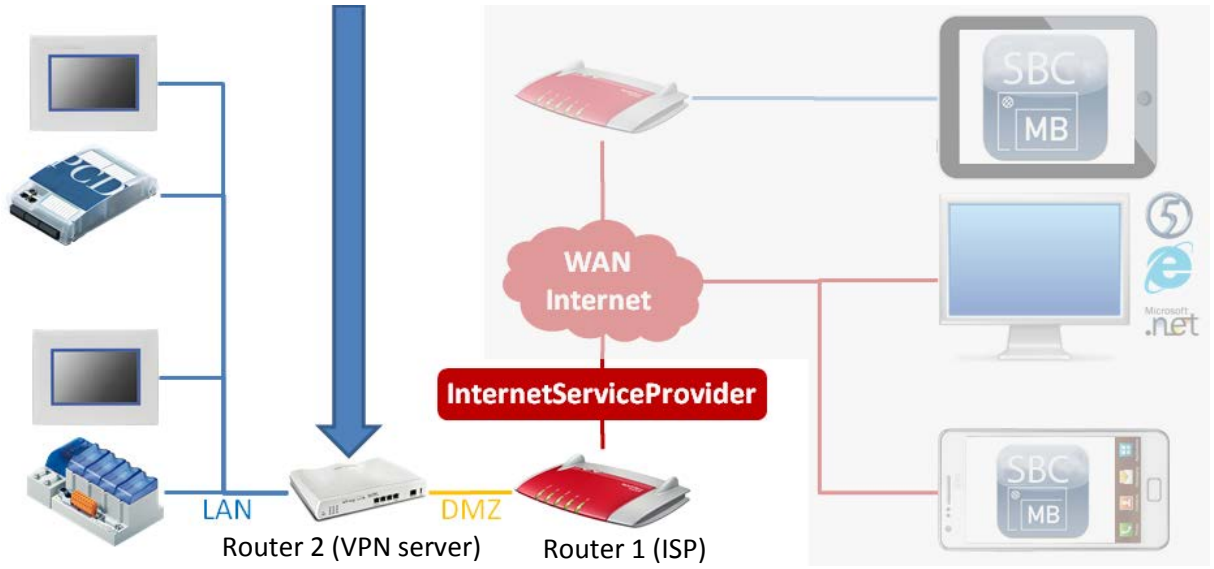
	DrayTek Vigor 2850Vn	**DrayTek Vigor 2920VN**	**EuroGard Service Router V2 (WLan)**	**EuroGard Service Router V2 (UMTS)**	**Net Module NB 1600-U**
Order data	2850Vn	2920Vn	ER 1201-WLAN	ER 1201-UMTS	NB 1600-U
Additional information	http://www.draytek.de/produkte/modem-router/vigor2850-serie.html	http://www.draytek.de/produkte/dual-wan/vigor2920-serie.html	http://www.eurogard.de/en/	http://www.eurogard.de/en/	http://www.netmodule.de/products/industrial-routers/mobile-router.html
Application/ Type	Business/Home	Business/Home	Industrial	Industrial	Industrial
Top-hat rail installation	No	No	Yes	Yes	Yes
Electrical supply	230 VAC	230 VAC	24 VDC	24 VDC	24 VDC
VPN Features					
Number of WAN interfaces	3: LAN/Modem/USB	3: LAN/Modem/USB	1: LAN	2: LAN/UMTS	2: LAN/UMTS
Integrated ADSL/VDSL modem	Yes	No	No	No	No
VPN PPTP	Yes	Yes	No	No	Yes
VPN L2TP/IPSec	Yes	Yes	No	No	No
openVPN	No	No	Yes	Yes	Yes
No. VPN clients	32 connections	32 connections	30 connections	30 connections	10 connections
Windows client	Yes (integrated in Windows)	Yes (integrated in Windows)	Yes (EurogardSRConnect)	Yes (EurogardSRConnect)	Yes (openVPN)
IOS Client	Yes (IPSec/L2TP, integrated in IOS)	Yes (IPSec/L2TP, integrated in IOS)	No*	No*	Yes (openVPN)
Android Client	Yes (IPSec/L2TP, integrated in Android)	Yes (IPSec/L2TP, integrated in Android)	No*	No*	Yes (openVPN)
Extensions					
3G/4G modem	Yes, with USB stick	Yes, with USB stick	No	Yes, with integrated UMTS modem	Yes, with integrated 3G modem

* IOS or Android systems can now be connected to the router via WLAN. This requires two routers. One VPN server and one VPN client. Support for VPN on mobile devices is in preparation.

2 Use of an existing internet access point

2.1 Preparation

Setting up a connection in an existing Ethernet infrastructure: The internet connection to the Internet Service Provider (ISP) is enabled by an existing device (Router 1 in the figure below).



In the case shown above the internet connection to the ISP is established by Router 1. The existing Ethernet infrastructure should not or cannot be modified. Router 2, which contains the VPN server, is installed behind Router 1 in the existing LAN. In this case, Router 1 must be configured such that all relevant VPN ports are transmitted to the IP address of Router 2, or the DMZ is configured to the IP address of Router 2.

Depending on the configuration of the VPN connection [the VPN connection may be configured with Point-to-Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP), which is usually used in combination with Internet Protocol Security (IPSec)], different ports from the public network are required at the WAN interface of the VPN server. A port represents a gateway for communicating with an application via TPC/IP, in this case with the VPN server.

	Protocol	**Port**
PPTP default	TCP	1723
L2TP default	UDP	1701
IPSec default	UDP	500, 4500

In a normal configuration, most of the ports on the router managed by the ISP connection are blocked by the internal firewall. It is therefore **not** possible to operate a VPN server without making slight changes to the existing Ethernet structure.

As a rule, firewall means that all data packages trying to access the LAN via undefined ports will be blocked by Router 1 which manages the ISP connection. It is therefore not possible for the undefined port to establish communication with the devices behind the firewall.

In order to be able to establish a connection to the VPN server (device behind the firewall) of the ISP-managing Router 1, the ports relevant for the VPN connection in Router 1 must be defined in a firewall rule.

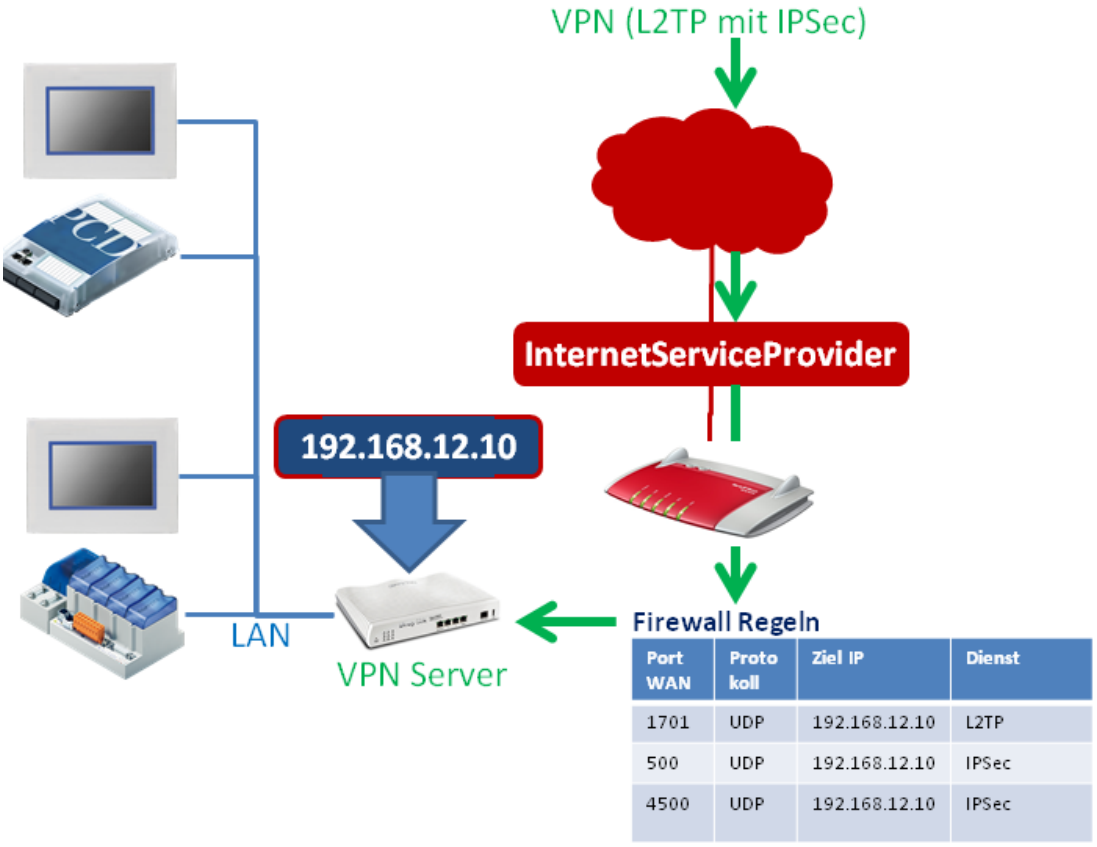
The configuration of Router 1 for forwarding ports depends on the manufacturer and software version of the device used. In general, there are 2 ways to forward these ports to the VPN server.

2.1.1 Explicit port forwarding (Forwarding)

The ports for establishing a VPN connection from the client to the server must be forwarded to the VPN server from the first router by means of a firewall rule.

Ports:

PPTP Standard	=	TCP/UDP	→ 1723
L2TP Standard	=	UDP	→ 1701
IPSec Standard	=	UDP	→ 500, 4500
SSL	=	TCP/UDP	→ 443



Port WAN	Proto koll	Ziel IP	Dienst
1701	UDP	192.168.12.10	L2TP
500	UDP	192.168.12.10	IPSec
4500	UDP	192.168.12.10	IPSec

Advantage of this configuration:

Very secure, since only the ports specified above are available on the VPN server.

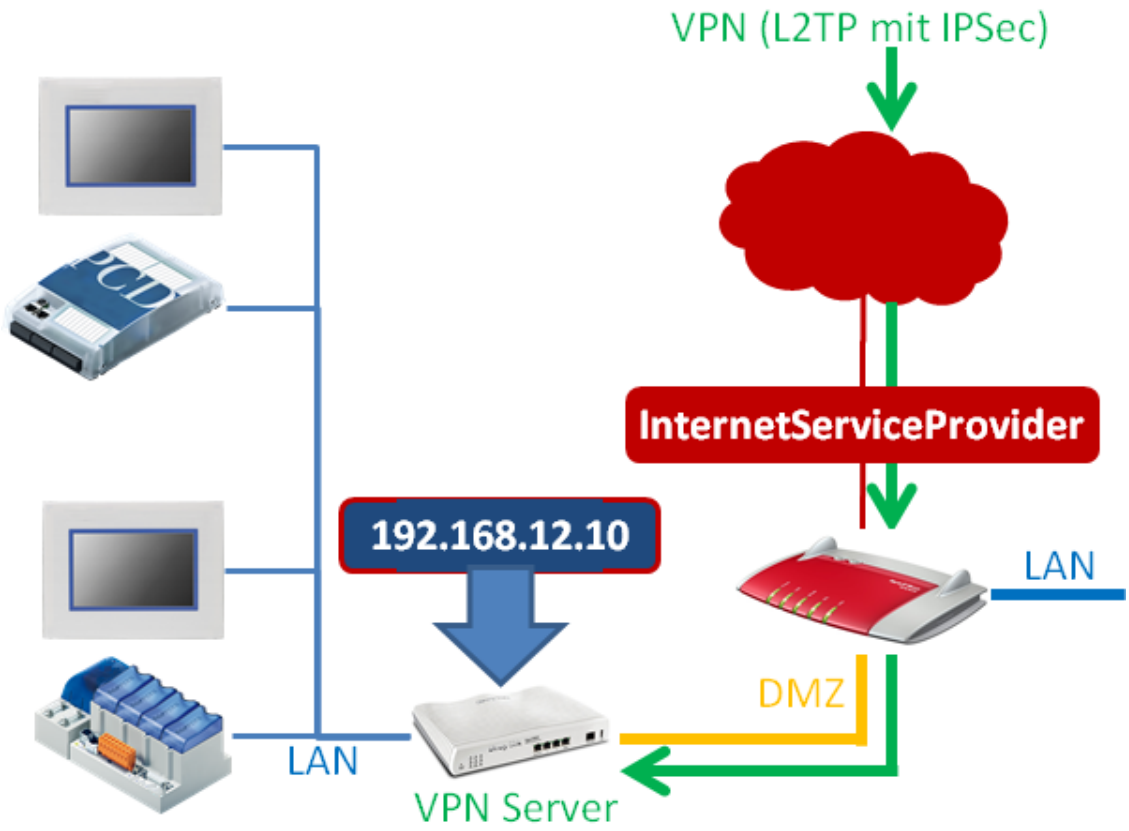
Disadvantage of this configuration:

The VPN ports are defined with the ports described above by default. However, these definitions are not fixed and can be modified in the VPN server setup. If port forwarding is not completely identical with the configuration of the VPN server, a connection cannot be established.

The use of a DMZ offers additional options.

2.1.2 Configuration of a DMZ

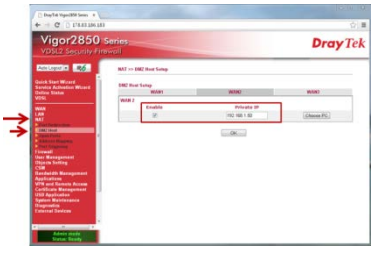
A DMZ allows all ports that are queried at the WAN interface and for which the first router cannot find a rule to be forwarded to a specific IP address.



Preparation of the existing router DMZ/NAT:

A DMZ must be established in order to keep the existing router that is connected with the ISP from distributing queries to unknown ports. This configuration may vary from router to router, but it is usually clearly described in the setup help section or in the router manual.

DMZ represents a “Demilitarized Zone”. For devices that don’t have their own security features, the zone is not protected and not more secure. In the DMZ, the properties of every device are comparable to those it would have if it were actually connected to the internet. This is because the router that is physically connected to the internet forwards all unrecognized data packages to or into the DMZ.



In most cases, the DMZ is configured with a designated IP address.

Caution:

Ports which have a rule that is recognized by the first router are not forwarded to the DMZ.

Disadvantage:

The VPN server requires its own protection system (firewall, etc.…)

Advantage:

Very easy to configure and manage.

3 Vigor 2xx0 DrayTek

In the document the configuration of the Vigor router DreyTec 2850 and 2920 will describe. Both have the same configuration interface for configuring the basic settings and VPN. As opposed to Vigor 2850, the Vigor 2920 has no built-in ADSL / VDSL modem

3.1 Opening the setup menu

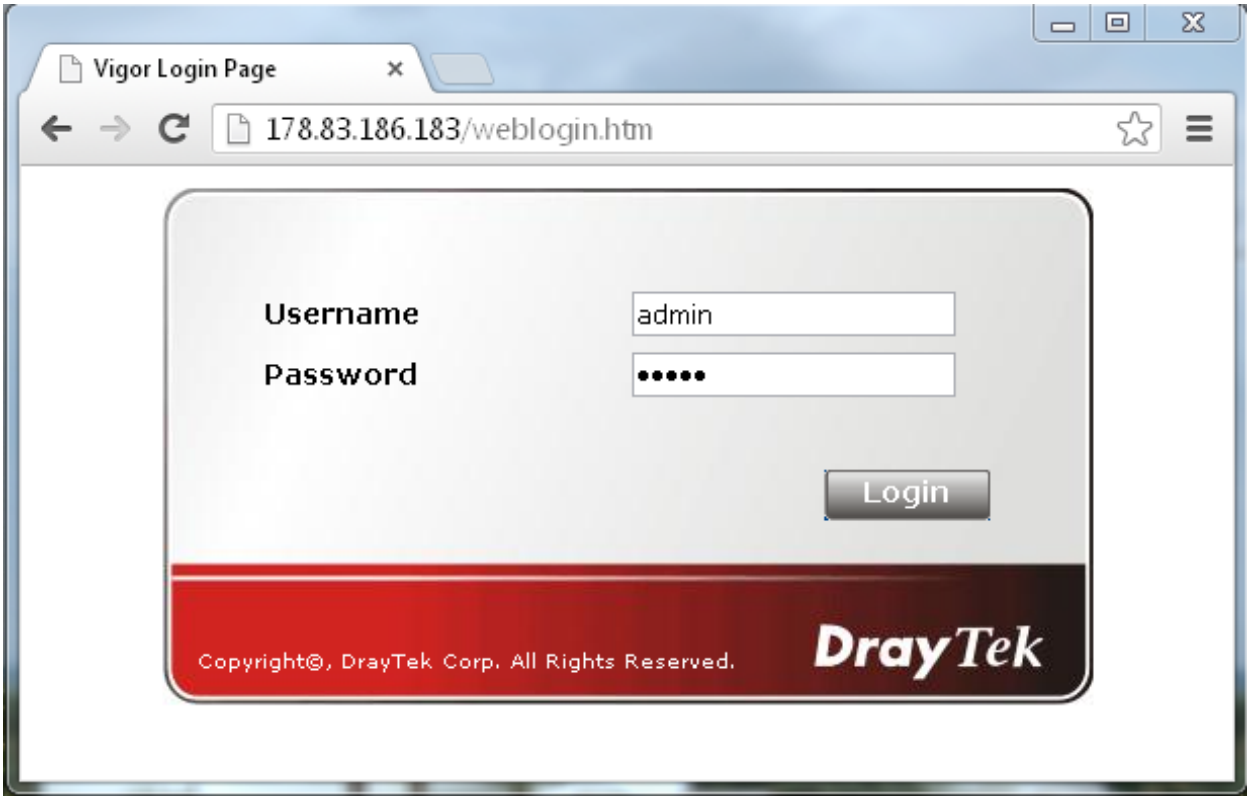
The PC must be connected to a LAN interface in order to set up the Vigor 2xx0. The router includes an active DHCP server with delivery. Configuring the Vigor 2xx0 with a factory configuration in an Ethernet infrastructure with an existing DHCP server should therefore be avoided.

Recommendation:
Disconnect your PC from all existing network connections.
Connect your PC directly to the router.

By default, the IP address of the router is configured to “192.168.1.1”. The router’s DHCP server provides the connected PC with an address in the DHCP server’s address space (usually “192.168.1.10” for the first device).

The router is configured in a browser.
In order to load the configuration interface in the browser, the router’s IP address must be entered in the browser.

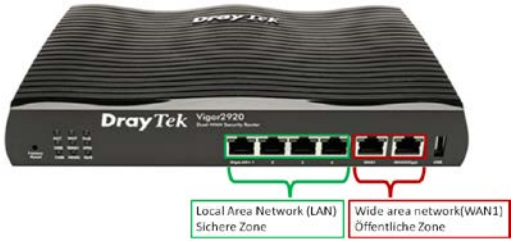
By default, the Vigor 2xx0 is delivered with the user name “admin” and password “admin”. You can also find user names and passwords in the router manual.


Vigor Login Page
178.83.186.183/weblogin.htm
Username
admin
Password
Login
Copyright©, DrayTek Corp. All Rights Reserved.
DrayTek

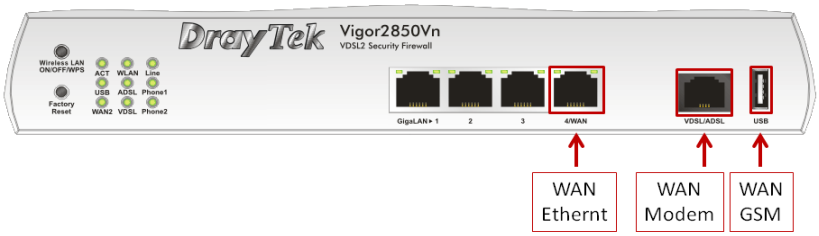
3.2 Configuring the WAN port

WAN stands for “Wide Area Network”. With a router, this is always the public interface in a public, unprotected area.

Vigor 2920



Vigor 2850



3.3 WAN operation behind a router/firewall

The Vigor 2xx0 allows 3 different WAN ports to be configured.

Note: The Vigor 2920 has no built-in ADSL / VDSL modem

Overview of possible connection types:

1) ADSL/VDSL modem → (only Vigor 2850)
   this configuration enables the router to be directly linked to an ISP’s ADSL/VDSL connection using the integrated modem. The ISP’s configuration parameters are needed for this type of connection.
2) Ethernet →
   this configuration allows the router to be operated behind an existing router. In doing so, the existing router provides the connection to the ISP.
3) USB →
   this configuration allows the use of a connected modem (3G/4G) to establish a link to an ISP. The ISP’s configuration parameters are needed for this type of connection.

This document outlines connection type 2. With this connection type, the router with the VPN server is positioned behind an existing router. In this case, the existing router manages the internet connection to the Internet Service Provider (ISP) and holds the system’s public IP address.

3.4 Configuring the VPN server

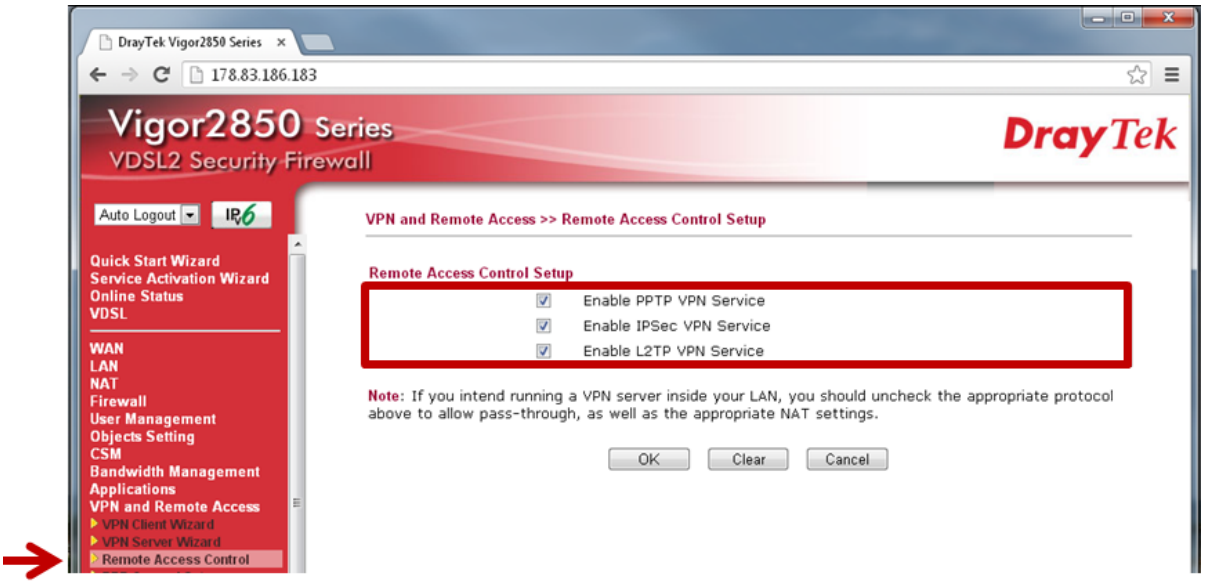
The Vigor2xx0 supports the following remote access capabilities:

1) Tunneling protocols:

   a. PPTP VPN service (Point-to-Point Tunneling Protocol)
   PPTP is used to establish a VPN by creating a tunnel for the point-to-point protocol. It provides sufficient scope for any type of authentication and encryption. The TCP port 1723 is usually used.

   b. IPSec VPN service (Internet Protocol Security)
   IPSec is a protocol suite that enables secured communication via potentially insecure IP networks, such as the internet.

   c. L2TP VPN service (Layer 2 Tunneling Protocol)
   Tunneling on the Layer 2 level of the OSI layer model (link layer). L2TP does not directly include encryption and is therefore most often used in combination with IPSec.

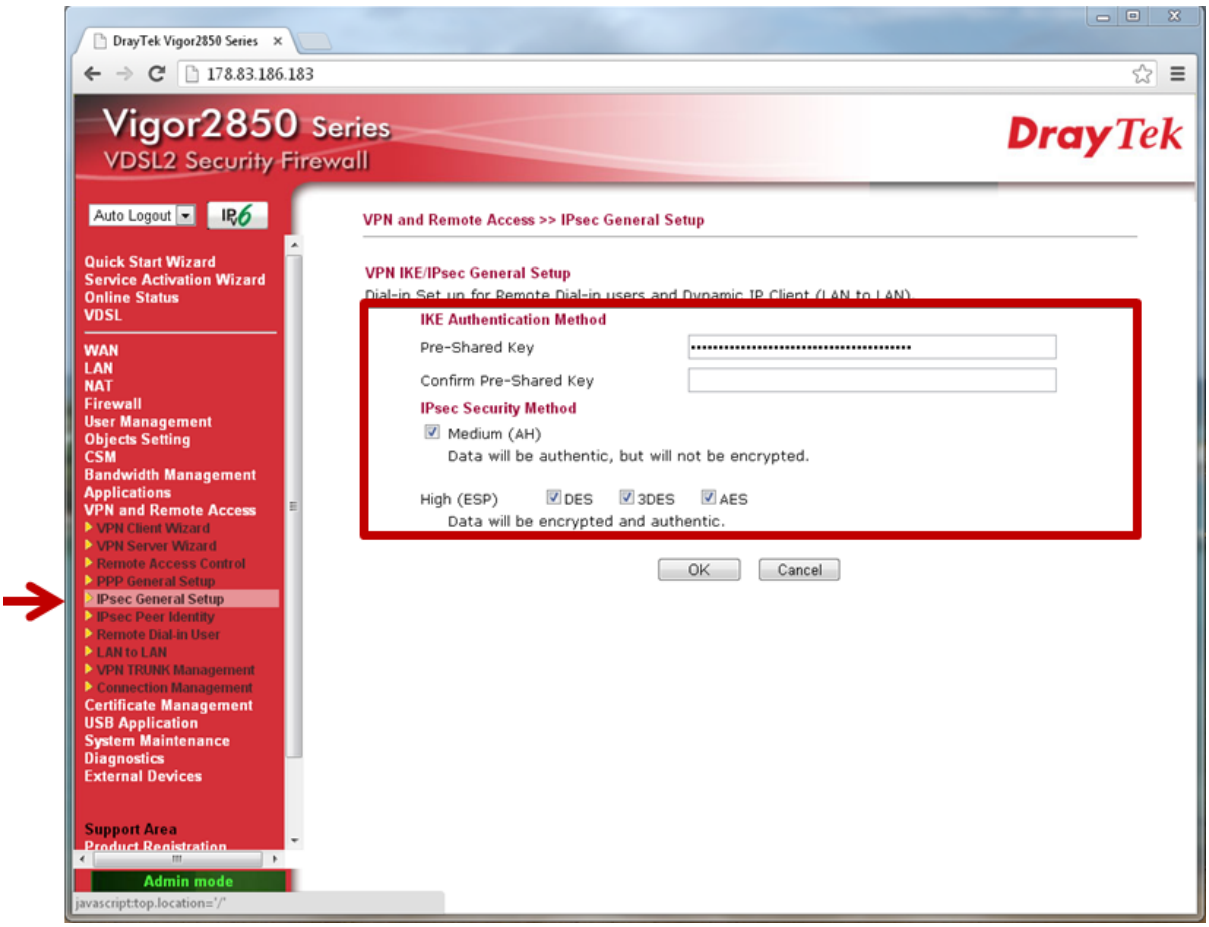


Remote Access Control Setup

L2TP is described in this document as it relates to establishing the VPN connection: Activate the service for IPSec and L2TP.
L2TP allows the routing of network NAT (Network Address Translation). In doing so, the VPN tunnel is created by IPSec.

2) IPSec settings Pre-Shared Key (PSK)

If a connection type with IPSec was selected, the PSK is required for configuring the connection options of the client.

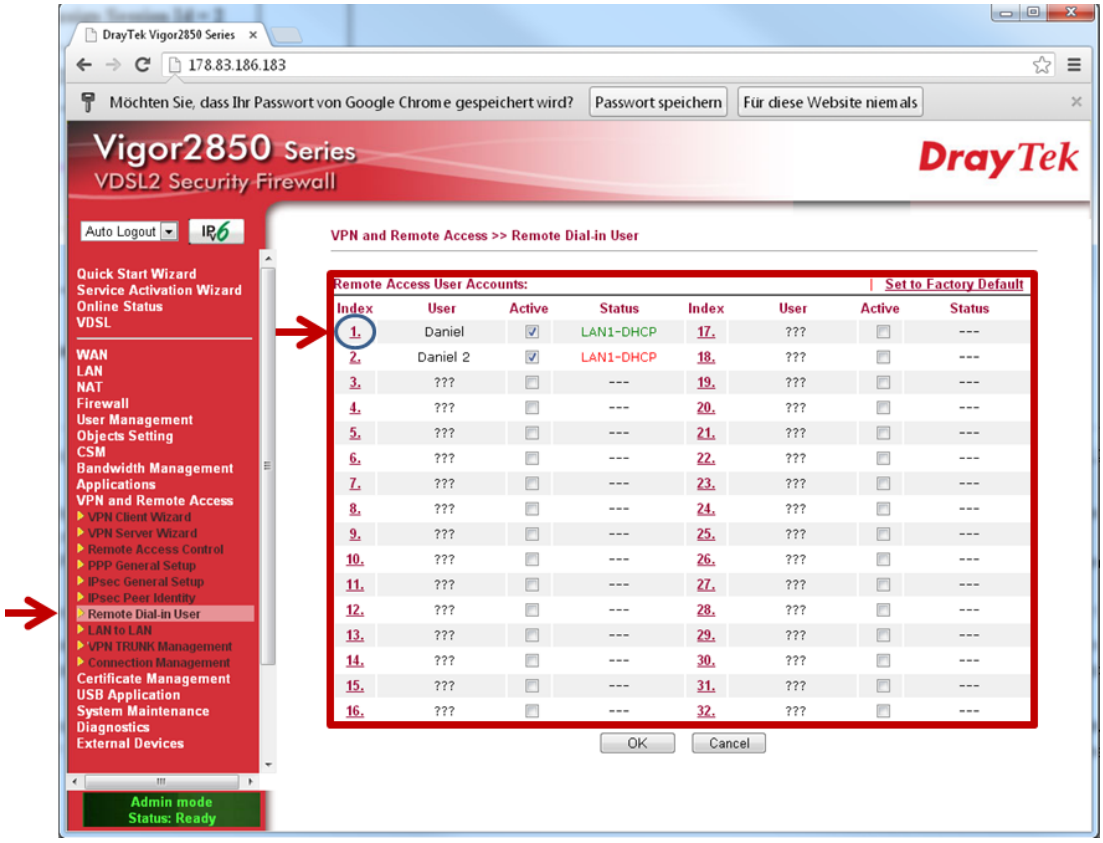


IPSec General Setup

Under no circumstances should the PSK be a word from the dictionary.
A password combining special characters, numbers and letters and totaling at least 12 characters is recommended.

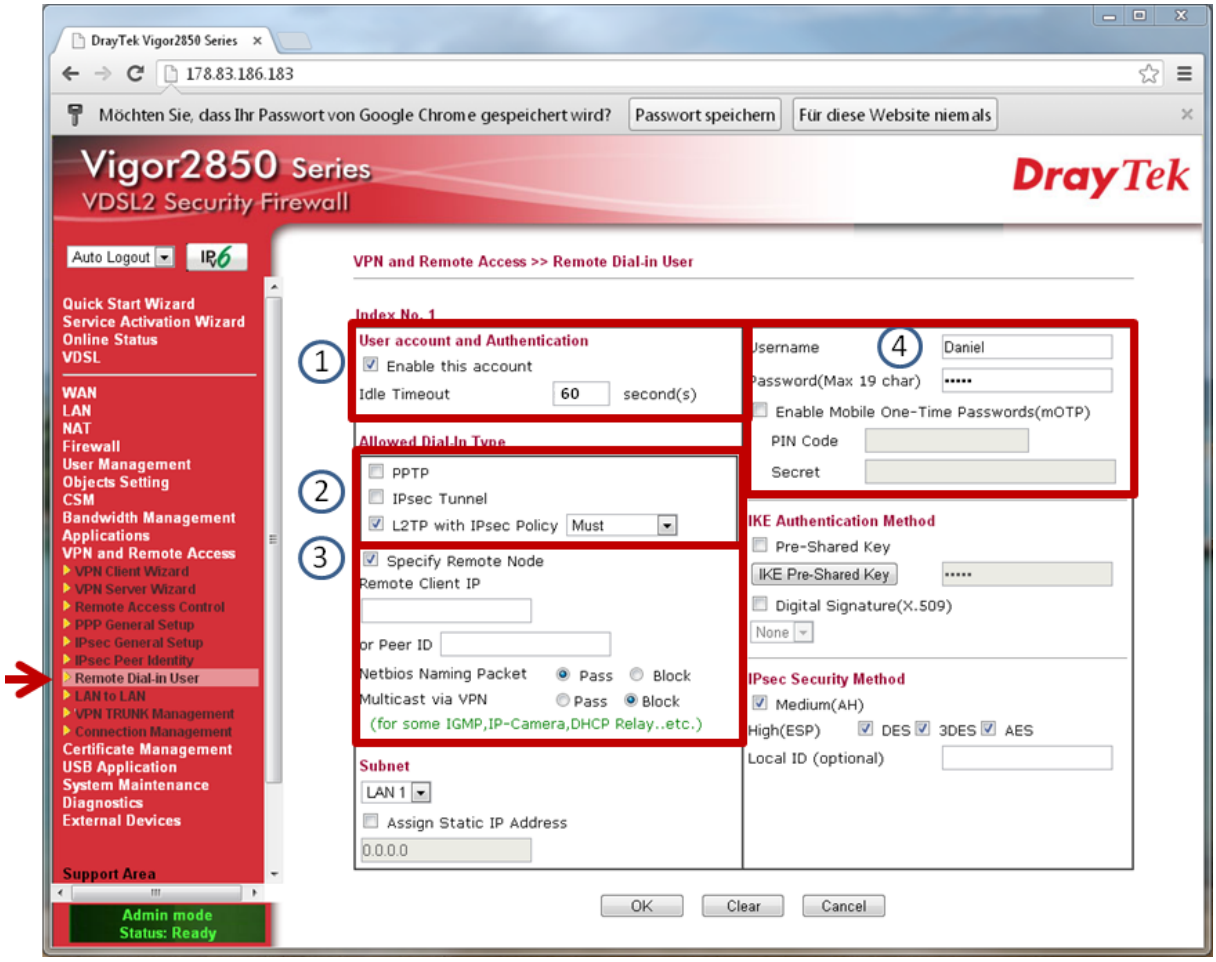
3) Remote Dial-in Users

Up to 32 users can be defined here. All of these users can log on to the VPN server. The index of the relevant line must be clicked in order to establish a new user.



32 Remote Dial-in Users

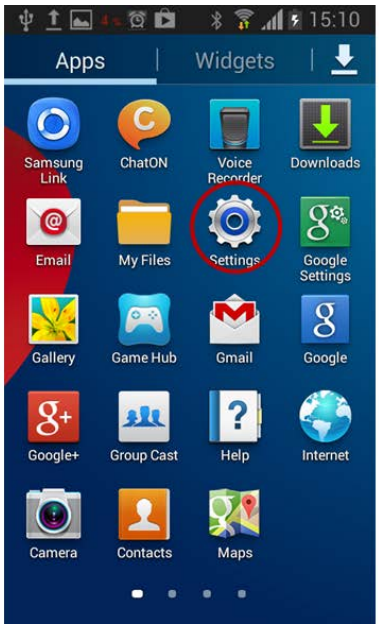
4) Remote Dial-in User Configuration
   1) Set the currently selected user to active user:
      Set the timeout to “60” seconds.
   2) Dial-in options for the currently selected user:
      Preferred setting is L2TP with IPSec policy (Must).
      In this case, a protected IPSec tunnel to the server is established. Another L2TP tunnel is then set up in this tunnel, which allows the network to route between server and client.
   3) Activate Specify Remote Node.
   4) Definition of a user name and password for authentication.

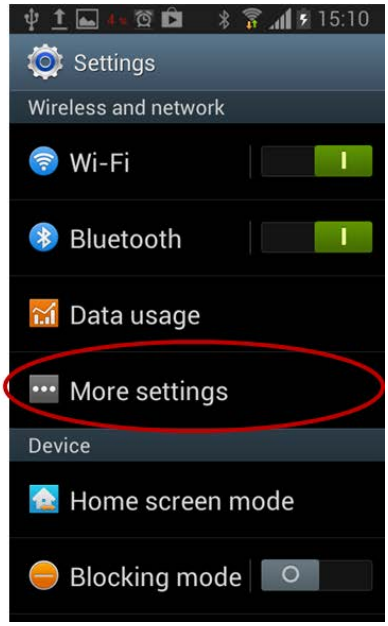


5) The VPN server is now fully configured and ready for client connections.
6) When the client is connected, a link to the application can be made simply by entering the IP and .html file in the micro browser.

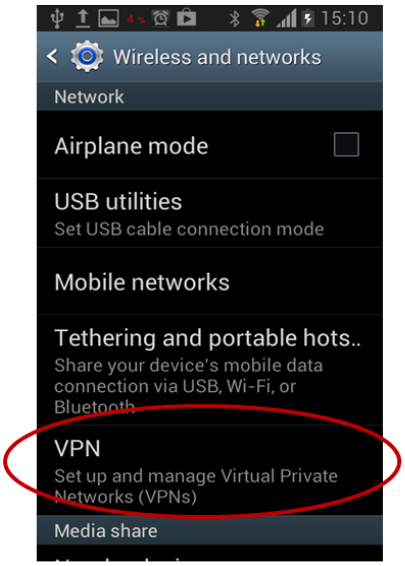
3.5 Android System 4.1.2 client

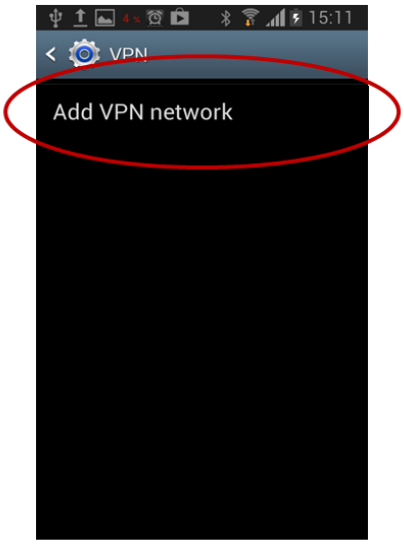
Open the menu → Settings → Additional settings:

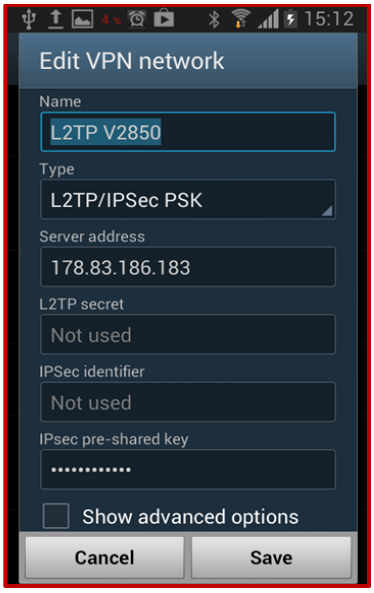




The submenu includes the entry VPN (Virtual Private Networks), which is used to configure the client:



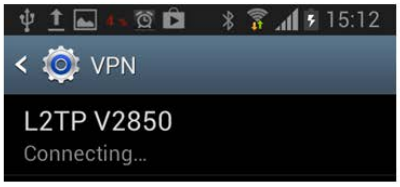


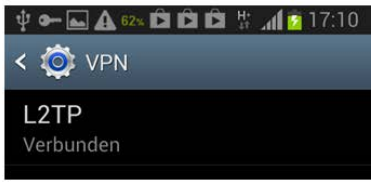


Add a VPN network connection:

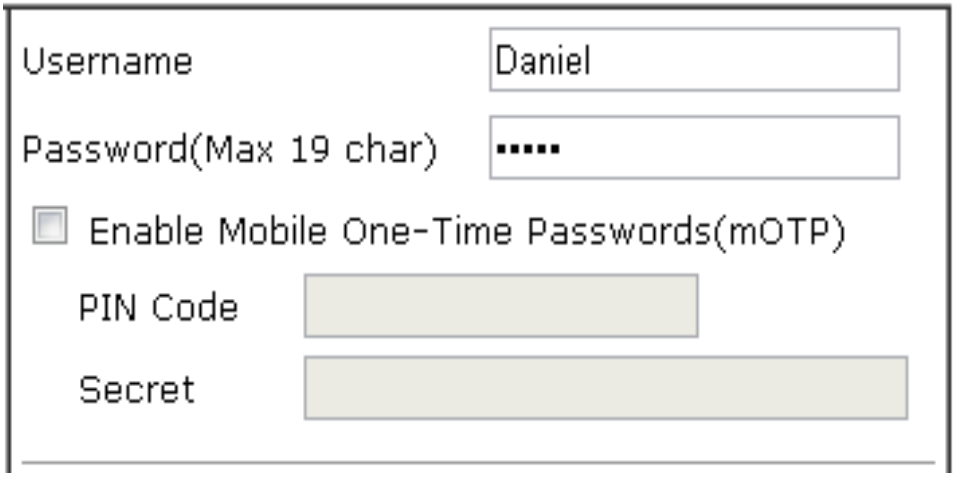
- ➔ Name = Can be freely defined
- ➔ Server address = Public IP address or DNS name of the DSL router
- ➔ L2TP key = Is not used for current router configuration
- ➔ IPSec Pre-shared Key = Key that was provided in the router IPSec general setup
- ➔ Save

Open the new VPN network connection:





- ➔ User name and password that were provided for the remote dial-in user configuration.



3.6 iPhone/iPad client

The following steps are required to establish a L2TP/IPSec connection with an I-OS device:

1) Open “Settings”. Under the menu item “General”, select “VPN”:

2) Add a new VPN connection:

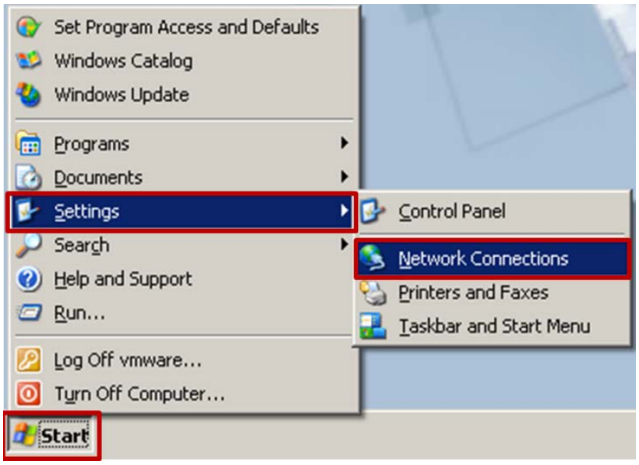
3) Create a L2TP IPSec connection with a remote VPN server.
Required settings or entries:

➔ Description: Can be freely defined
➔ Server: IP address or DNS of VPN server
➔ Account: User profile with VPN access rights to the VPN server
➔ Password: The password stored for this user profile
➔ Shared Secret: The pre-shared key (PSK) that was provided for the VPN tunnel

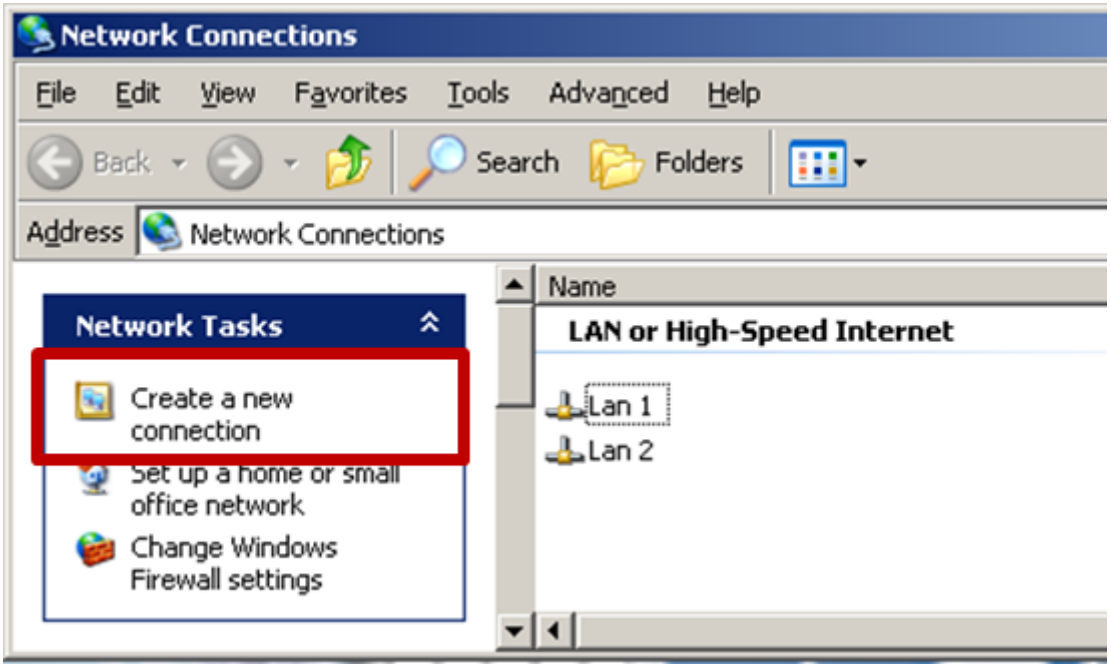
4) Select the tunnel used for VPN access and activate this tunnel. The status field displays that the tunnel was successfully established:

3.7 Client Microsoft Windows XP

1) Open the network configuration:

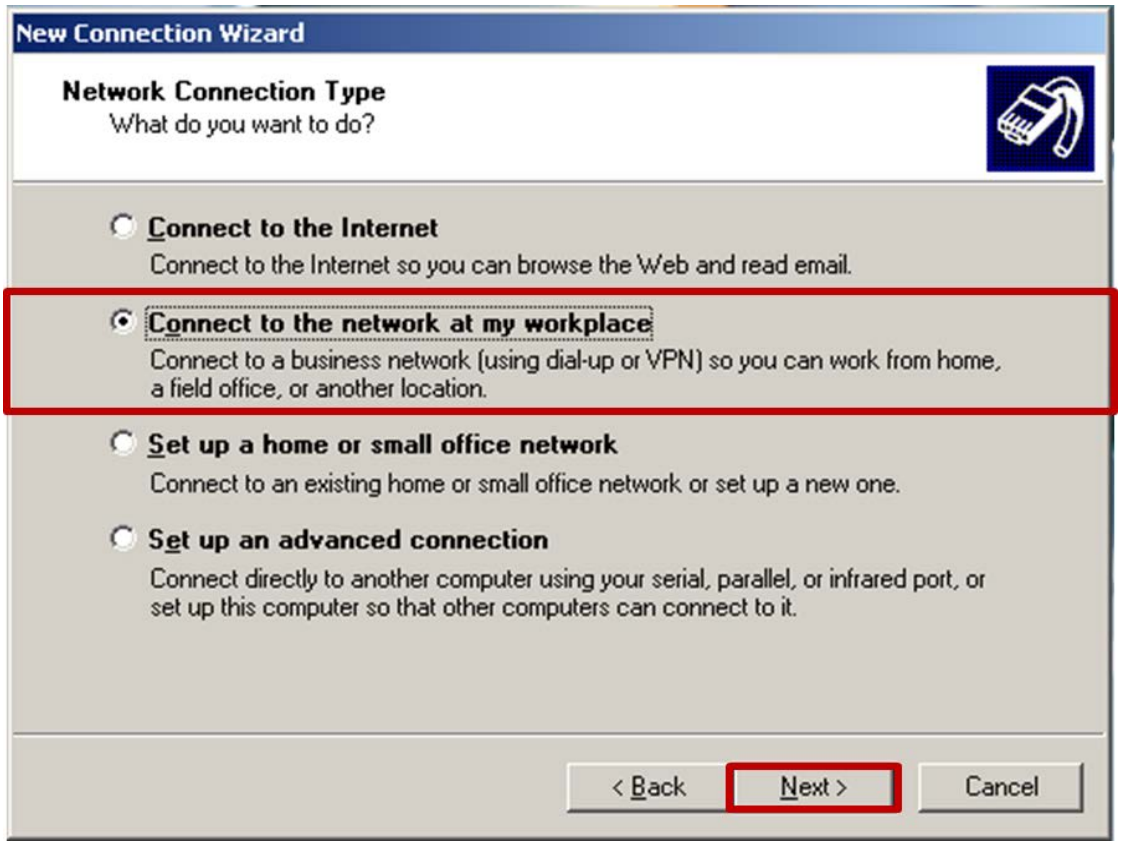


2) Create a new connection:

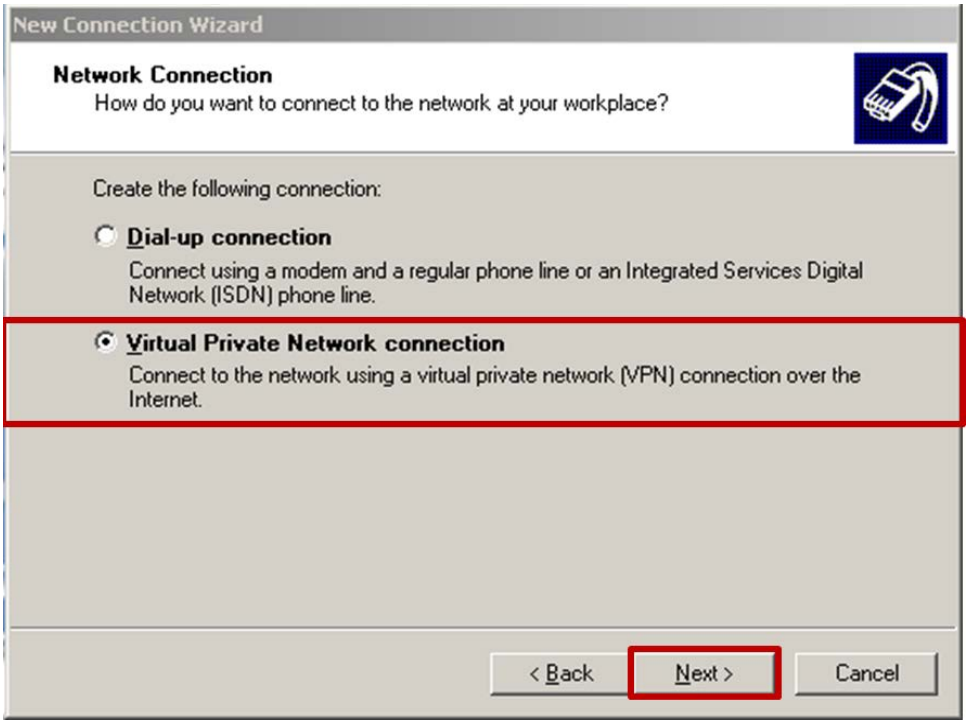


3) The new connection wizard is loaded:

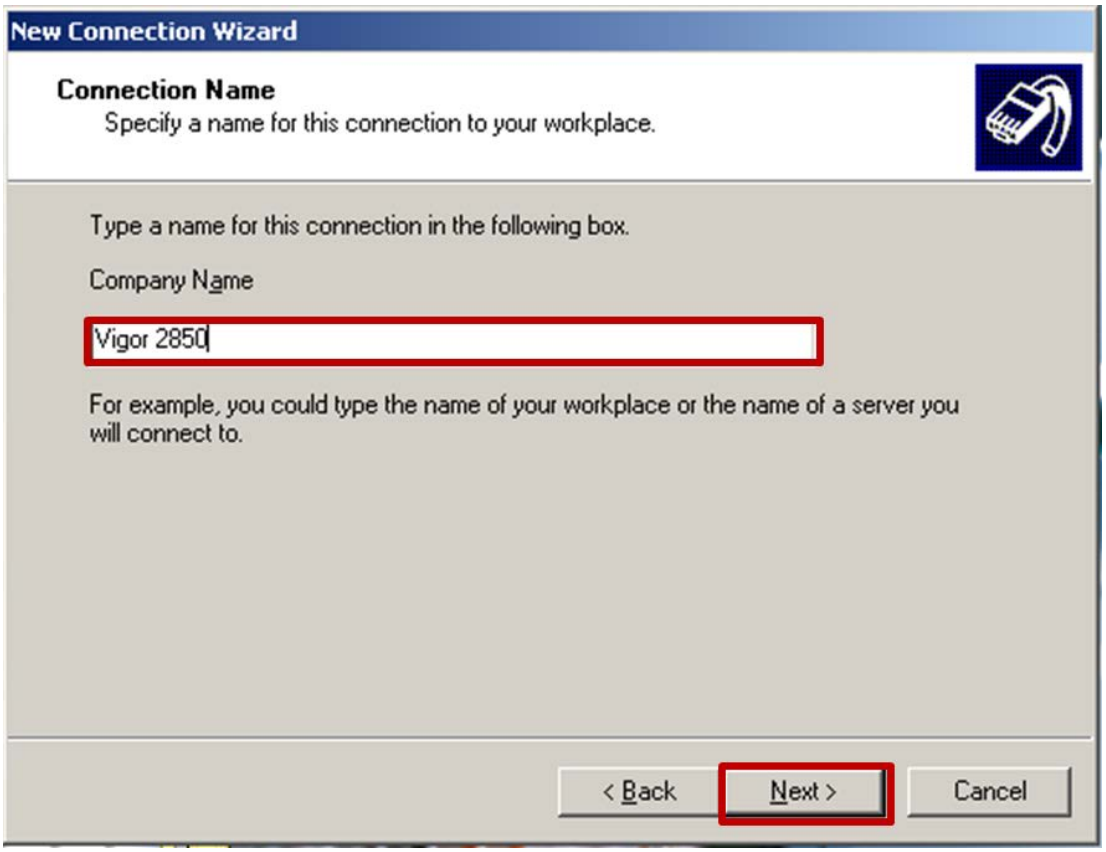
4) Connect to the network at my workplace (VPN):



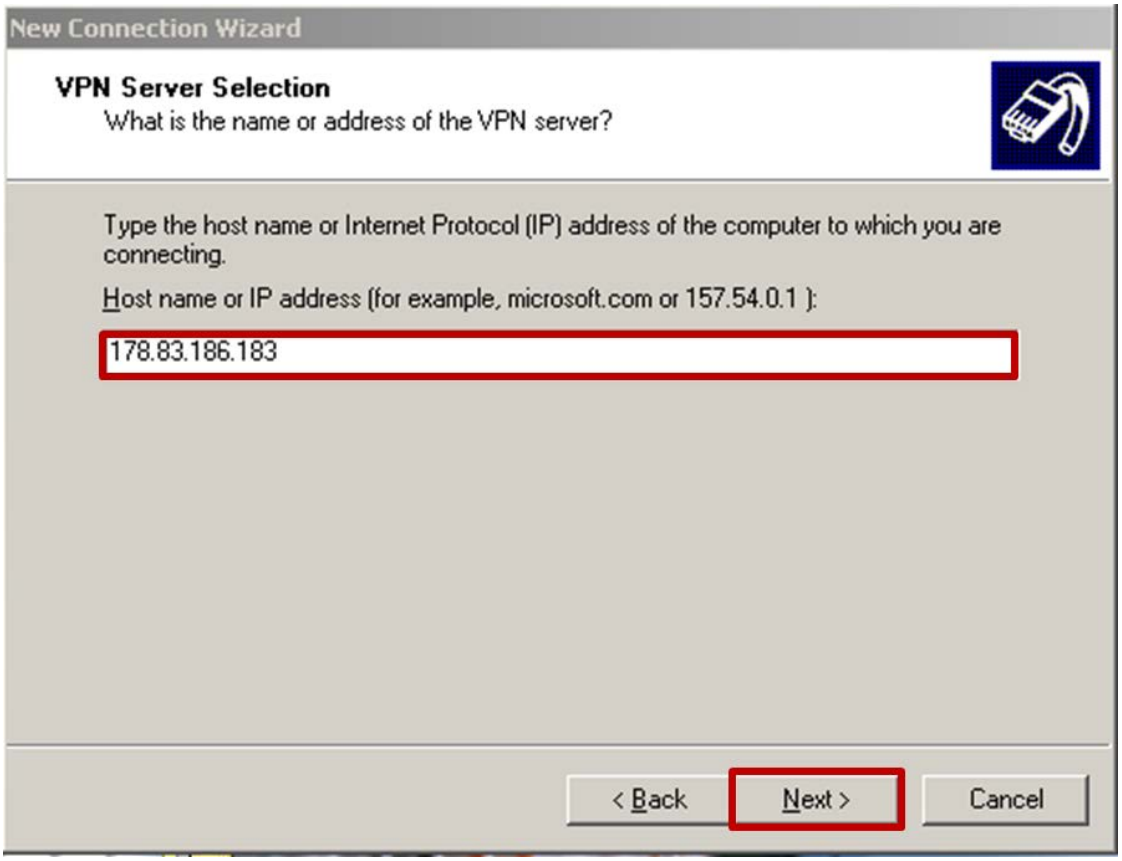
5) Virtual Private Network connection (VPN):



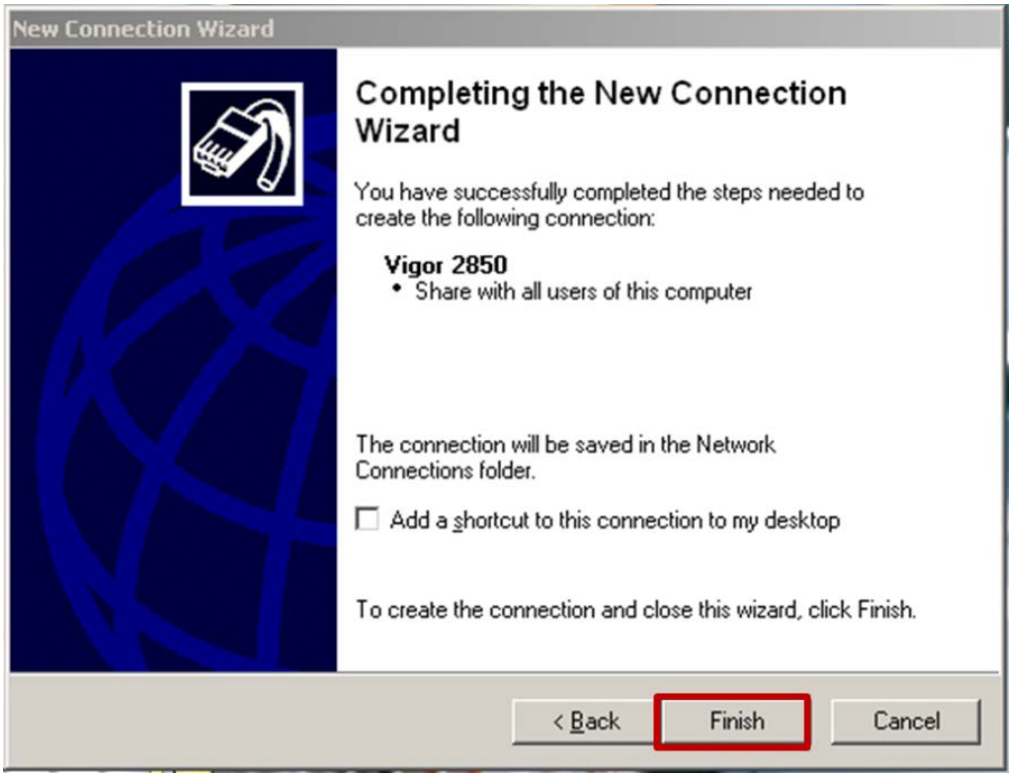
6) Name of VPN:



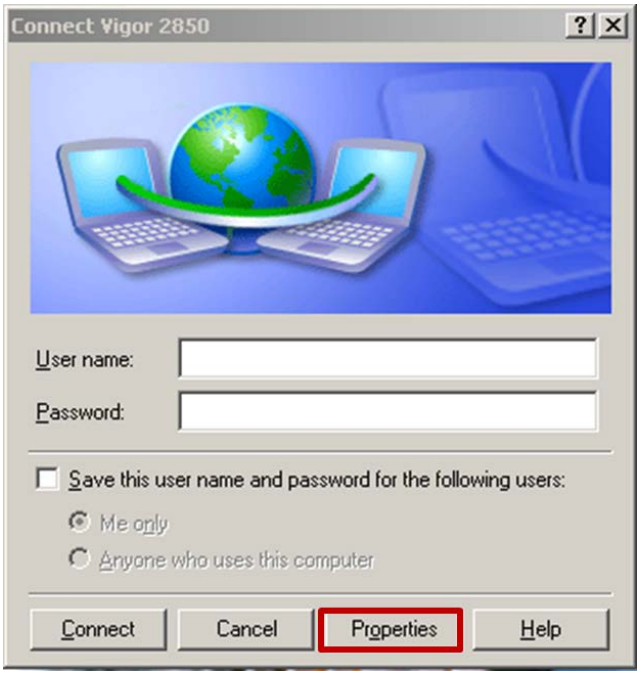
7) VPN server address:



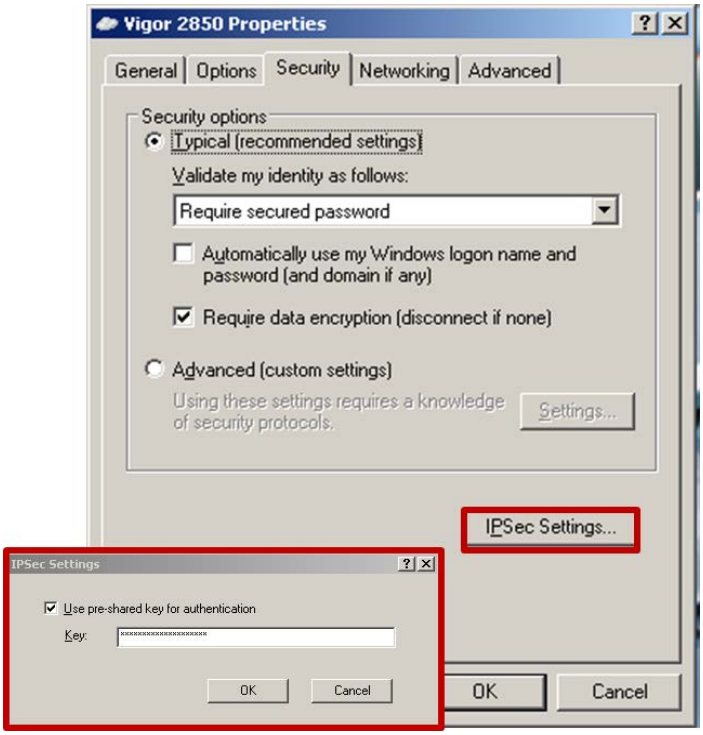
8) Close wizard:



9) Select properties in the connection dialog:

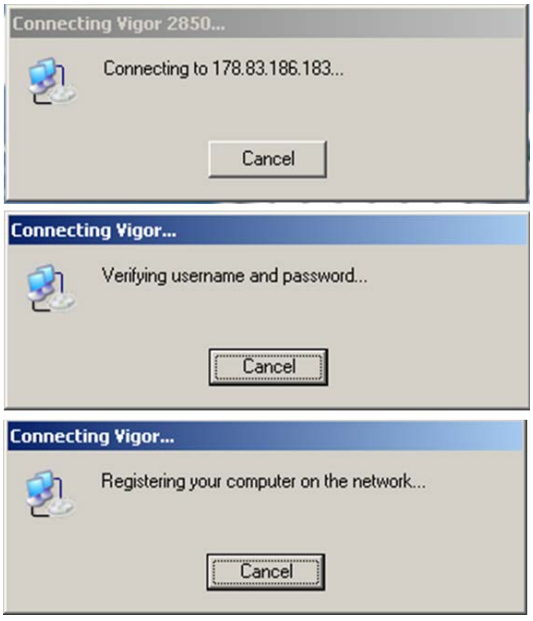


10) Security Tab → IPSec Settings → Enter IPSec key:



11) Enter user name and password of the VPN user:

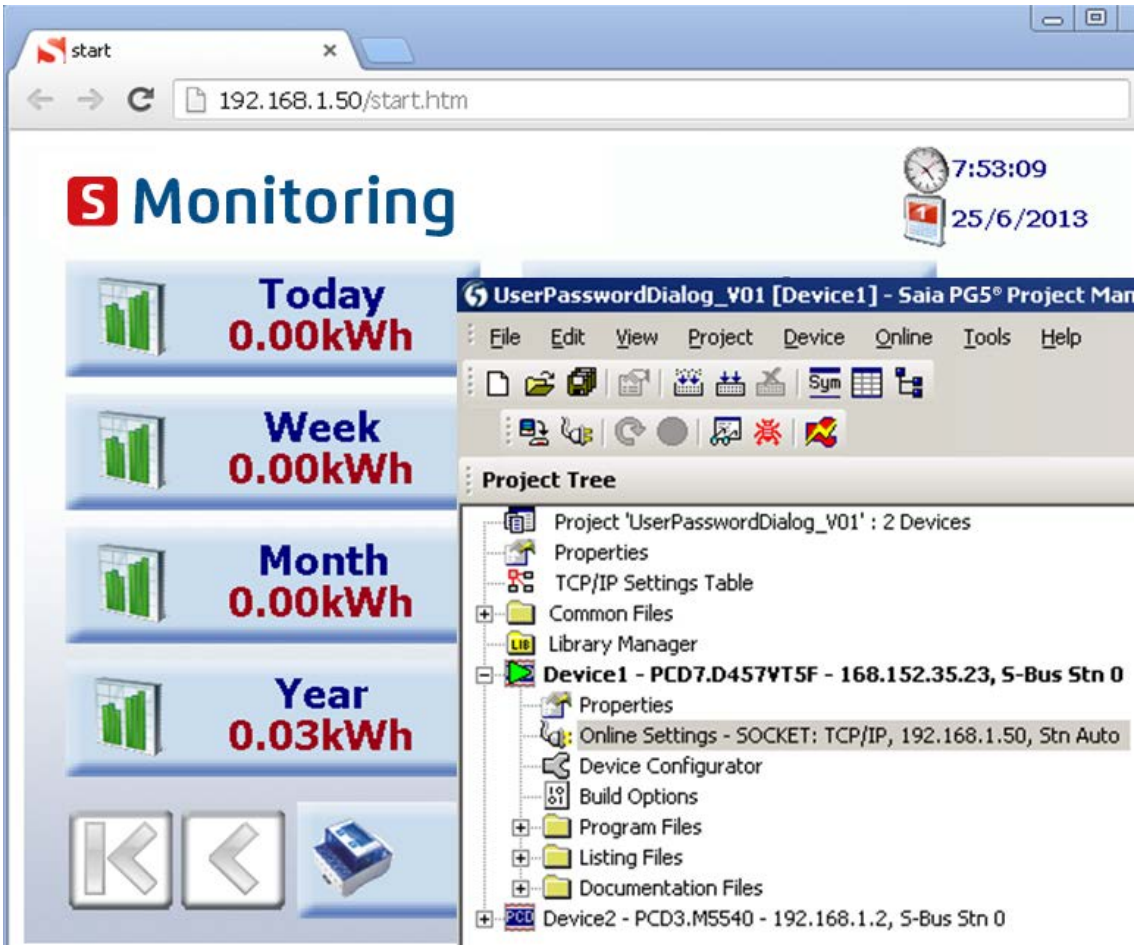
12) Connection was made:



13) The PC is now a member of the remote network. Access to devices is now possible with all applications that support Ethernet:

➔ Browser

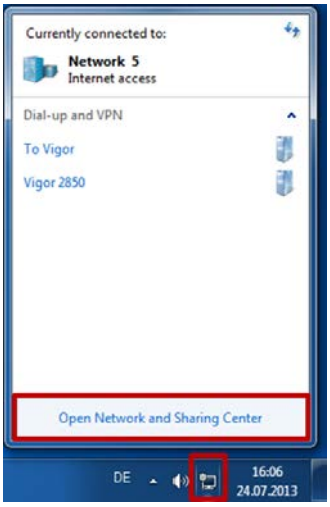
➔ PG 5



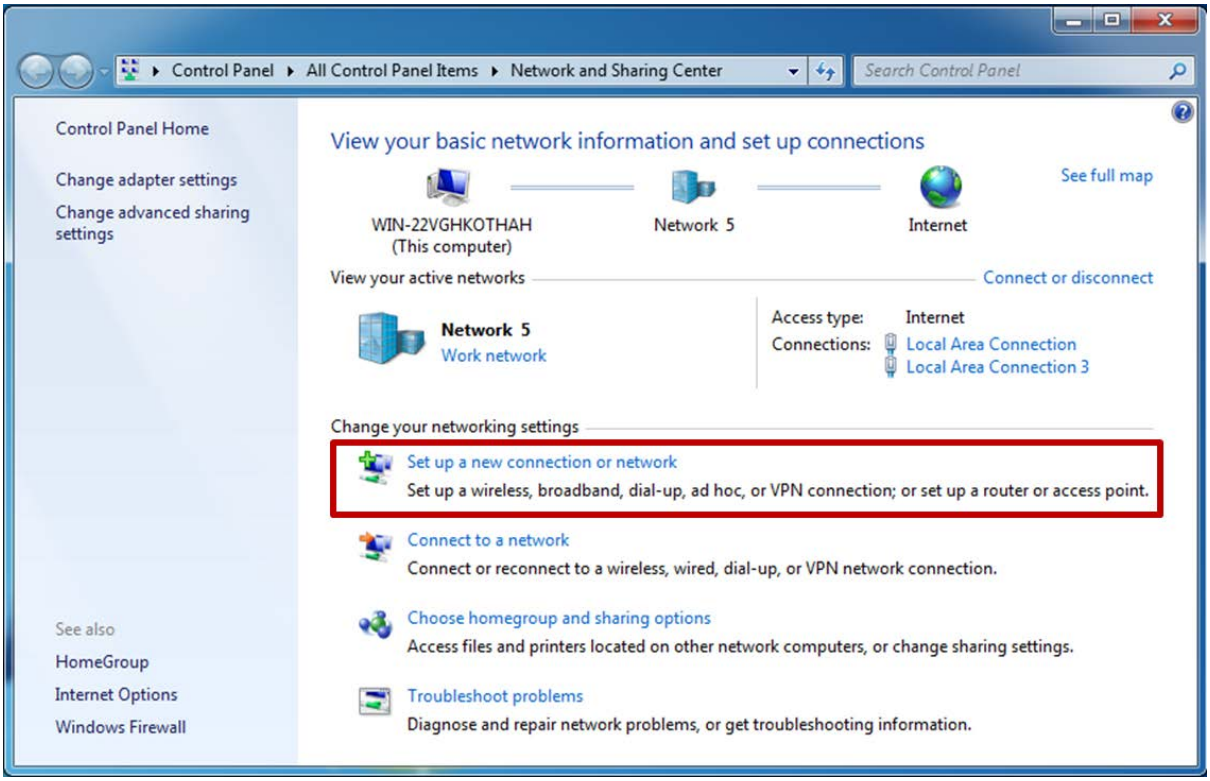
3.8 Microsoft Windows 7 client

Create a VPN connection in a Windows 7 system. Administrative rights are required to set up a VPN connection.

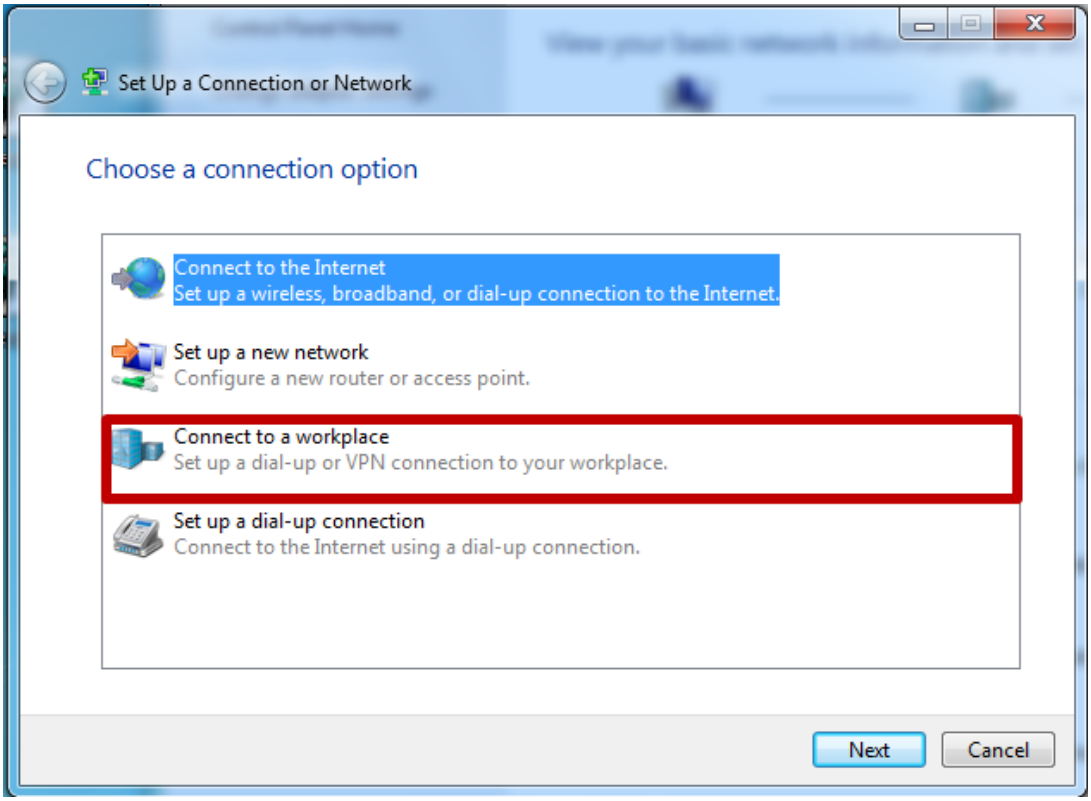
1) Open the Network and Sharing Center:



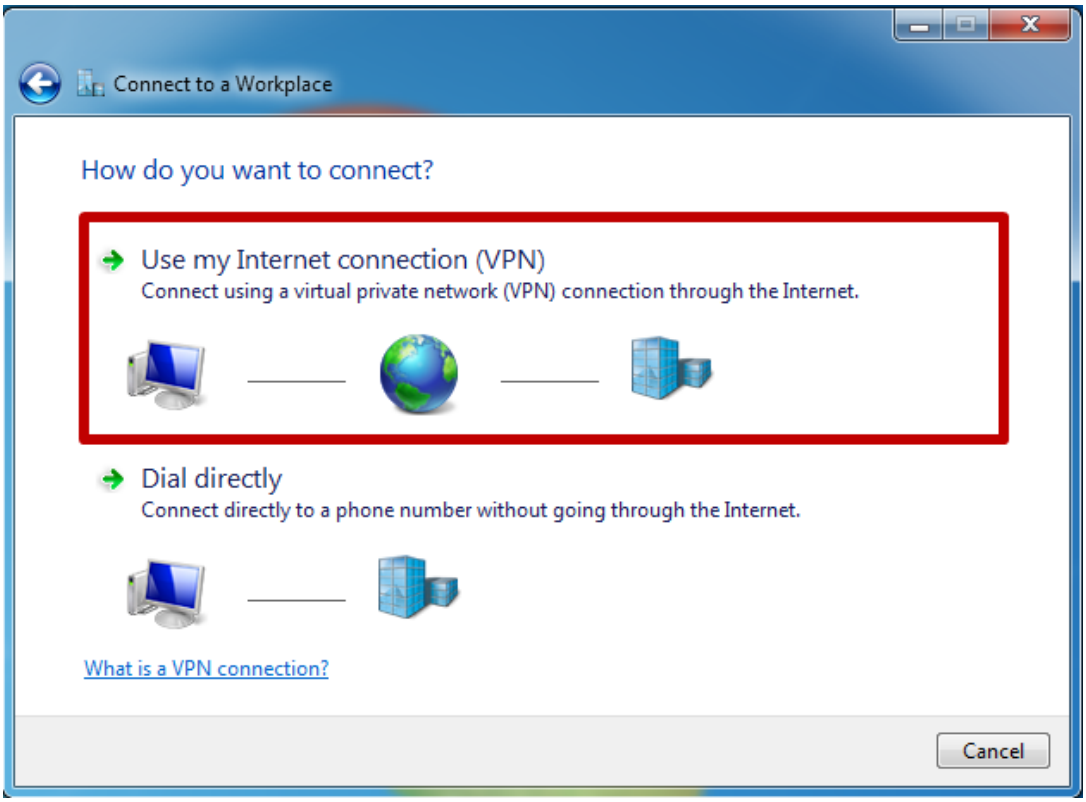
2) Create a new connection to a network:



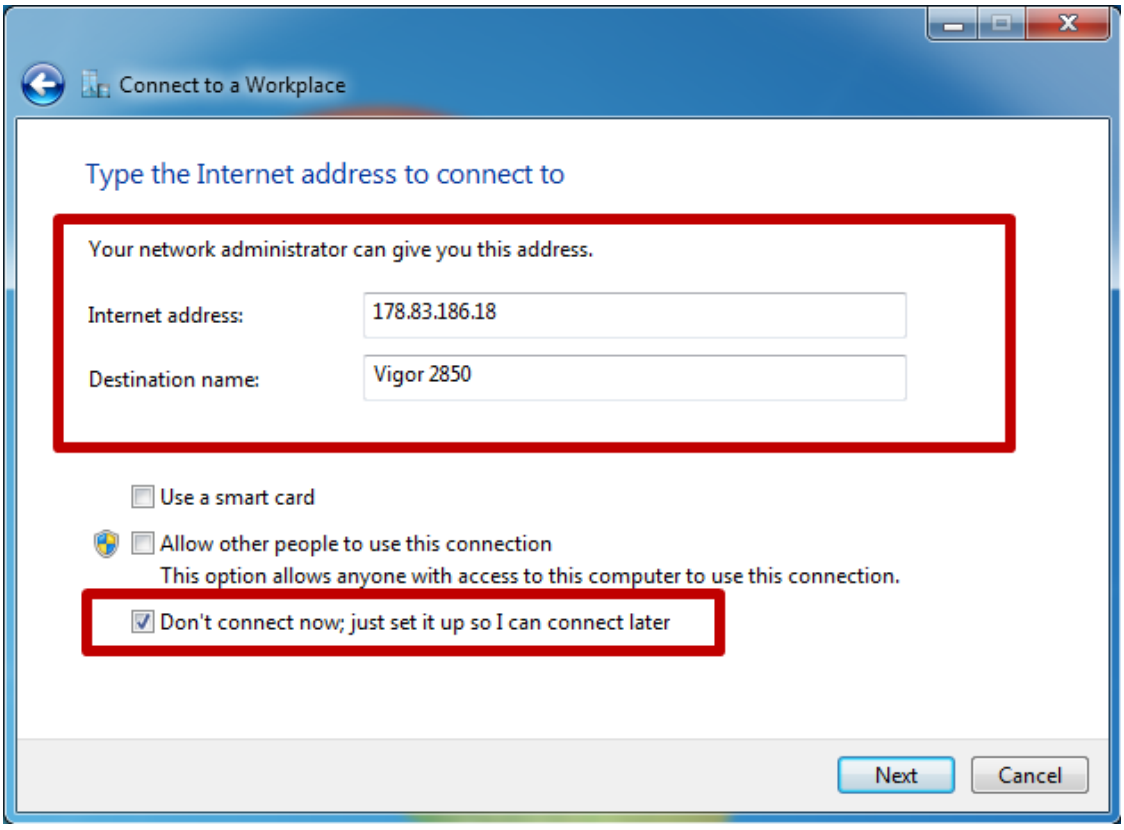
3) Connect to the network at my workplace:



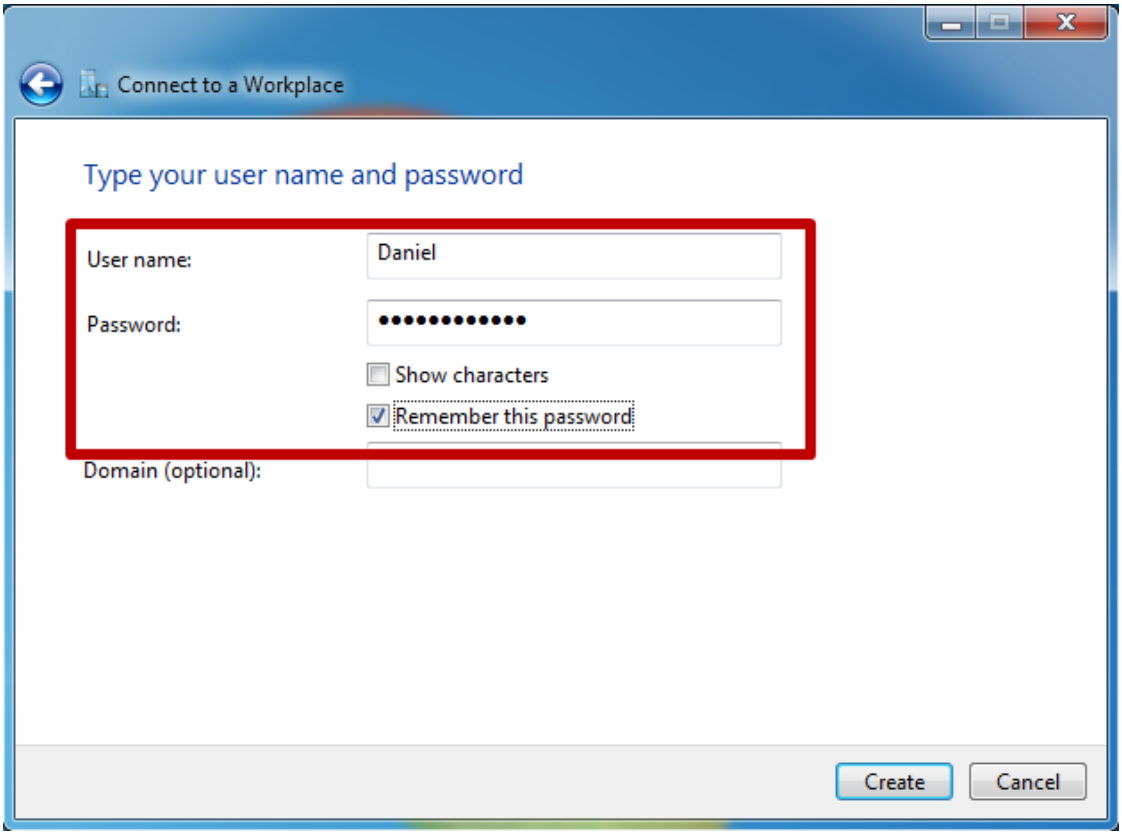
4) Use the internet connection:



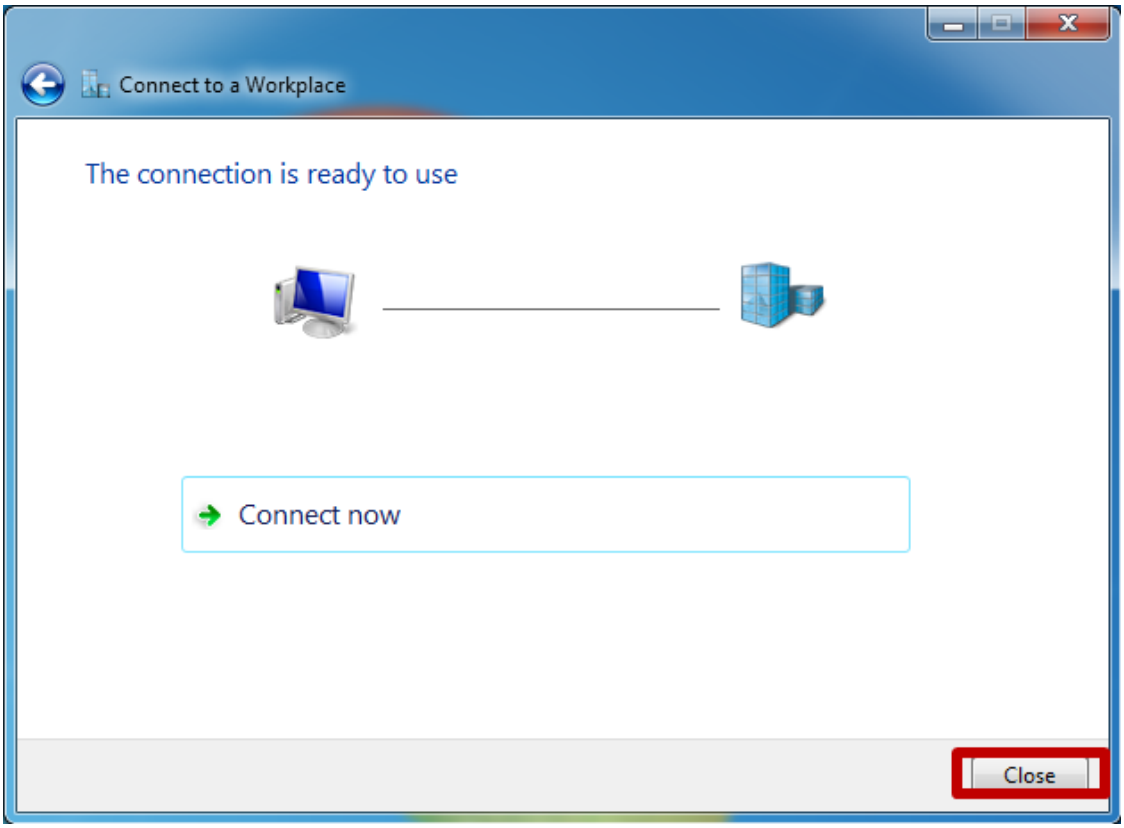
5) Define internet address and name of the connection:



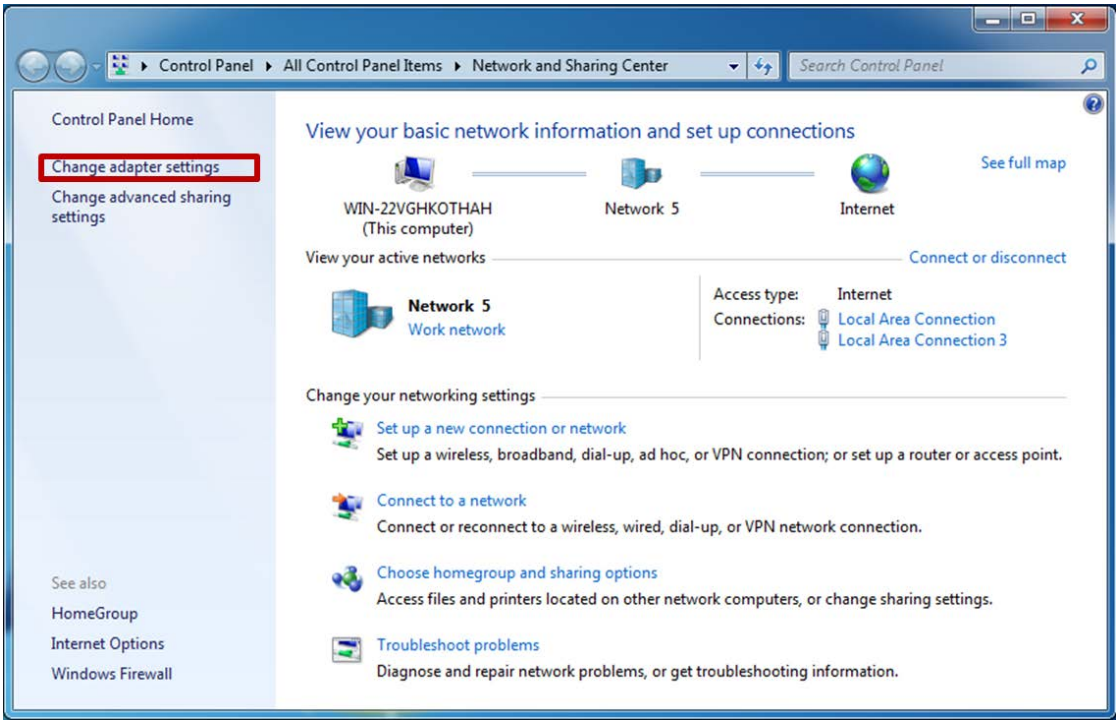
6) Enter user name and password of the VPN server:



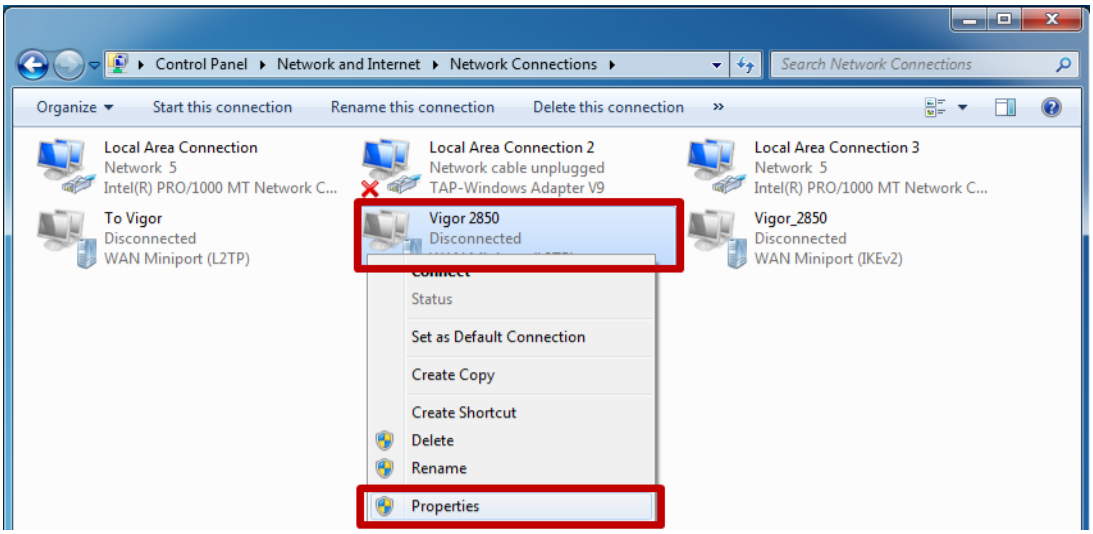
7) Close wizard:



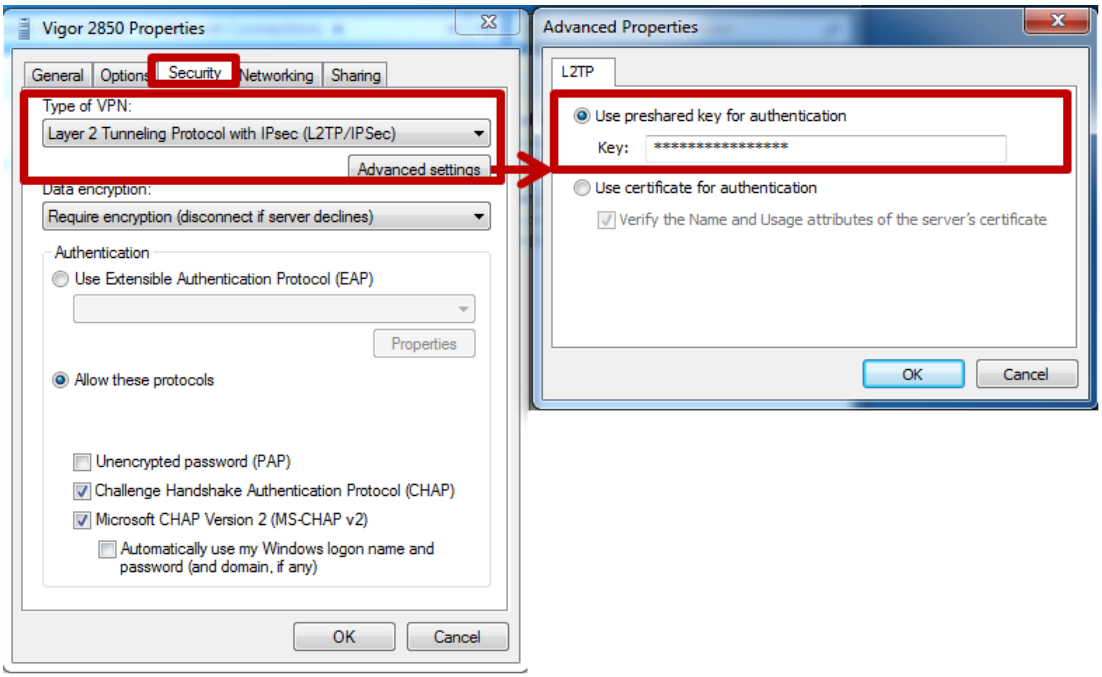
8) Open the Network and Sharing Center → Change adapter settings



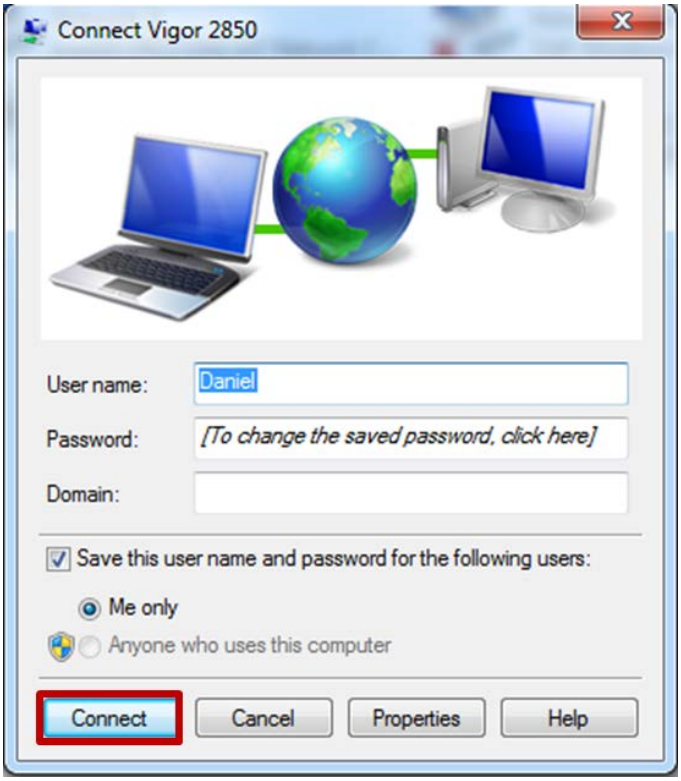
9) Open properties of the VPN connection:



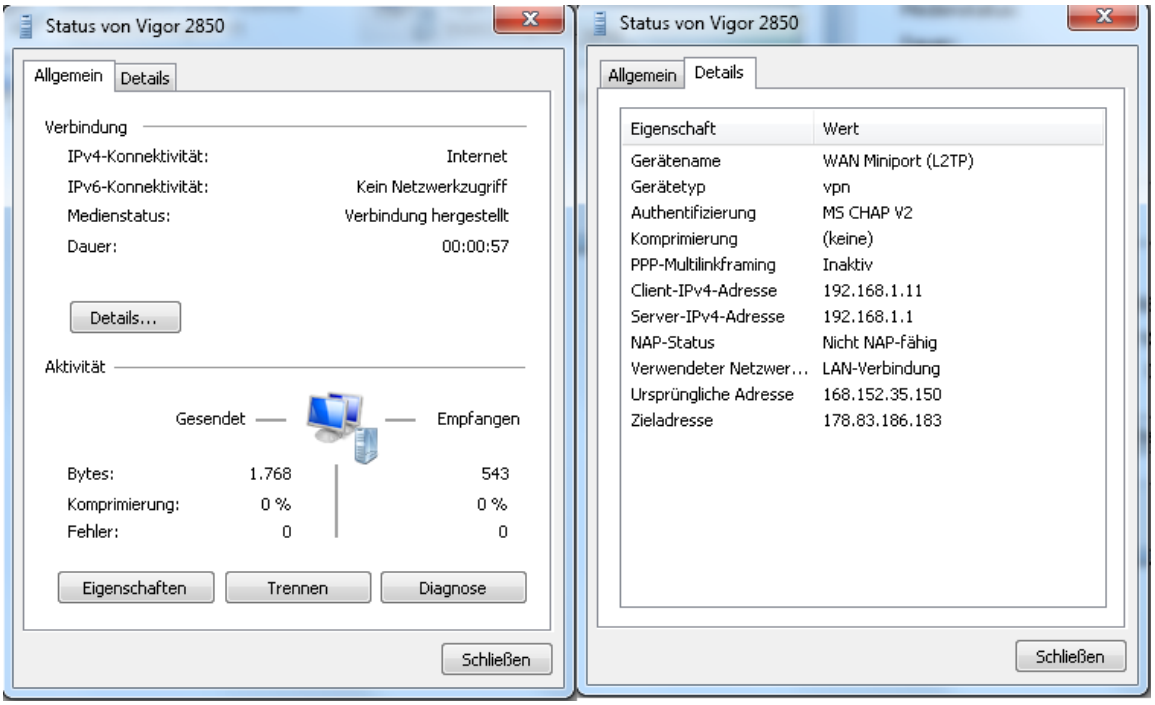
10) Enter L2TP/IPSec connection settings and set the IPSec Pre-Shared Key (PSK):



11) Open the VPN connection and establish the connection.



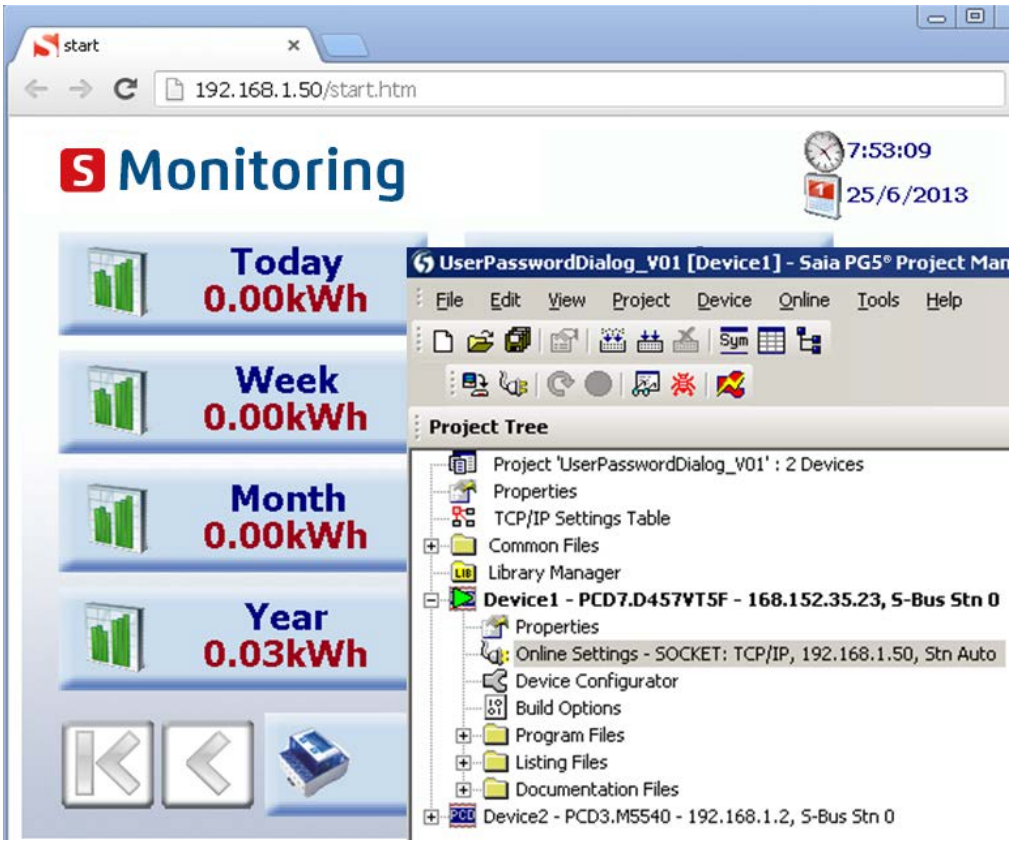
12) The connection was made, IP addresses from the router's DHCP server were assigned



13) The PC is now a member of the remote network. Access to devices is now possible with all applications that support Ethernet.

➔ Browser

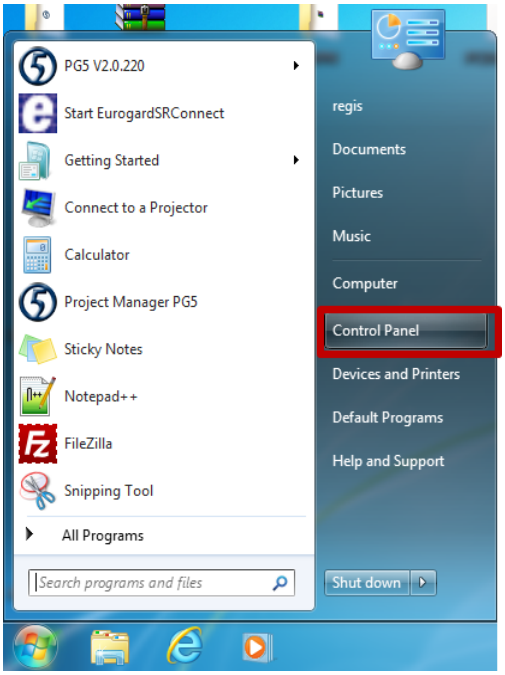
➔ PG 5



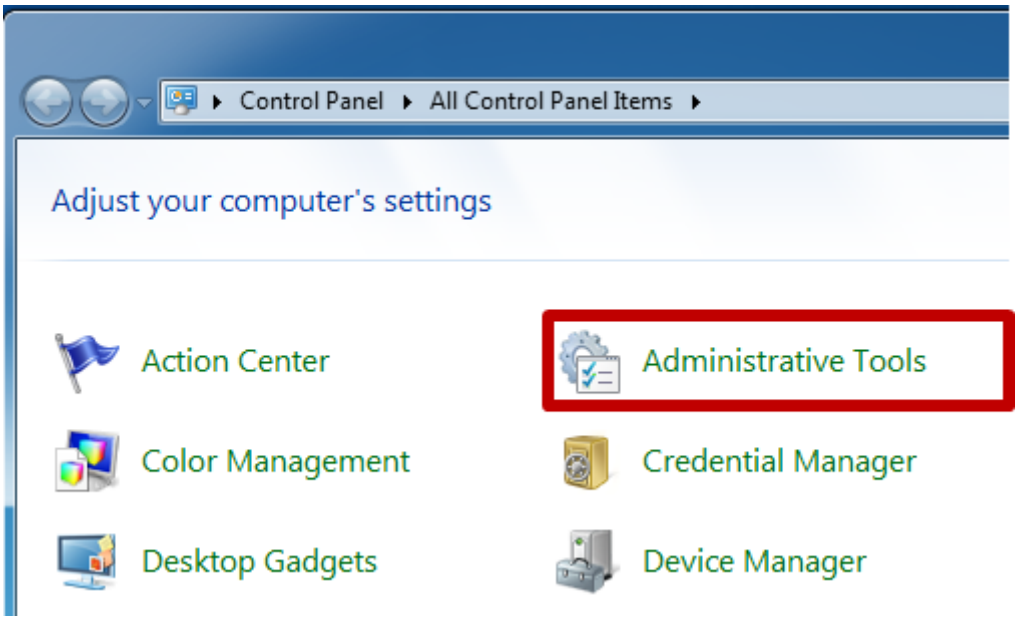
3.9 Windows troubleshooting:

In the event that the connection was not successful, please check the following points and repeat the process starting at number 15. Activate the IPSec Policy Agent and the IKE and AuthIP IPSec keying modules.

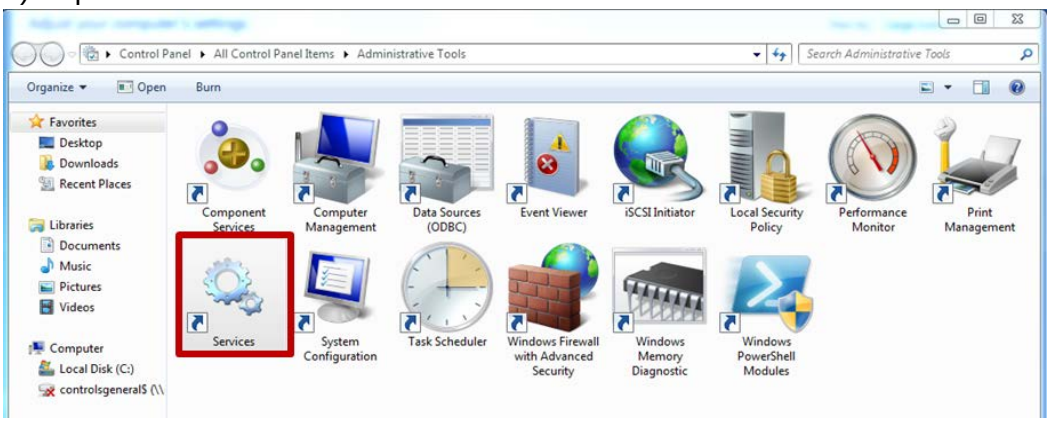
1) Open Control Panel:



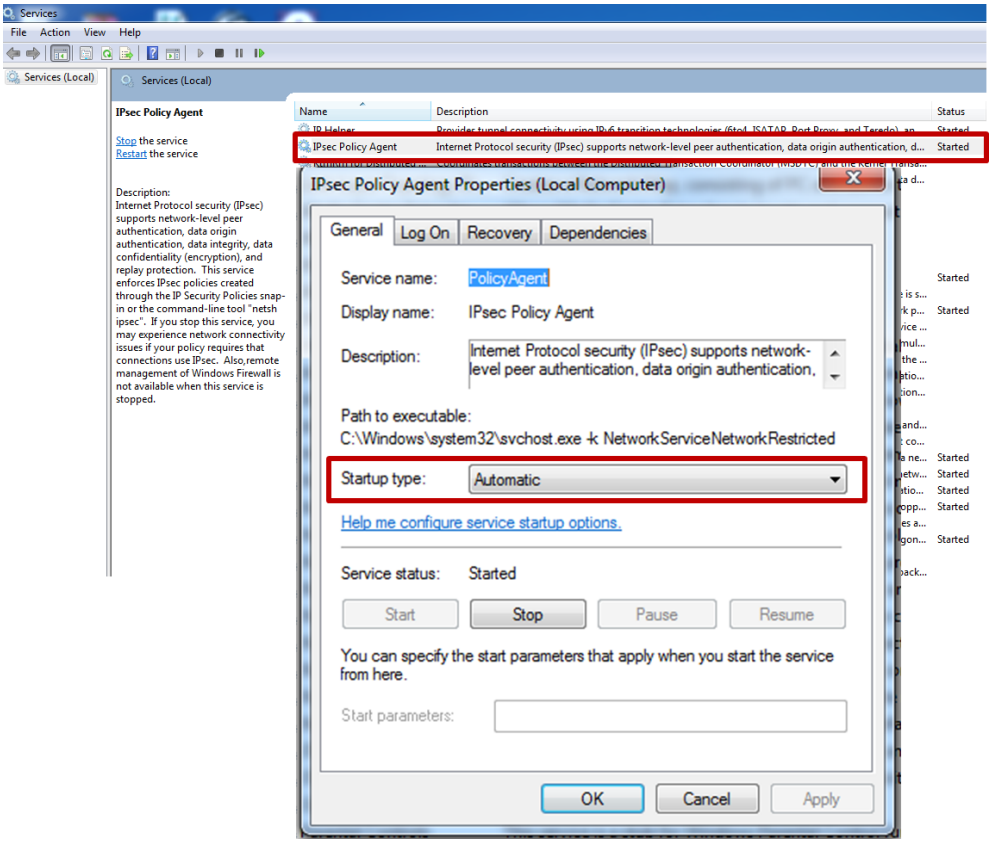
2) Open Management:



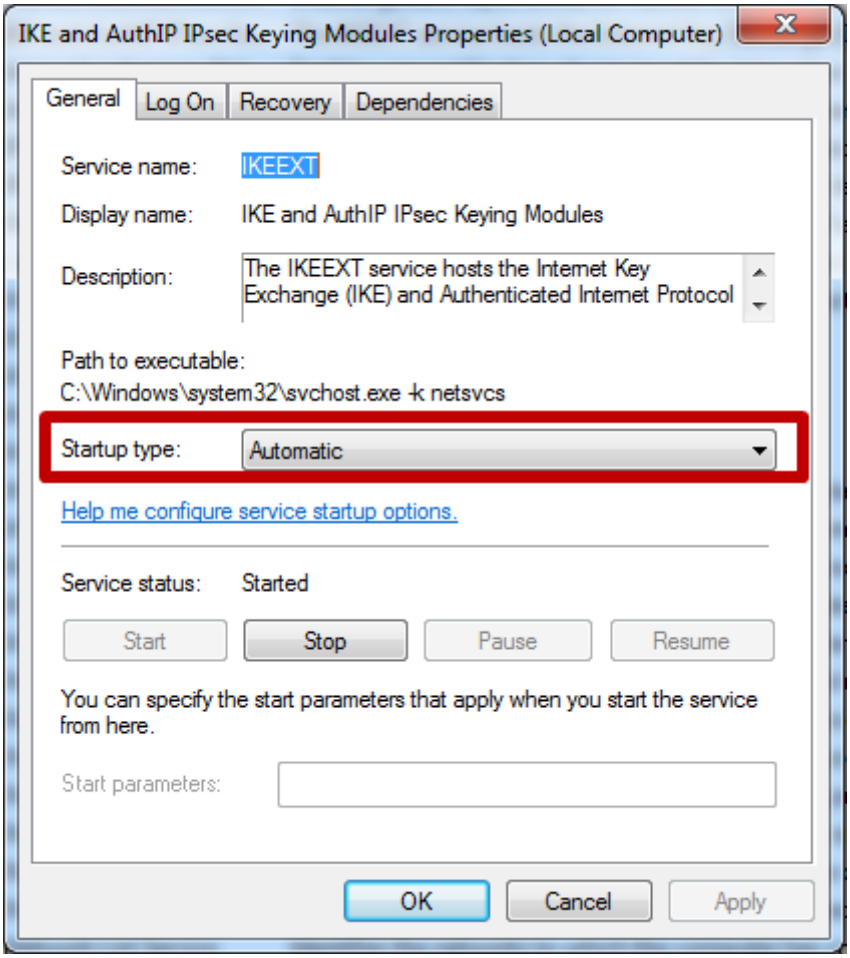
3) Open Services window:



4) Start Services
(IPsec Policy Agent and IKE and AuthIP IPSec keying modules)
   a. IPsec Policy Agent

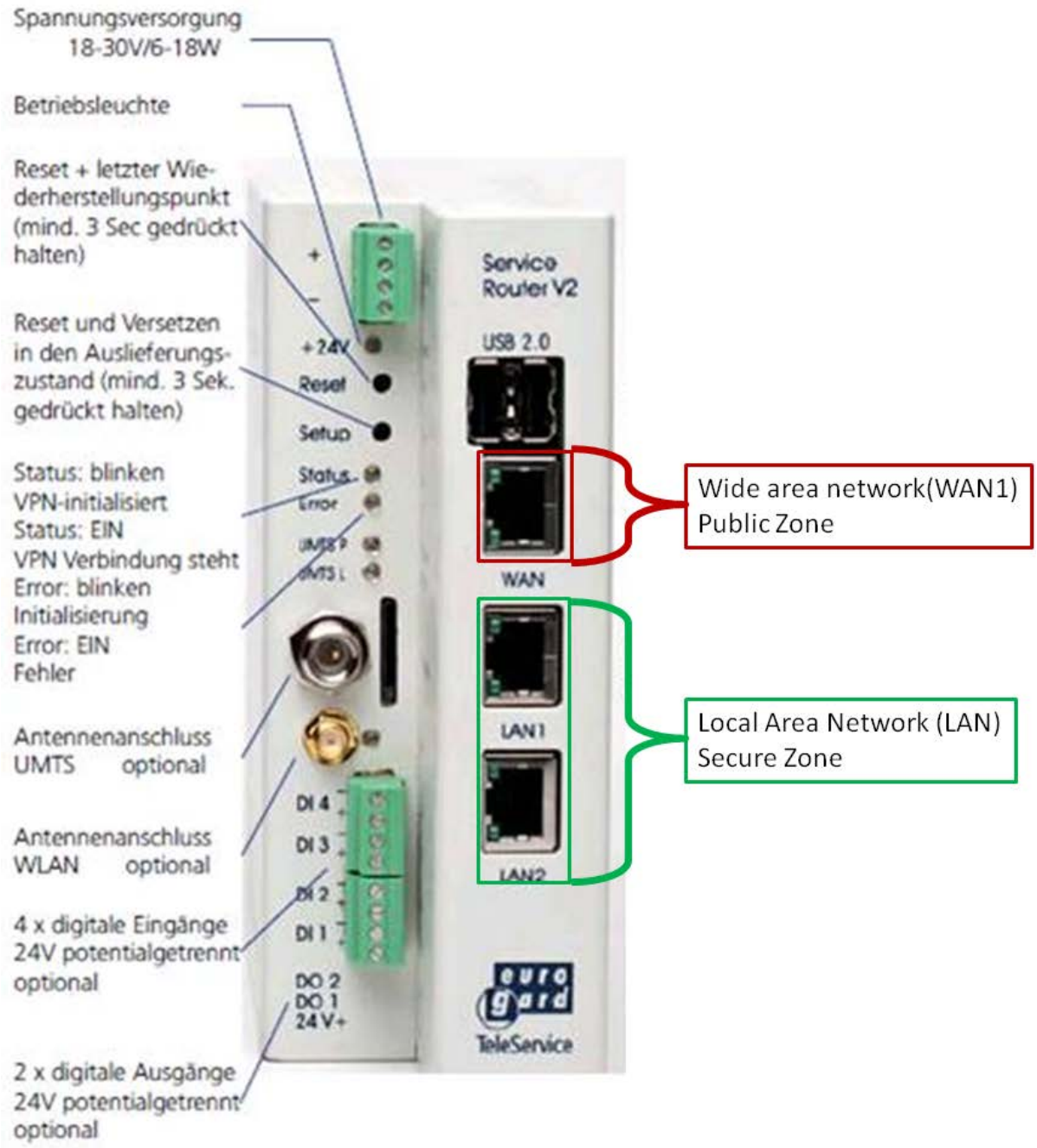


b. IKE and AuthIP IPSec keying modules:



4 EuroGard Service Router 2

The router should always be configured starting with the settings for the local network (LAN) and ending with those for the VPN server. The reason for this is that parameters of the local configuration and system time are used when generating the server certificate in the router.



Wide Area Network (WAN) → Connection to router with public IP address
Local Area Network (LAN) → Connection to local network

4.1 Opening the setup menu

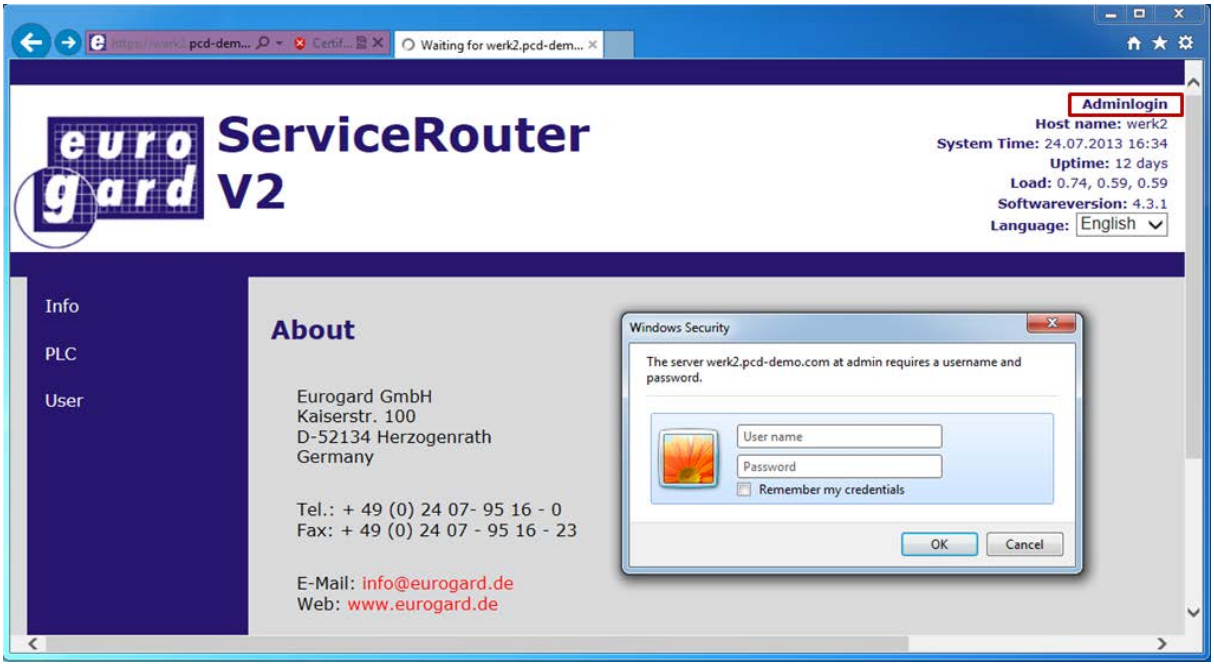
The PC must be connected to the router's LAN interface in order to set up the Eurogard Service Router V2. The router includes an active DHCP server with delivery. Configuring the Eurogard Service Router V2 with a factory configuration in an Ethernet infrastructure with an existing DHCP server should therefore be avoided.

Recommendation:
Disconnect your PC from all existing network connections.
Connect your PC to the router directly.

By default, the factory-set IP address of the router is configured to "192.168.155.1". The router's DHCP server provides the connected PC with an address in the DHCP server's address space.

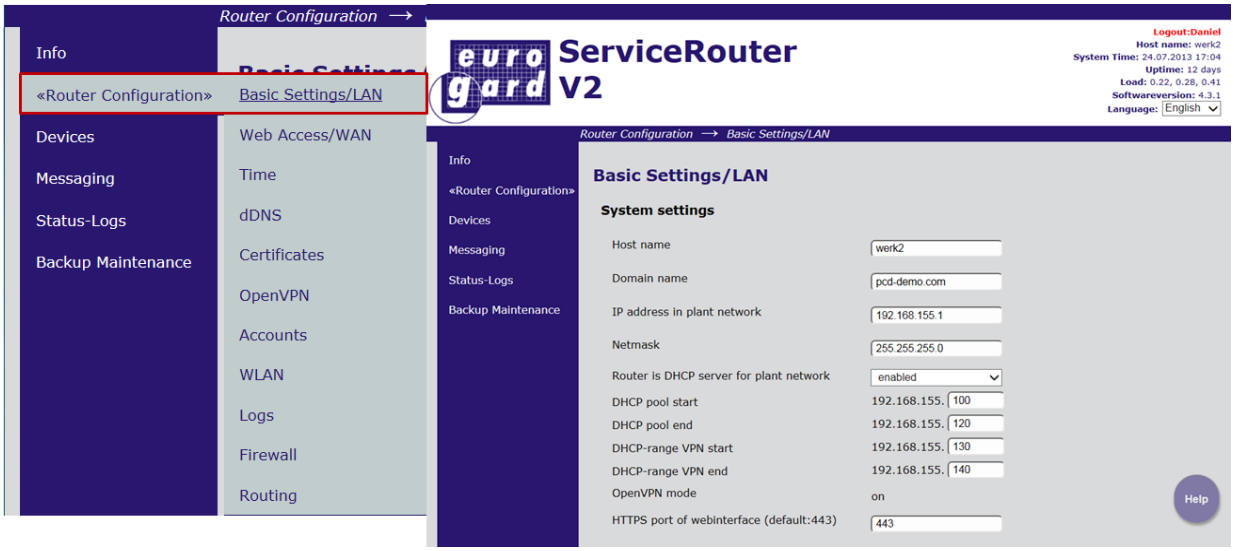
The router is configured in a browser.
To load the configuration interface in the browser, the router's IP address must be entered in the browser.

The Eurogard Service Router V2 is delivered with the factory-set user name "eurogard" and password "eurogard". You can also find user names and passwords in the router manual.



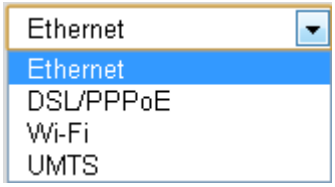
4.2 Configuring the LAN port (Local Area Network)

Open the router configuration and set the basic settings for the local network: Use the addresses in the address space of your existing applications or define a new address space for a new system. At a minimum, the host name, domain name and location should be changed. This is because these entries are later used in generating the server certificate. The domain name is later entered in this certificate as the connection name to the VPN server.



4.3 Configuring the WAN port (Wide Area Network)

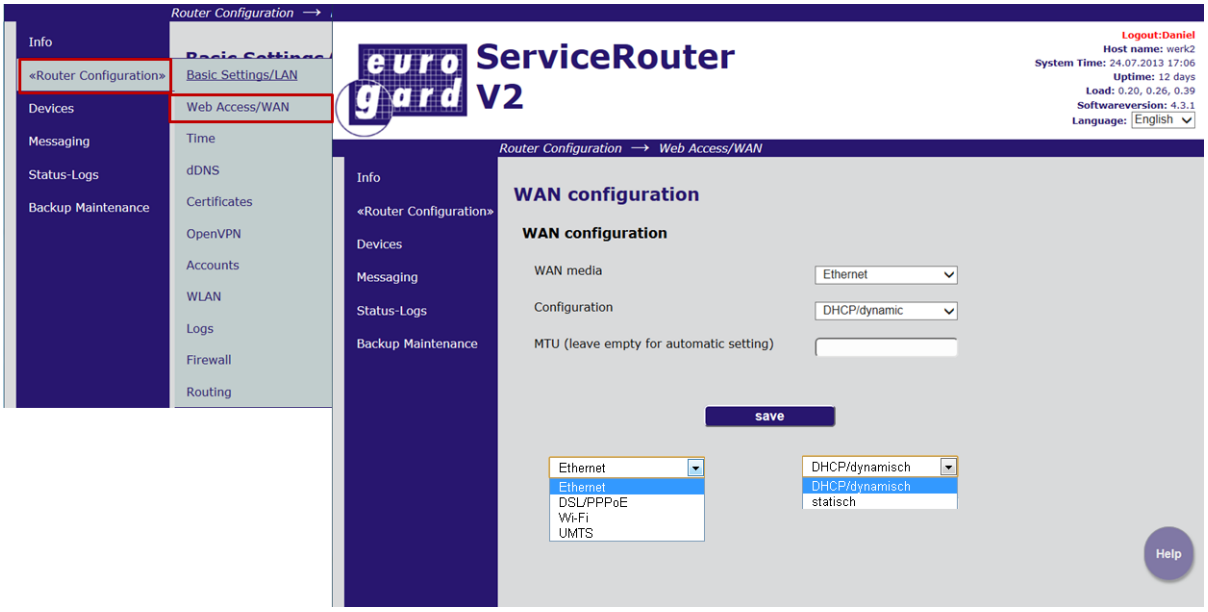
The Eurogard Service Router V2 allows 4 different WAN ports to be configured.



1) Ethernet →
   This configuration allows the router to be operated behind an existing router. In doing so, the existing router provides the connection to the ISP.
2) DSL/PPPoE → (an external ADSL/VDSL modem is required)
   this configuration enables the router to be directly connected to an ADSL/VDSL modem. The ISP's configuration parameters are needed for this type of connection.
3) UMTS →
   This configuration allows use of the integrated UMTS modem to establish a connection to an ISP. The ISP's configuration parameters are needed for this type of connection.
   Please note: In this configuration (UMTS), the router can only be operated as a VPN client.

4.3.1 WAN over Ethernet

If you are using an internet connection that already exists.
DHCP: The IP address of the device is acquired from the DHCP server at the WAN interface.
Statically: The IP address is permanently defined.

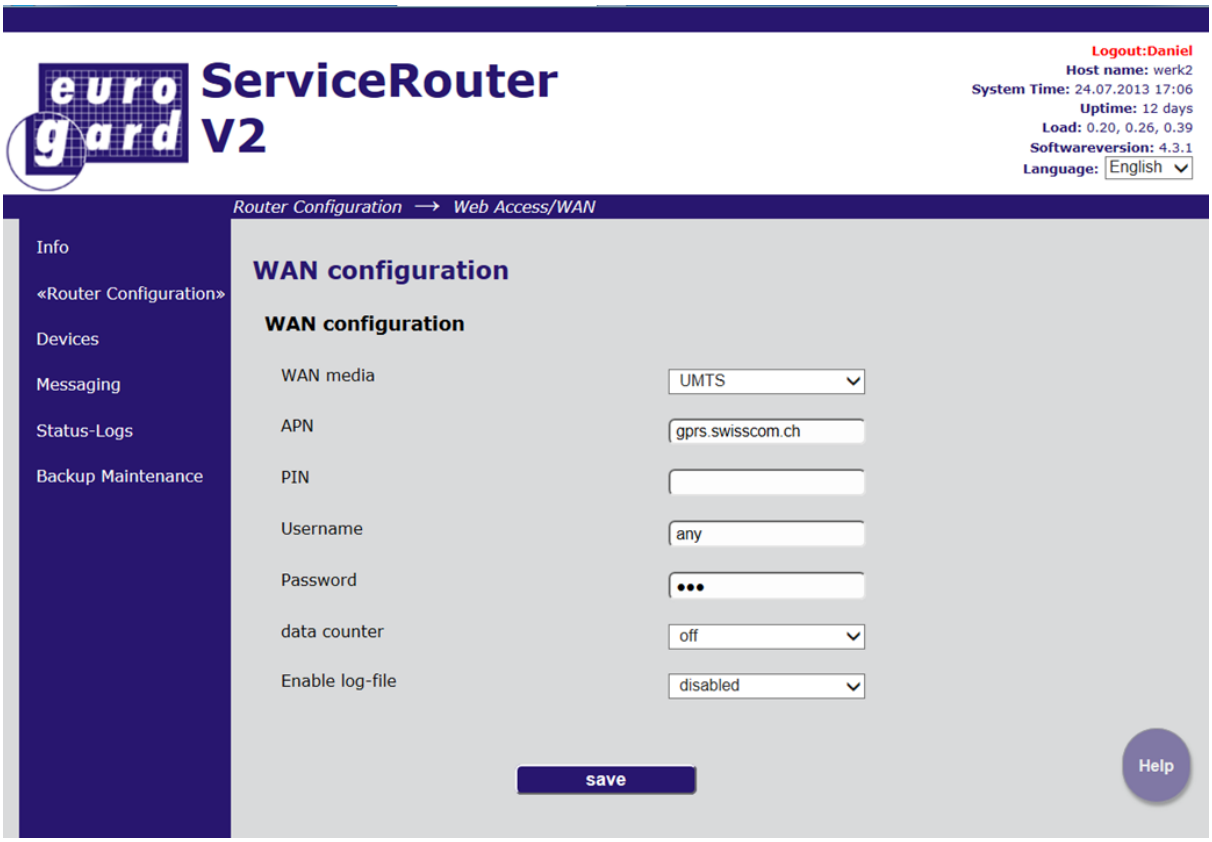


4.3.2 WAN over UMTS

If the router is equipped with an integrated UMTS modem, the UMTS modem can be used as a WAN interface.

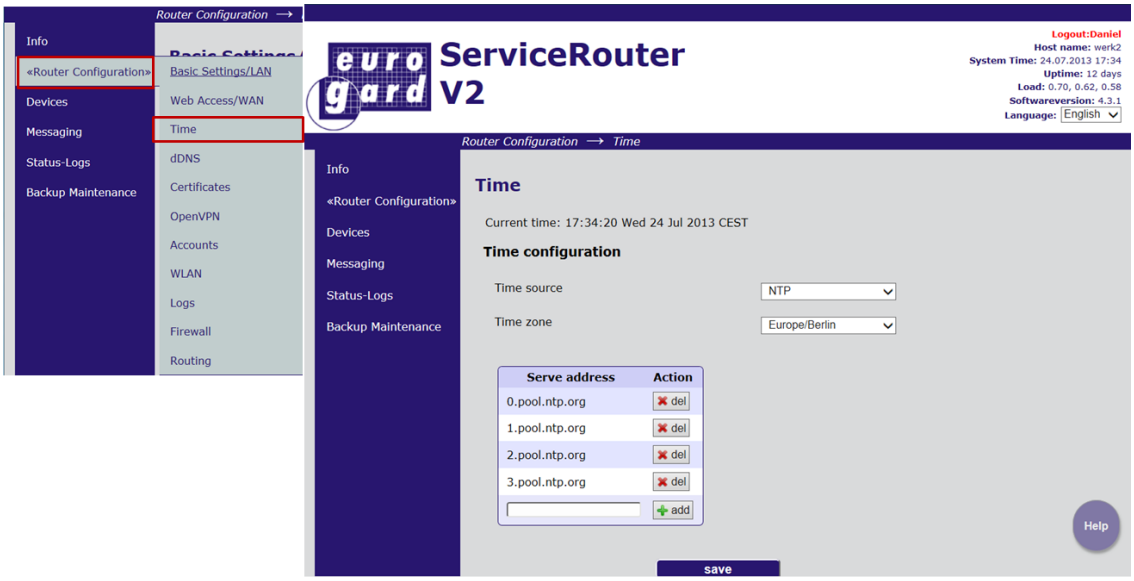
Please note that a connection via UMTS supports only VPN client functionalities. In doing so, the router cannot be used as a VPN server.

The parameters required to dial in are provided by your ISP.



4.4 Time configuration

Before the certificate is generated, the time of the router must be checked and, if necessary, the time server activated or the time manually set.



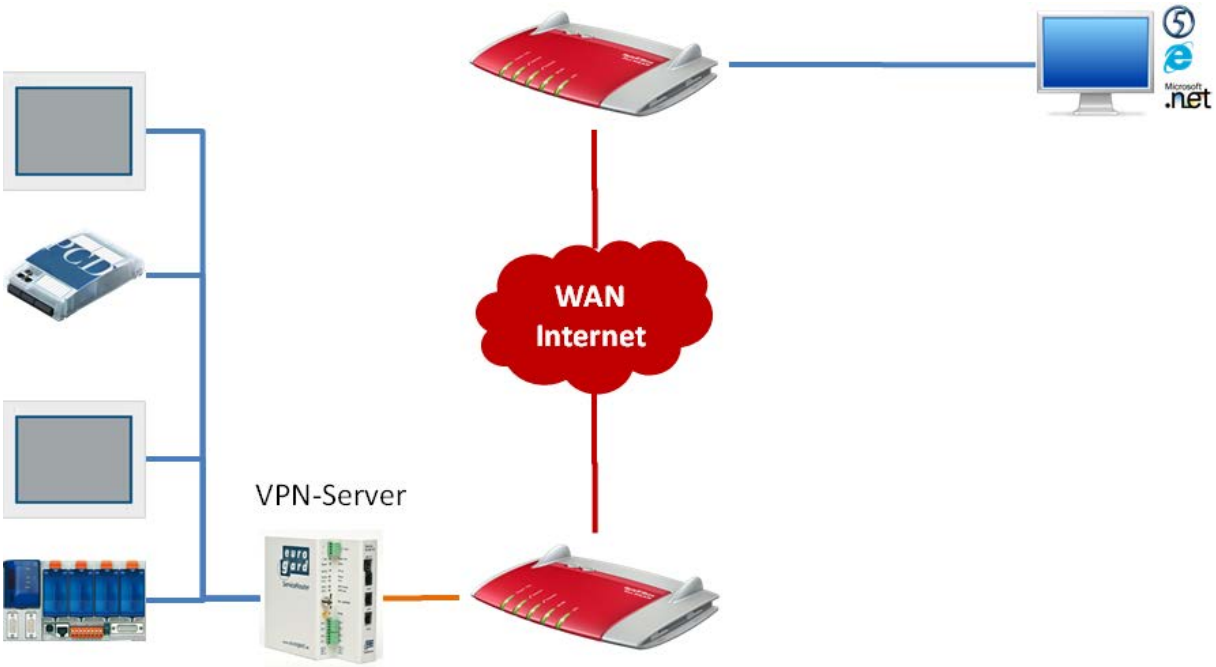
4.5 Generate server certificate

To generate the server certificate, the information provided in the steps above are also used as additional parameters, which you need to add on the page “Certificate”. It is therefore important that the above steps are completed before generating the certificate.

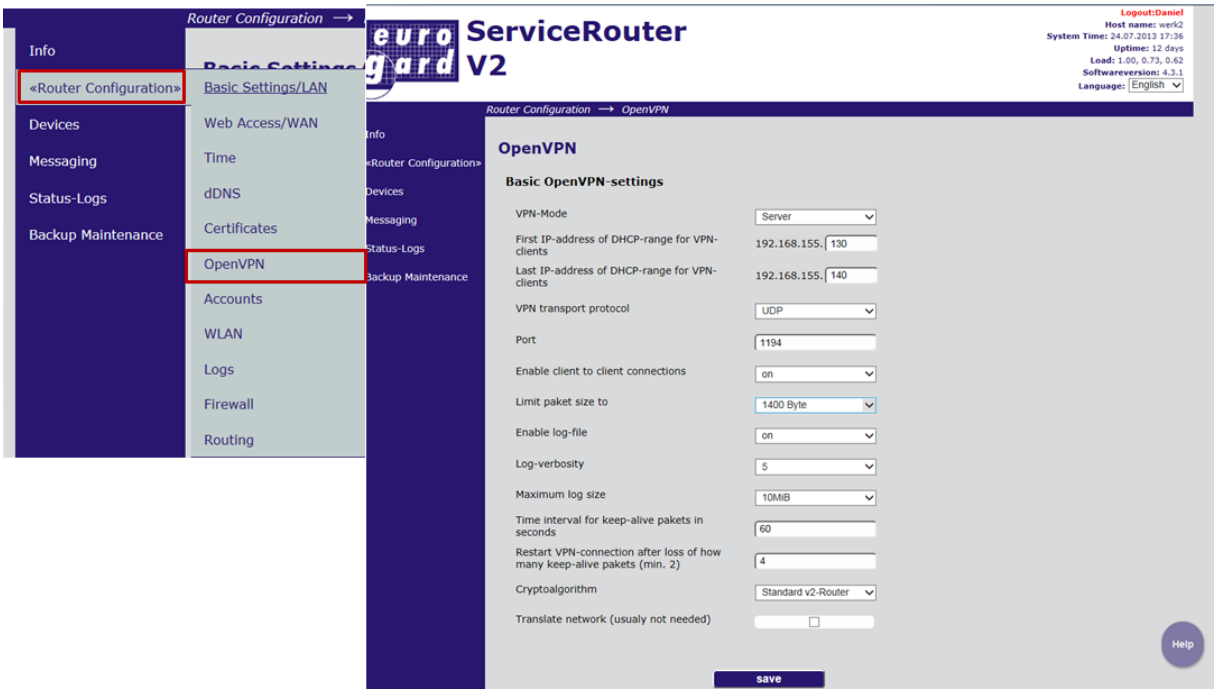
4.6 Activating the openVPN server

4.6.1 VPN mode server

The server must be activated in order to activate the VPN functionality. In addition, the IP address range within which the VPN client will receive an IP address from the VPN client should be defined.



Please note:
An IP address should not be statically configured in the range of the VPN client IP addresses.

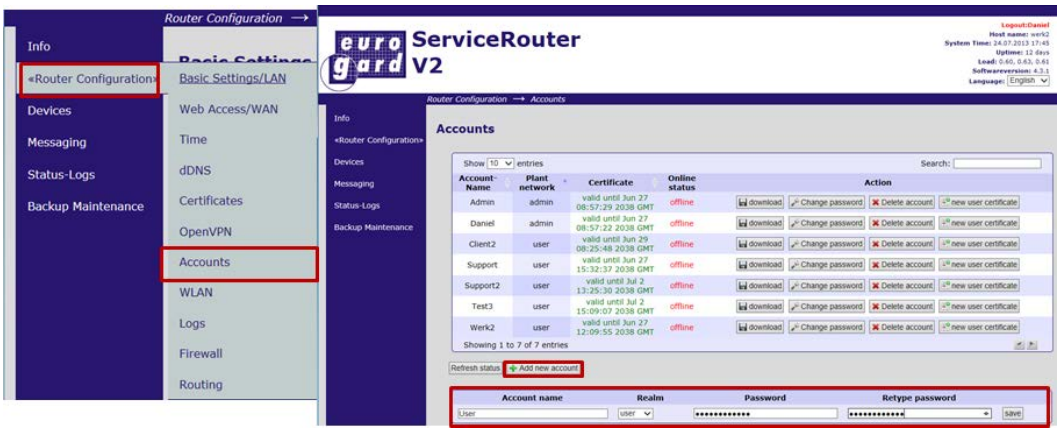


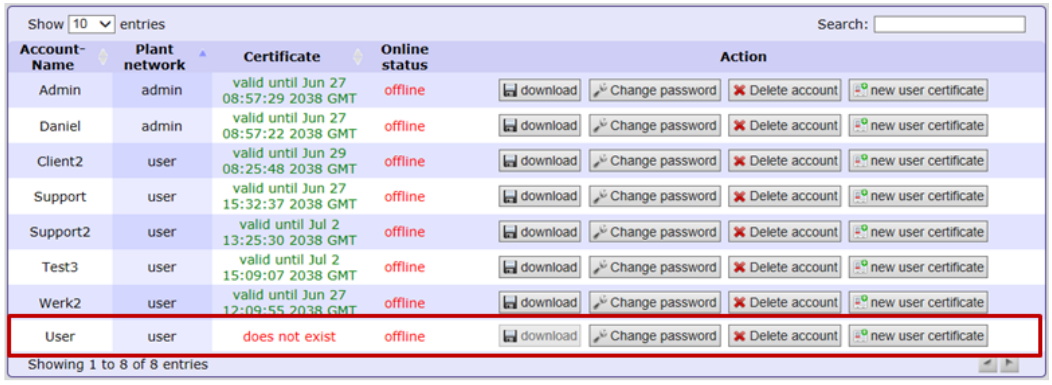
In most cases, the default values do not need to be changed.

4.6.2 Create accesses

Create a new access. Every client requires access and the certificate associated with it. In doing so, the “group” (see figure below) represents what rights that access has. The group “user” has no rights to change the router configuration. However, it can connect as a VPN client or via the SSL proxy server. “Admin”, on the other hand, can authorize access to modify the router configuration.

- ➔ New access (entry of user name, group and password)
- ➔ New certificate → Create client certificate.
- ➔ Download of certificate required for access.

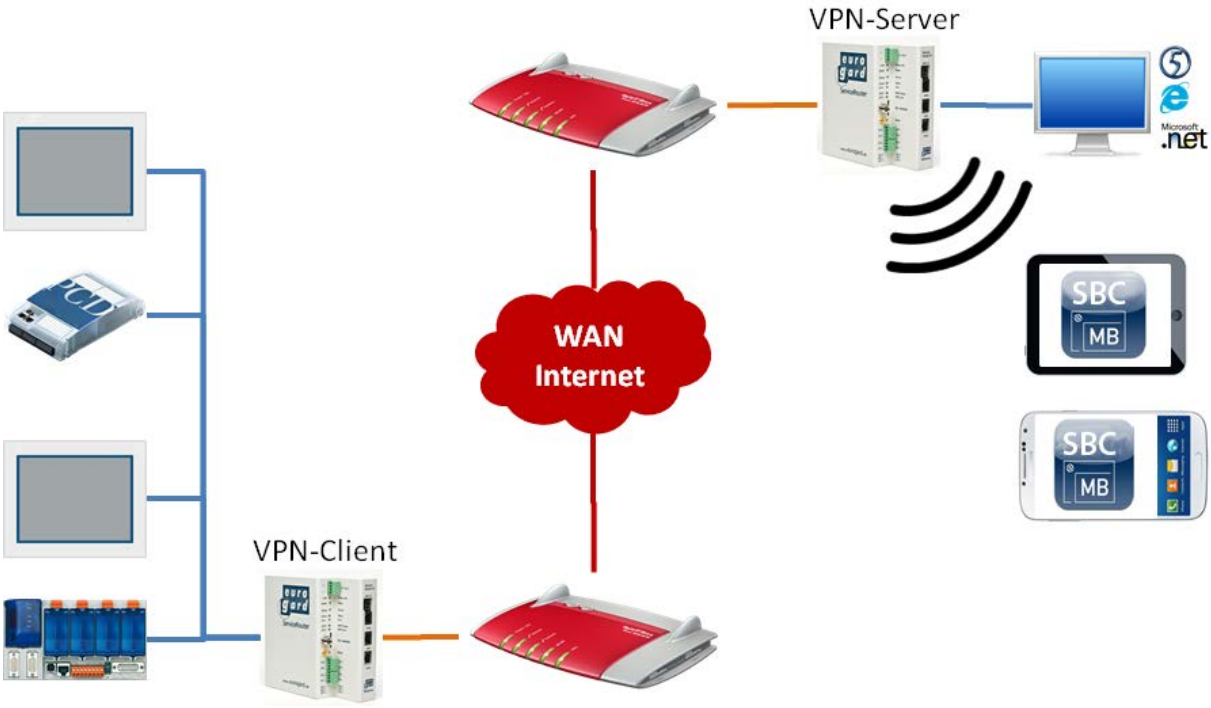




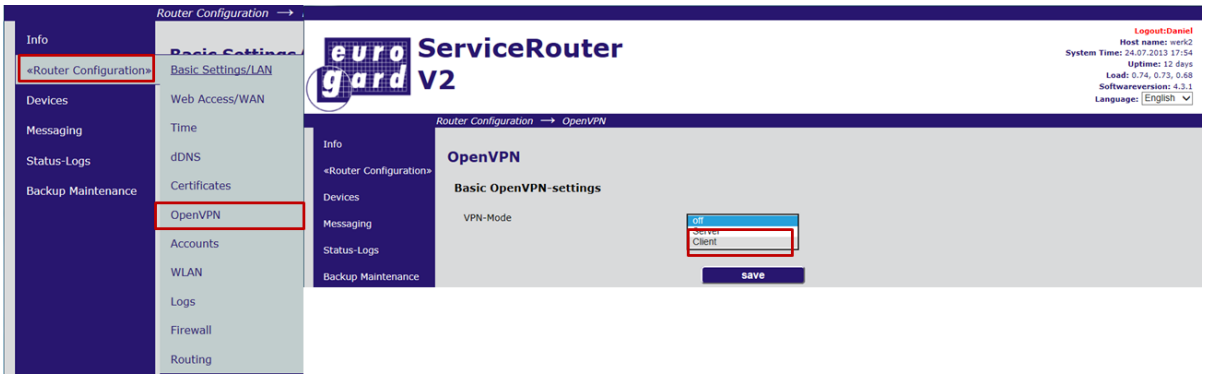
Please note:
When creating a new server certificate, all client certificates must be also be regenerated.

5 EuroGard Service Router 2 VPN Client

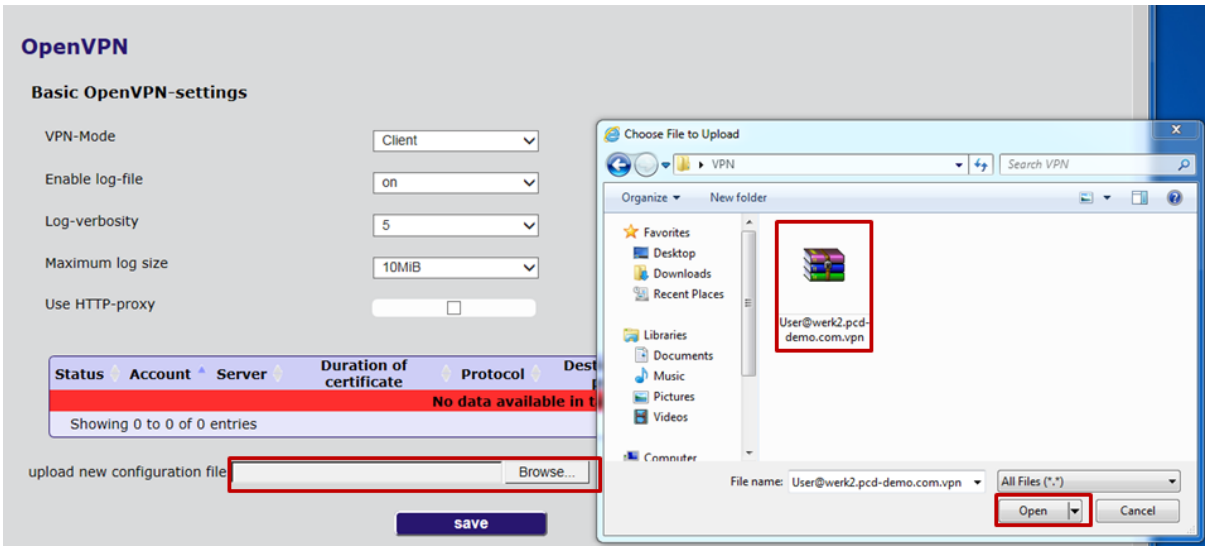
The EuroGard Service Router can also be used as a VPN client:



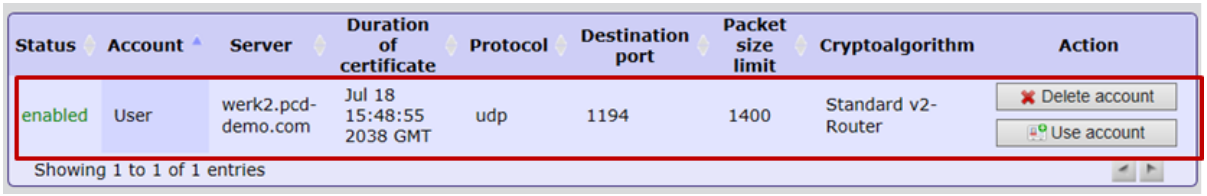
1) A EuroGard router is likewise employed as the VPN server. Configuring OpenVPN access as a client:



2) Load the certificate generated by the server when creating the accesses. This certificate contains all keys and information for establishing the connection to the VPN server.



3) The VPN server is entered in the table. Activate access in the list.



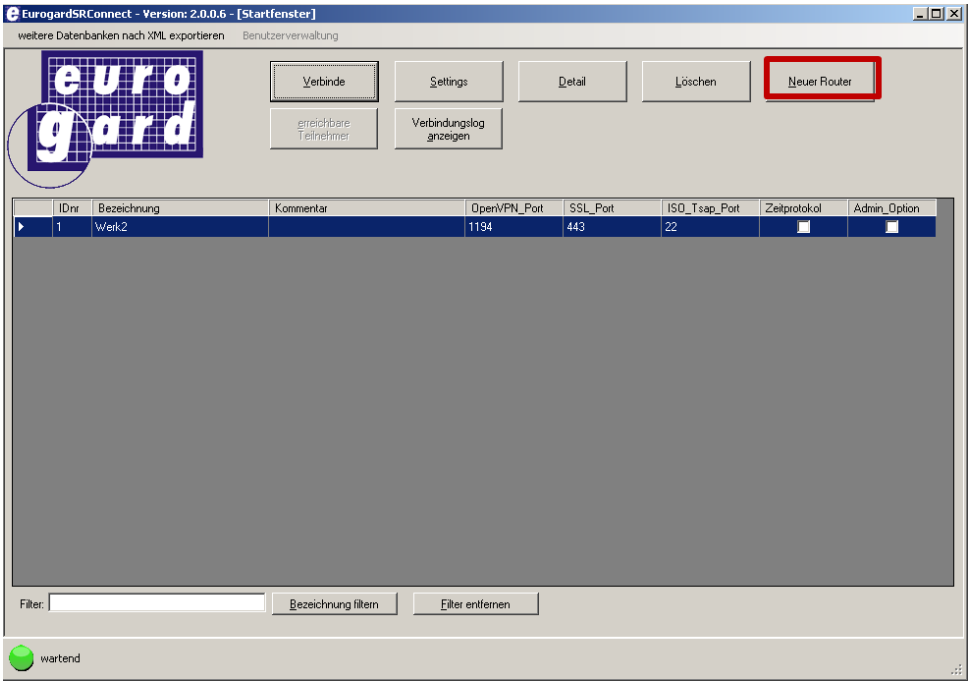
4) When the VPN tunnel has been successfully created, the current status is displayed under Status Logs → Network (CONNECTED)

5.1 EurogardSRConnect client software

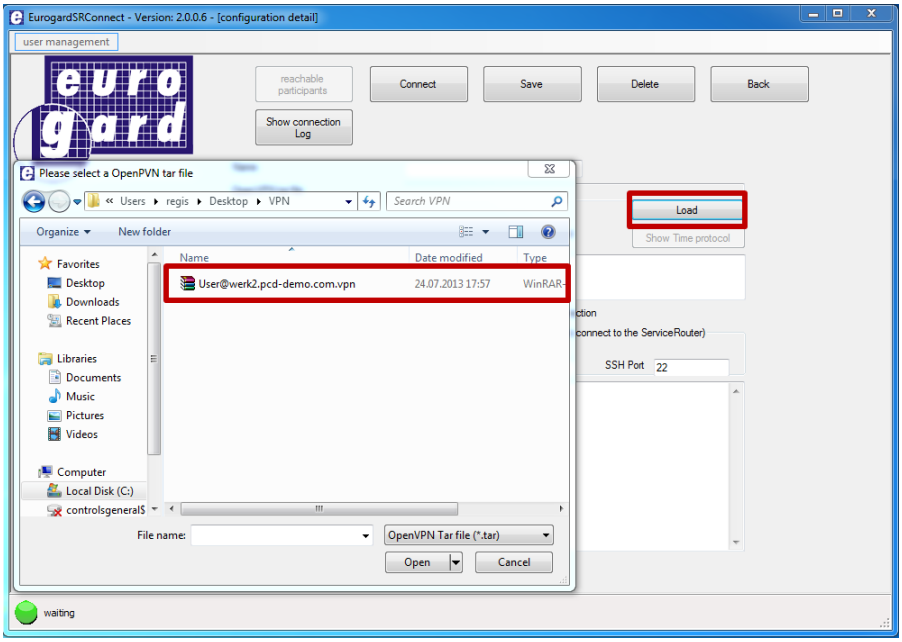
The client software is needed to establish an openVPN connection with the server of the Eurogard router. Administrative rights are required for installing the openVPN client.

The EuroGardSRConnect software is available on the EuroGard homepage
http://www.eurogard.de
Software tool EuroGardSRConnect

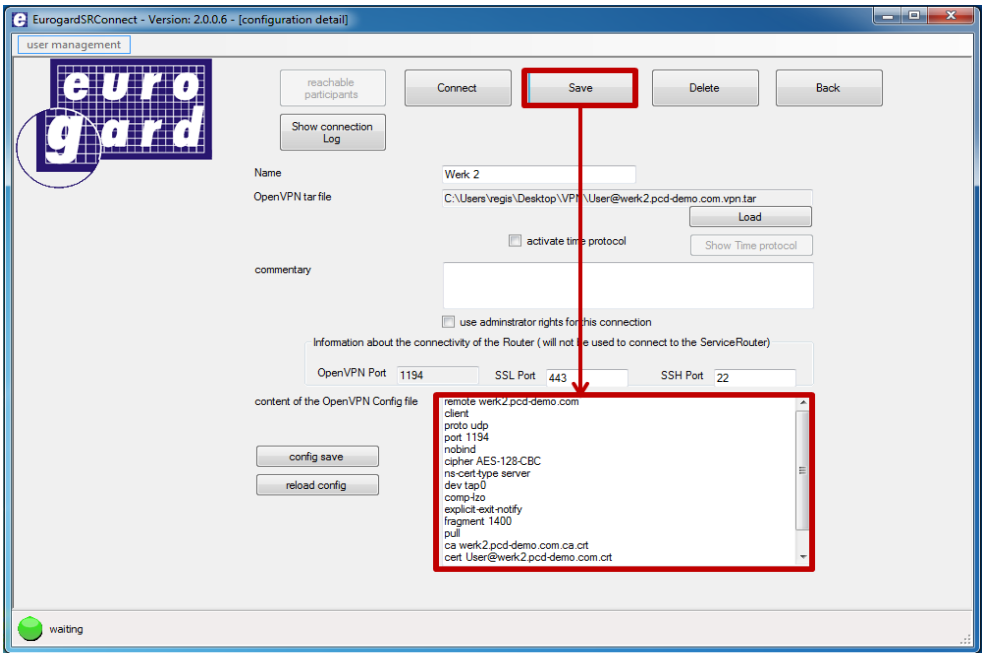
14) Add a new router:



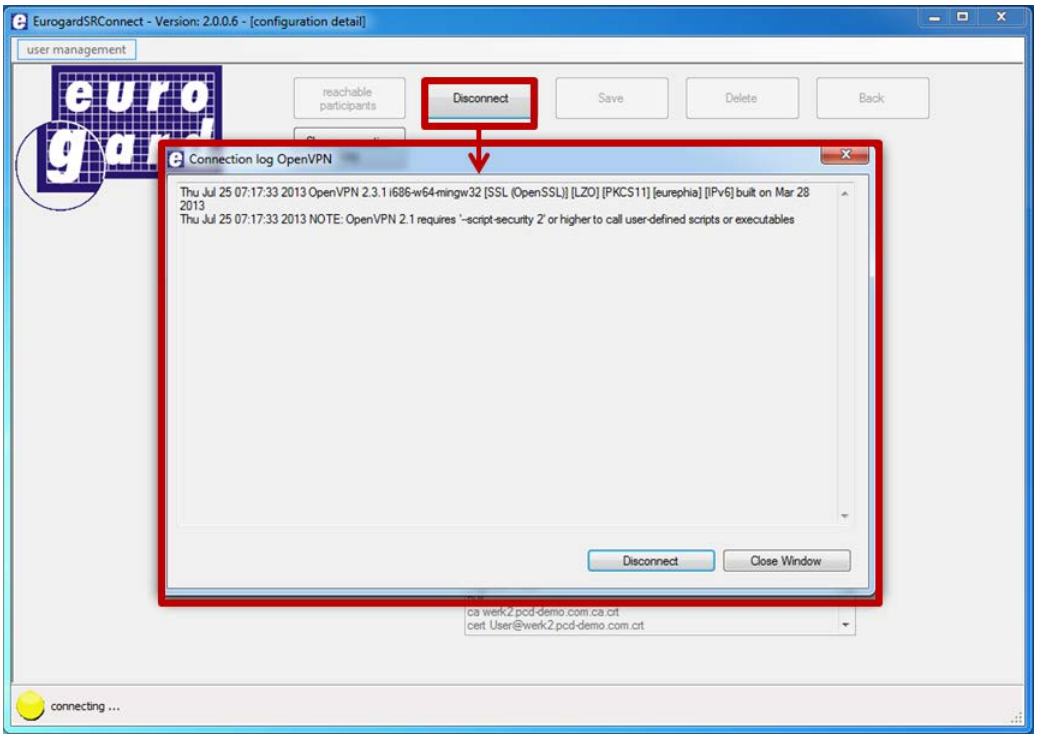
15) Load the user certificate generated by the router in the application. This certificate contains all key and information.



16) Save the user certificate. After saving, you will see the connection parameters in the lower window. In most cases, the parameters do not need to be modified.



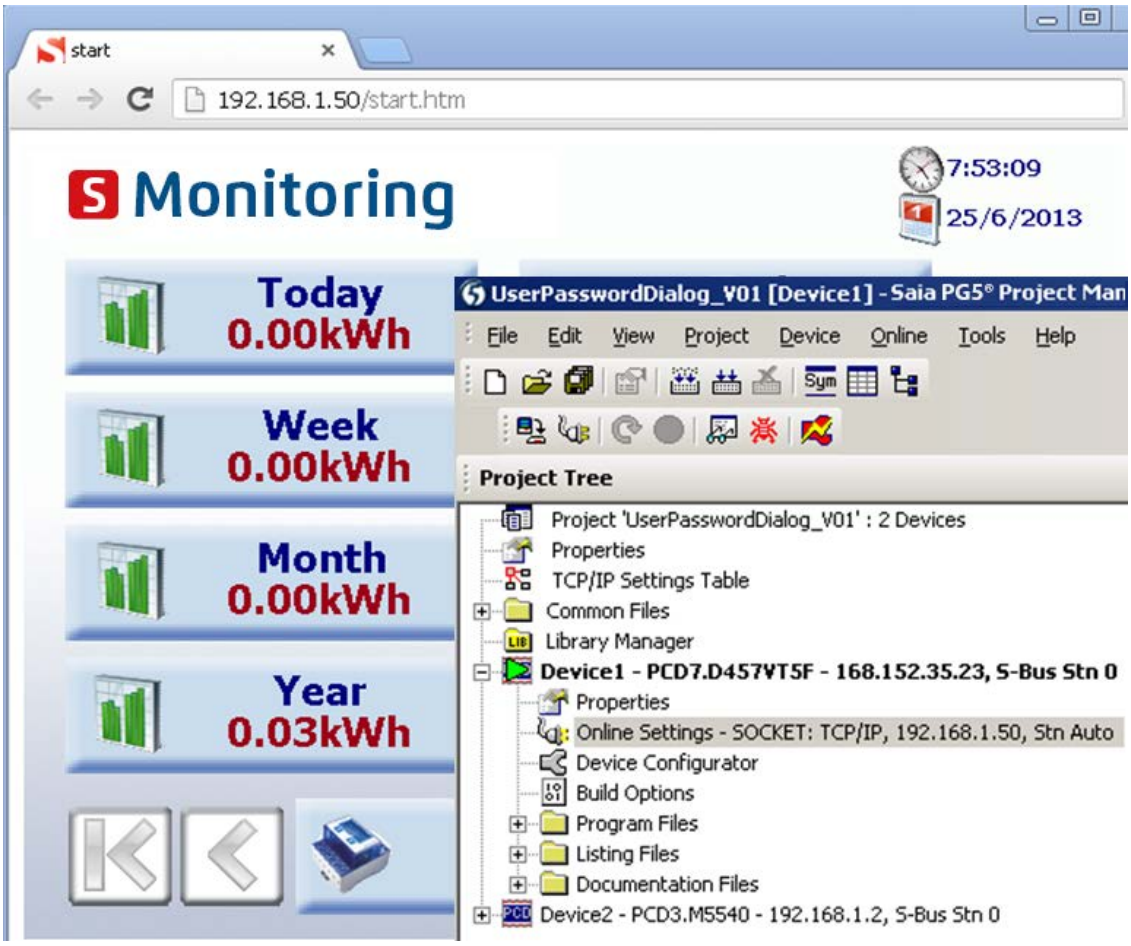
17) Connect to the VPN server



18) The PC is now a member of the remote network. Access to devices is now possible with all applications that support Ethernet.

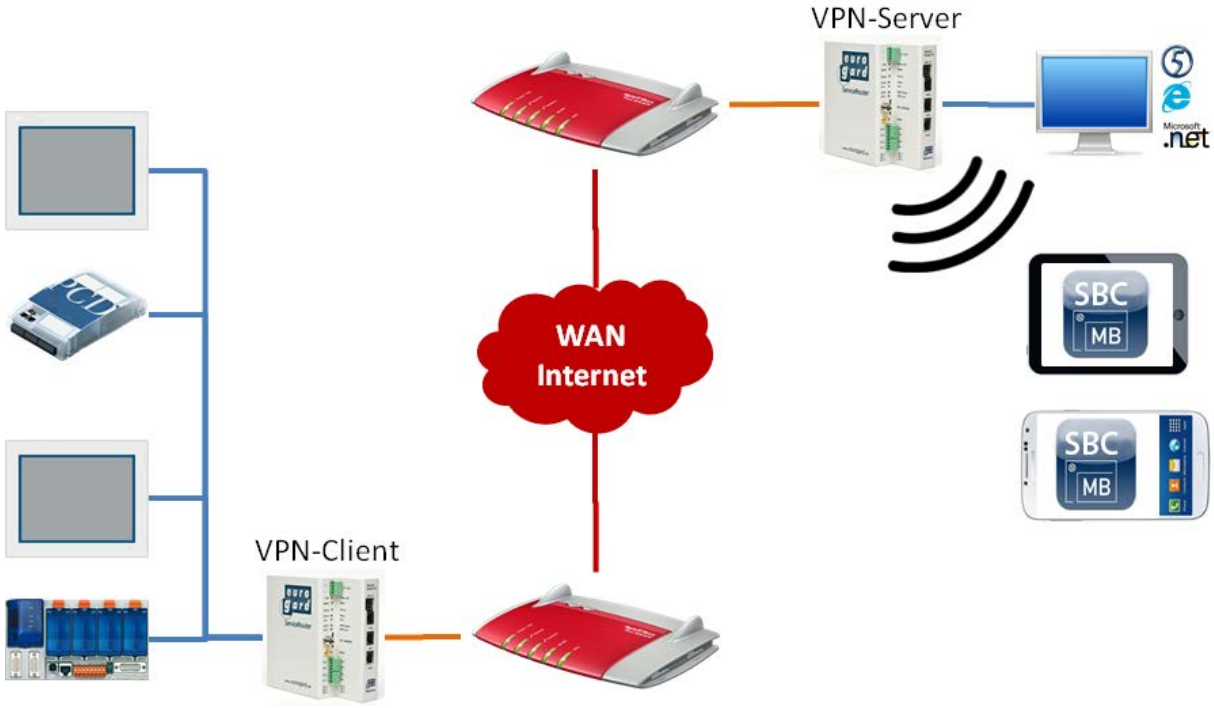
➔ Browser

➔ PG 5



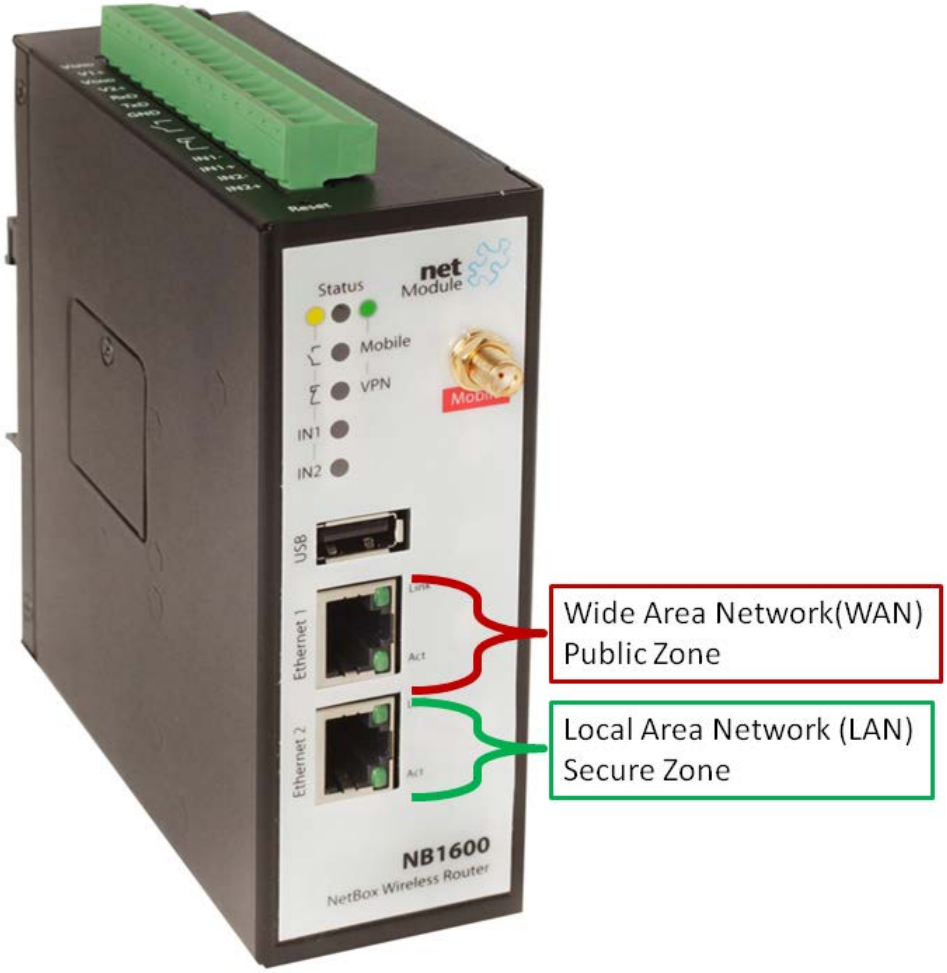
5.2 IOS and Android systems

If two routers are used in the client/server operation, it is possible for IOS and Android systems to be wirelessly connected to the network of the EuroGard Service Router 2. To do this, the router to which the systems are to be connected must be equipped with a W-LAN option.
The EuroGard Client Router can be connected to the server by either a cable or UMTS connection.



6 Net Module VPN Router NB 1600 and 1600-U

Configuring of NB 1600 or NB 1600-U as openVPN-server in Modus TUN.



Wide Area Network (WAN) → Connection to router with public IP-address
Local Area Network (LAN) → Connection to local network

6.1 Specifications

	Net Module NB 1600	**Net Module NB 1600-U**
Order data	NB 1600	NB 1600-U
Additional information	http://www.netmodule.de/products/industrial-routers/wireline-router.html	http://www.netmodule.de/products/industrial-routers/mobile-router.html
Application/ Type	Industrial	Industrial
Top-hat rail installation	Yes	Yes
Electrical supply	24 V DC (-15% +20%)	24 V DC (-15% +20%)
VPN Features		
Number of WAN interfaces	1; LAN	2; LAN, UMTS
Integrated ADSL/VDSL modem	No	No
VPN PPTP	Yes	Yes
VPN L2TP/IPSec	No	No
openVPN	Yes	Yes
No. VPN Clients	10	10
Windows Client	Yes openVPN	Yes openVPN
IOS Client	Yes openVPN	Yes openVPN
Android Client	Yes openVPN	Yes openVPN
Extensions		
3G / 4G Modem	No	3G (UMTS 7.2 Mbps)

6.2 Opening the setup menu

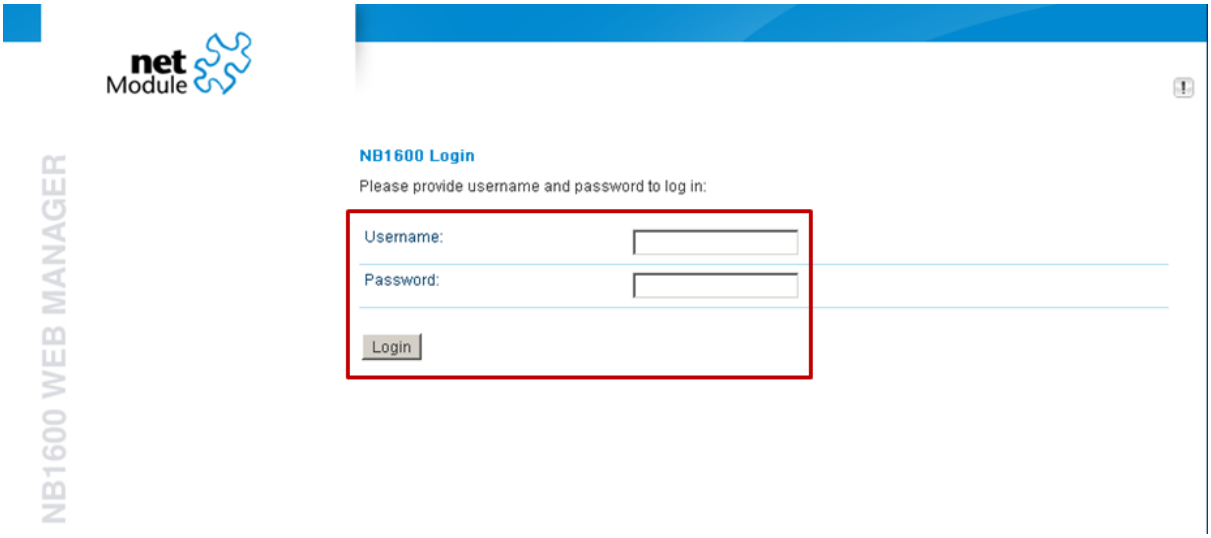
In order to set up the Net Module router, the PC must be connected with a LAN-interface of the router. The router is delivered with an activated DHCP-server. Therefore, it should be avoided to configure the Net Module router with its factory configuration in an Ethernet infrastructure with an existing DHCP-server.

Recommendation:
Disconnect your PC from all existing network connections.
Connect your PC directly to the router.

By default, the IP address of the router is configured to “192.168.1.1”. The router’s DHCP-server provides the connected PC with an address in the DHCP-server’s address range (usually “192.168.1.10” for the first device).

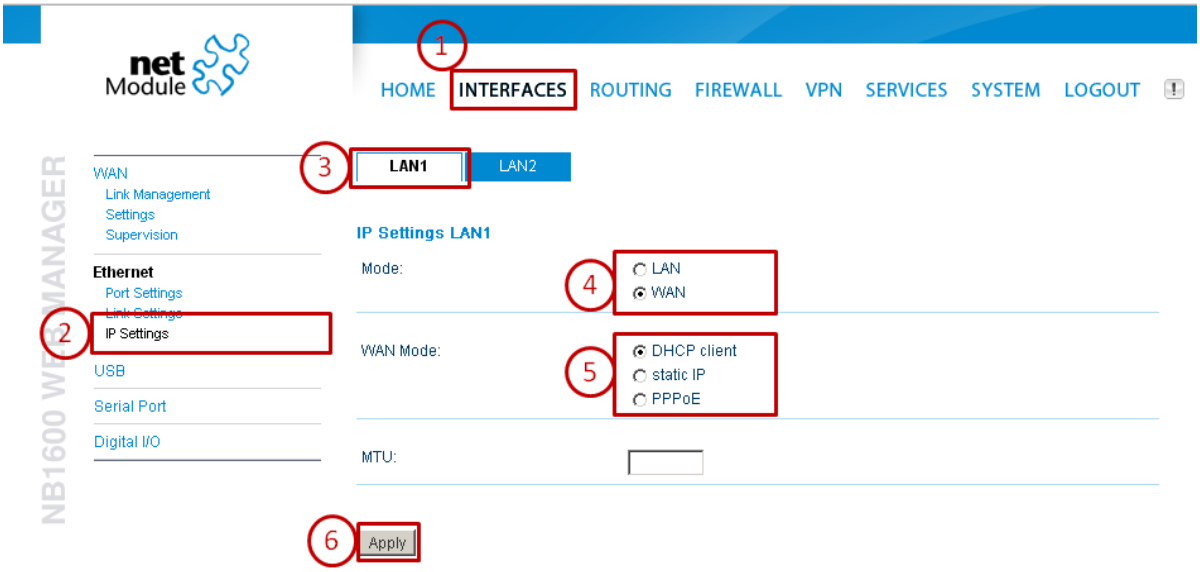
The router is configured in a browser.
In order to load the configuration interface in the browser, the router’s IP address must be entered in the browser.

When connected for the first time, the router opens a configuration wizard where the user has to set the user name as well as password.

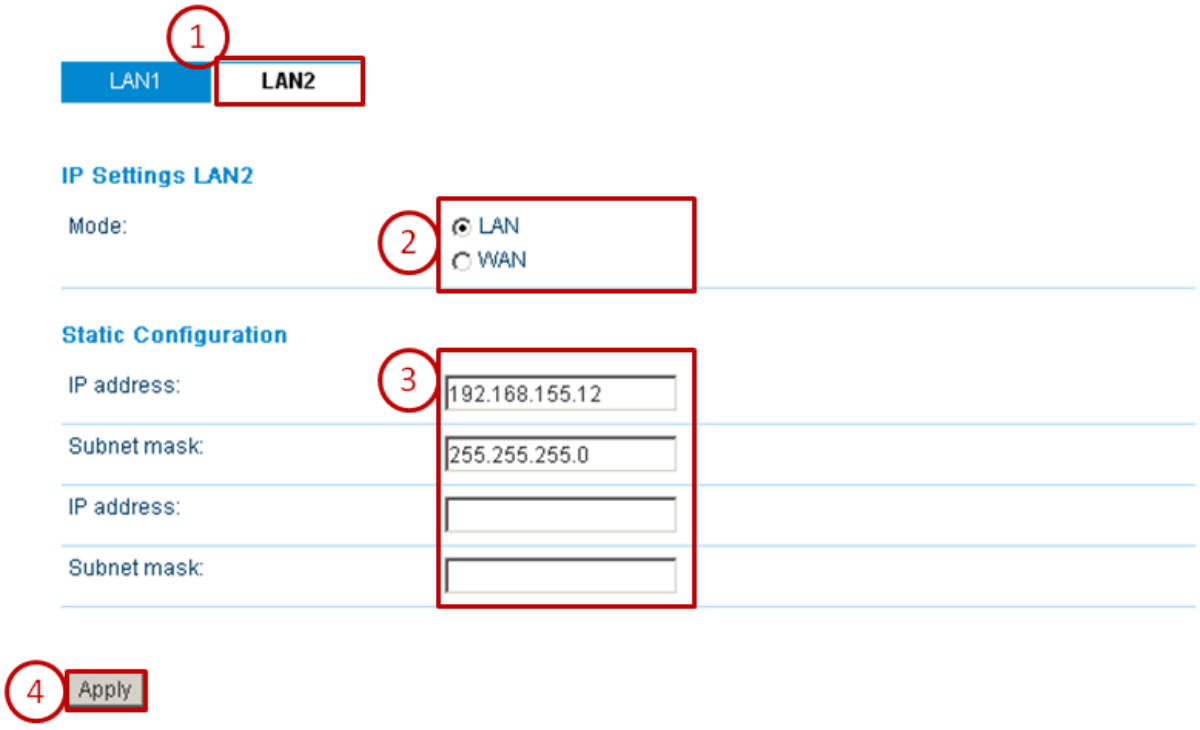


6.3 Configuration of WAN and LAN ports (Wide Area Network)

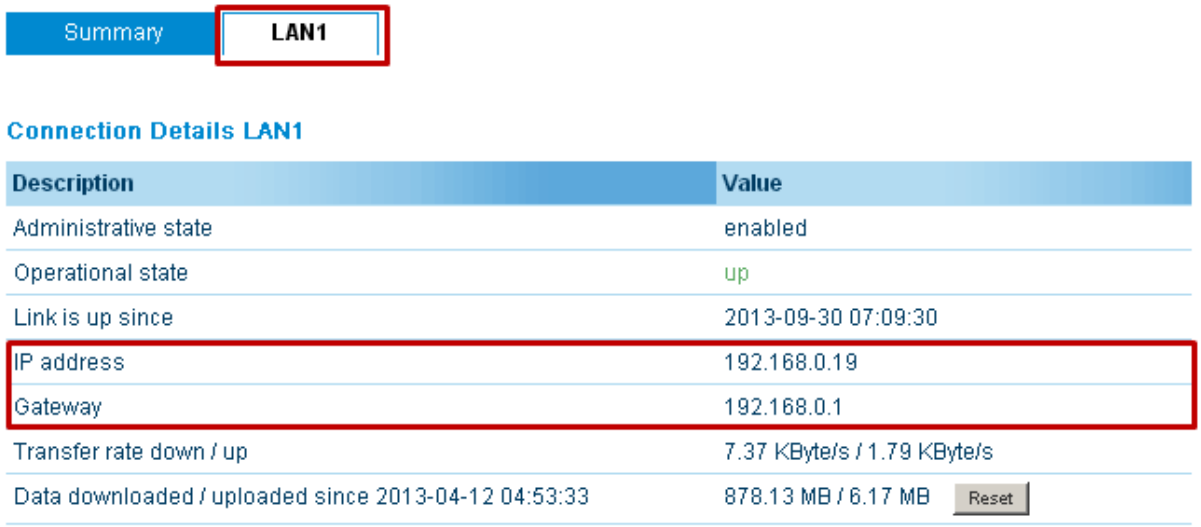
Configuring the LAN1 interface as a WAN interface. The IP-address of the WAN interface is provided by the previously-placed router or can be assigned statically in the region outside of the previous DHCP-server.



The LAN2 interface is used for the automation network and should receive an IP-address in the IP range of this network. In the following example, the automation network is located in the IP-address range 192.168.155.0/24.



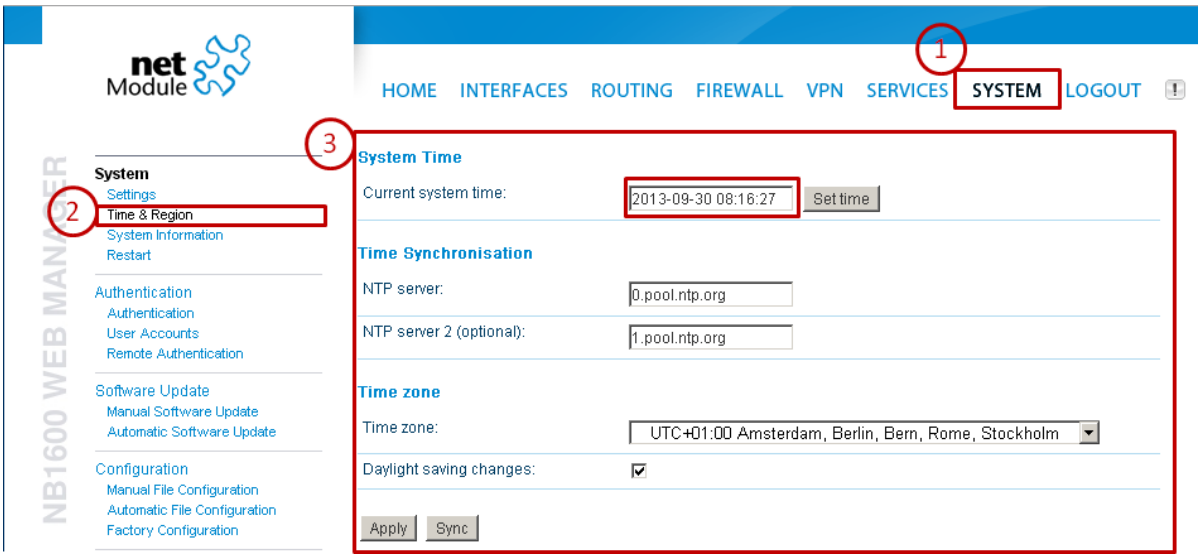
As soon as the DHCP-client is activated for the WAN interface, the IP-address received from the DHCP-server can be checked in the HOME menu.



6.4 Time configuration

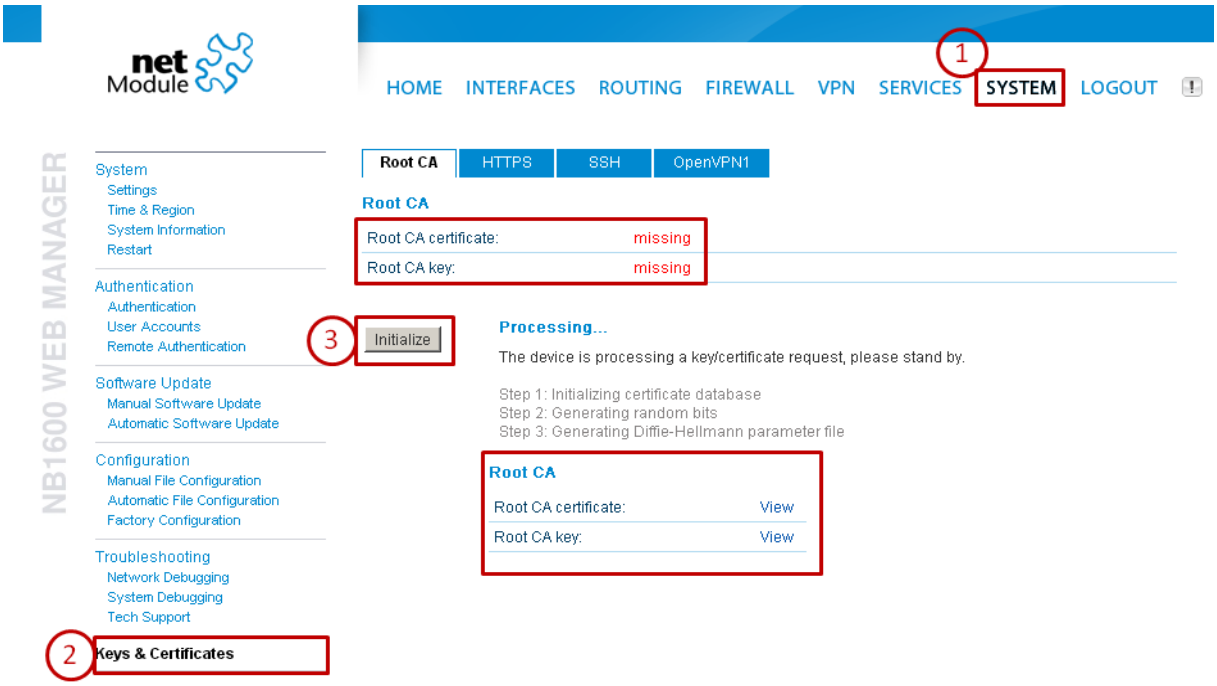
The time configuration of the router must be checked before creating the certificates. You can set the time manually or activate the time synchronization.

→ For the time synchronization is an internet connection necessary.

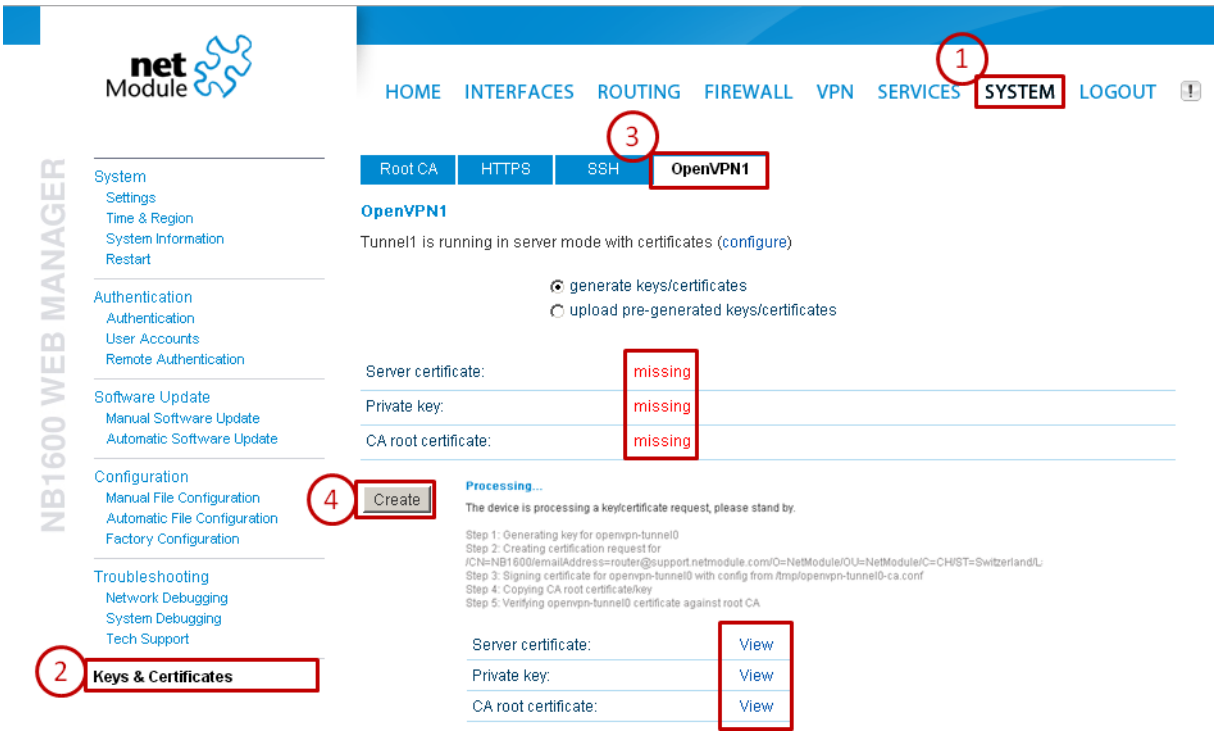


6.5 Create server certificates

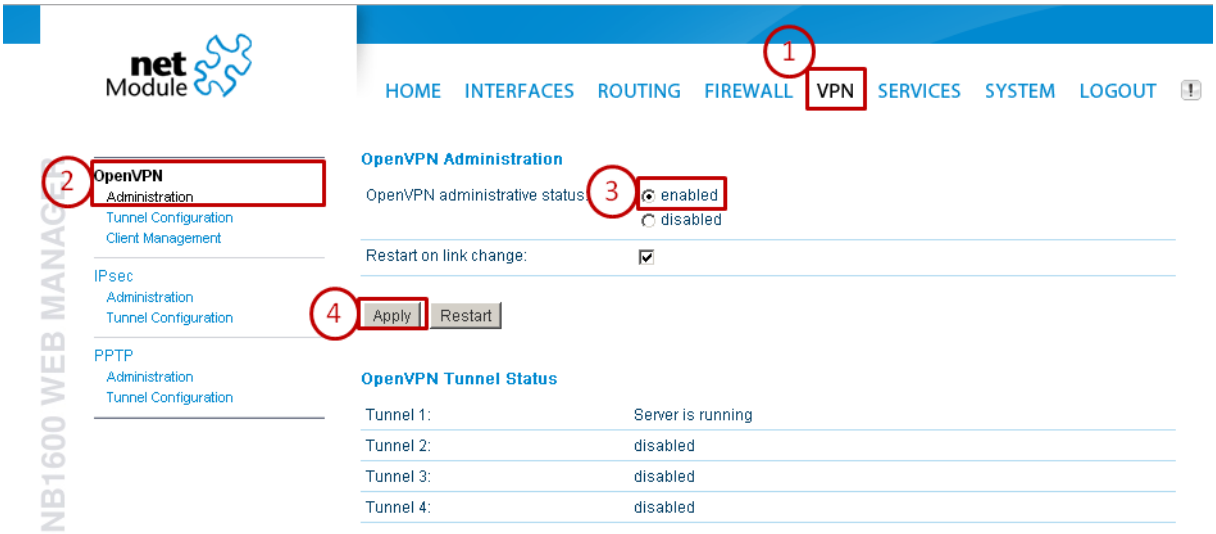
The server certificates are required in order to create an openVPN user. The information stored in the router, such as host name and e-mail addresses etc., are used for the certificate.



After creating the server certificate a certificate for the openVPN tunnel must be created.



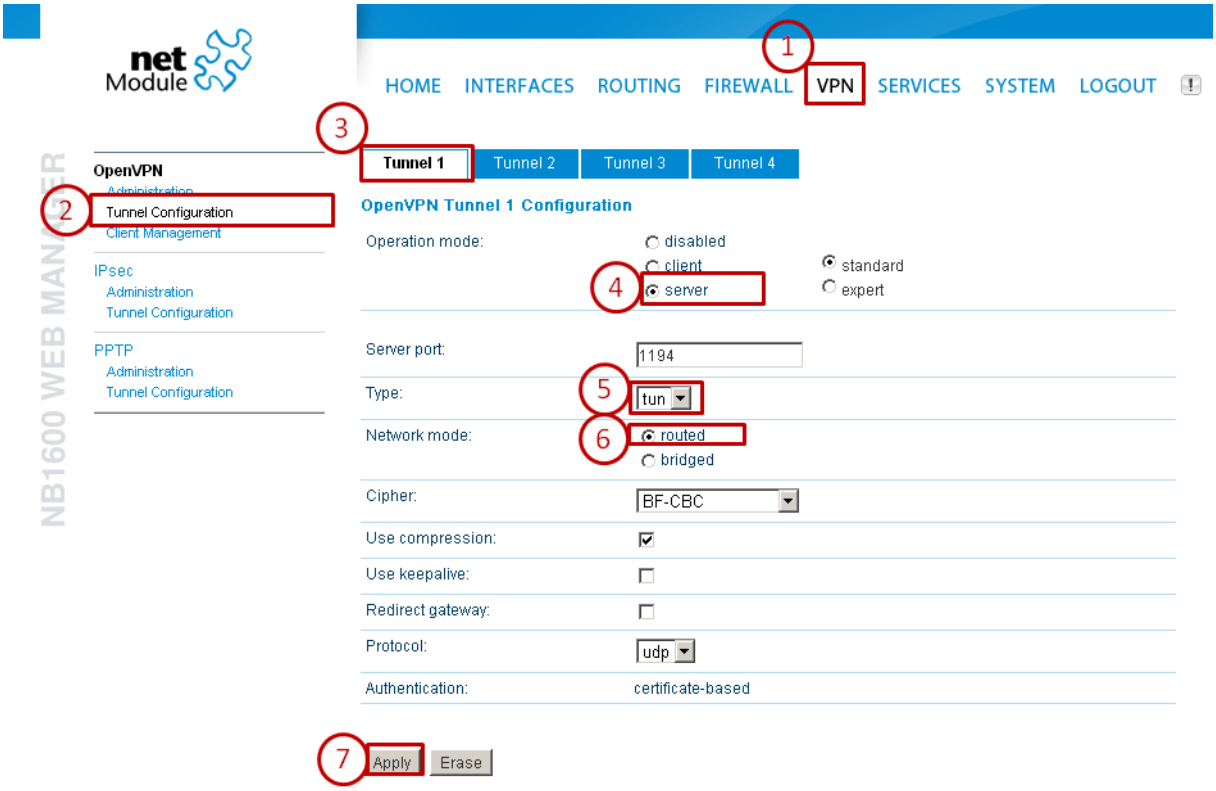
6.6 Enabling the openVPN server



In order to sign in a client, the tunnel must be configured. The Net Module router allows you to configure a VPN-server tunnel or 4-client tunnels.

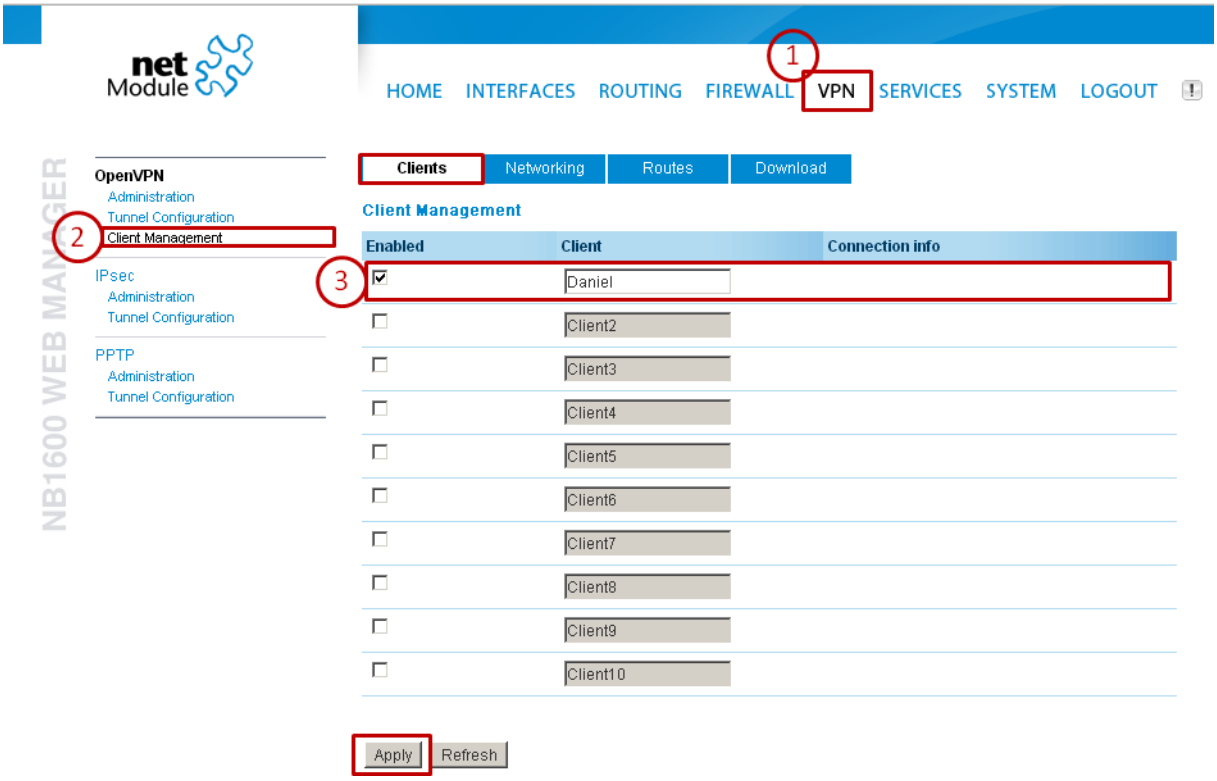
Enable the tunnel as a server.

If mobile devices with an Android or I-OS system must log in to the openVPN server, the TUN mode (routing) must be activated.

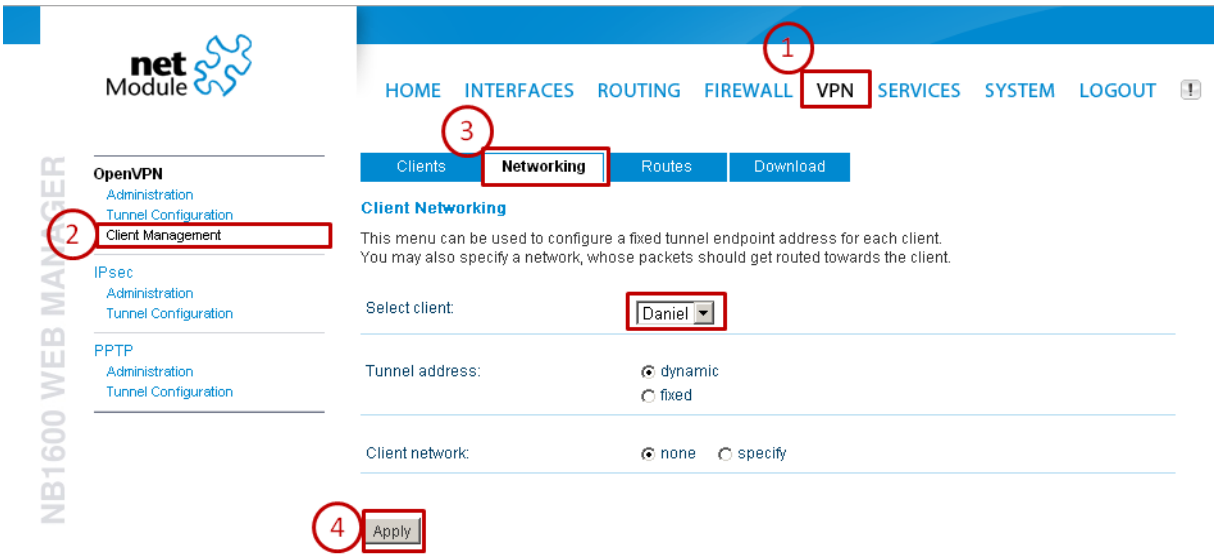


6.7 Creating a client access

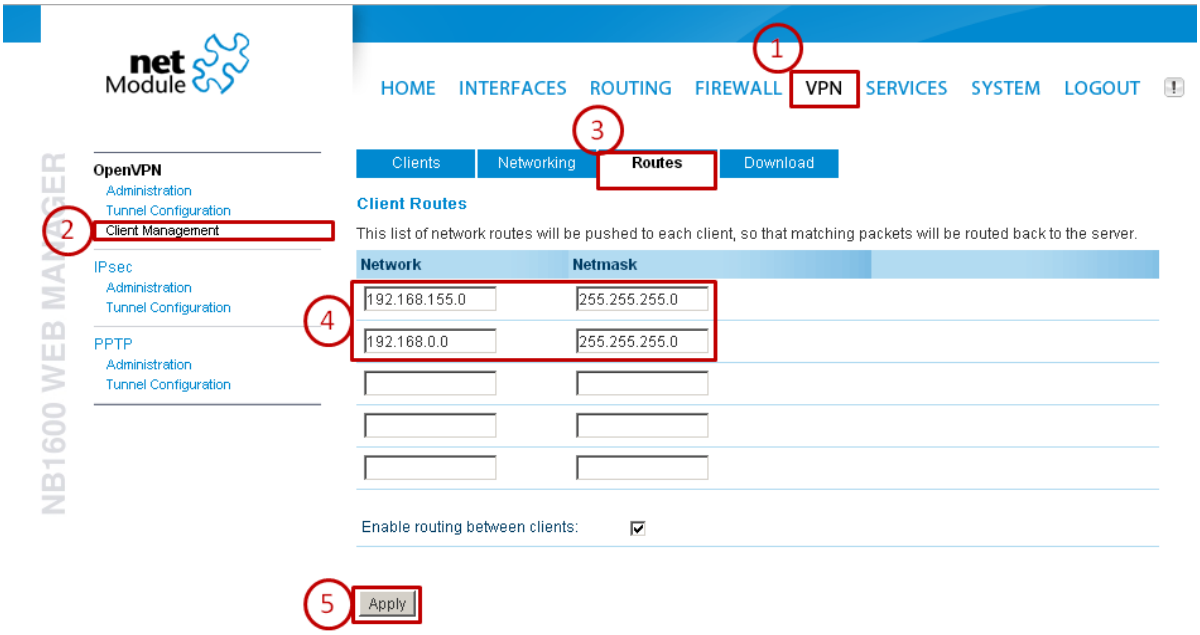
A client is created by activating the checkbox. It is recommended to give the client a name.



You don't need to change the tunnel address as well as client network address with the current tunnel settings.



In order to know the networks behind the VPN tunnel, the routs must be defined. You have to enter the net-address of the automation network here.



The configuration files for the client can be downloaded from the router. Make sure that the server address is correctly written and accessible.

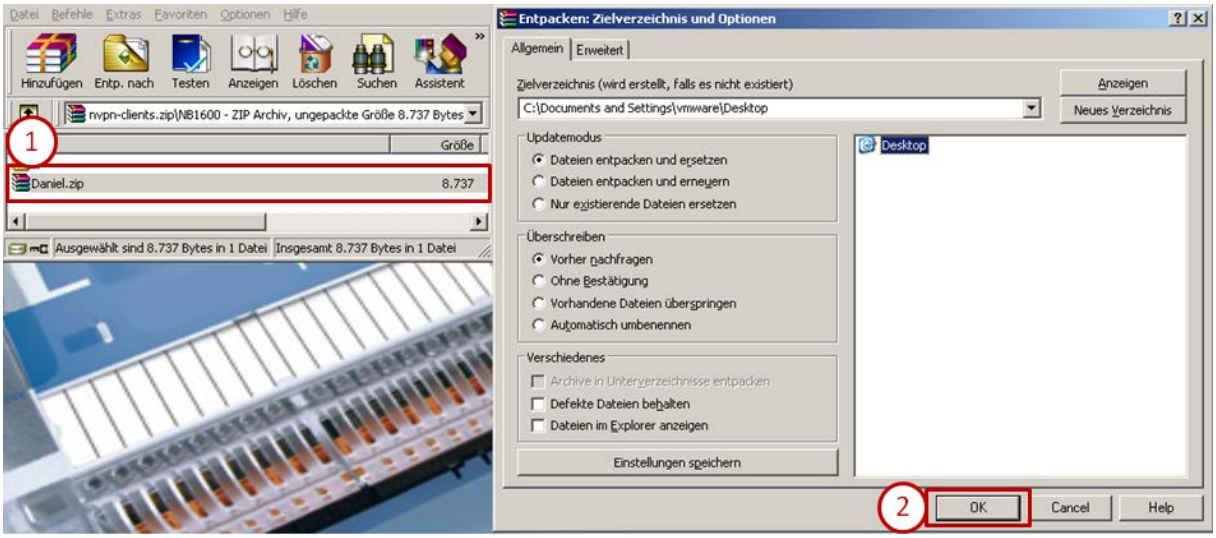
7 Windows openVPN client for Net Module router

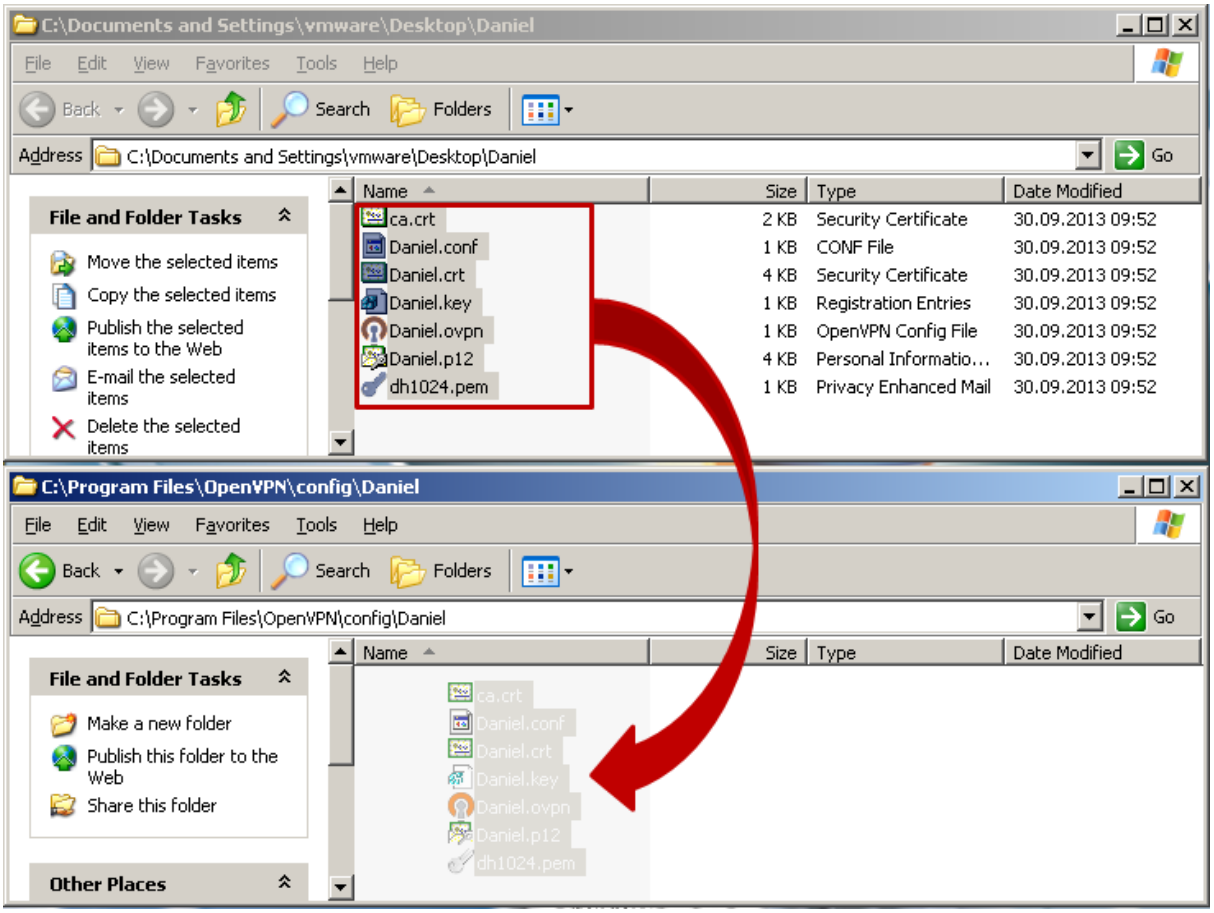
7.1 Installation

Install the application openVPN 2.2.2 (http://www.netmodule.com/download/openvpn-client/windows). You need administration rights for the installation.

7.2 Unpacking the configuration package

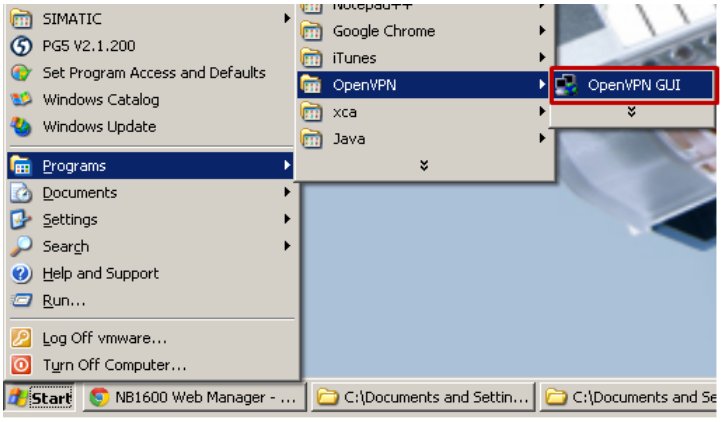
Unpack the configuration package downloaded from the router and copy the content in the config folder, which you will find in the installation path of the openVPN client „C:\Program Files\OpenVPN\config“.

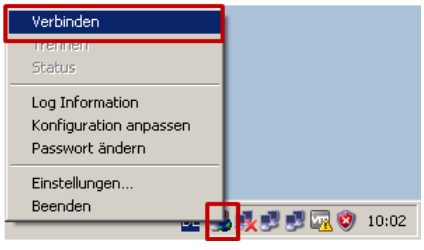


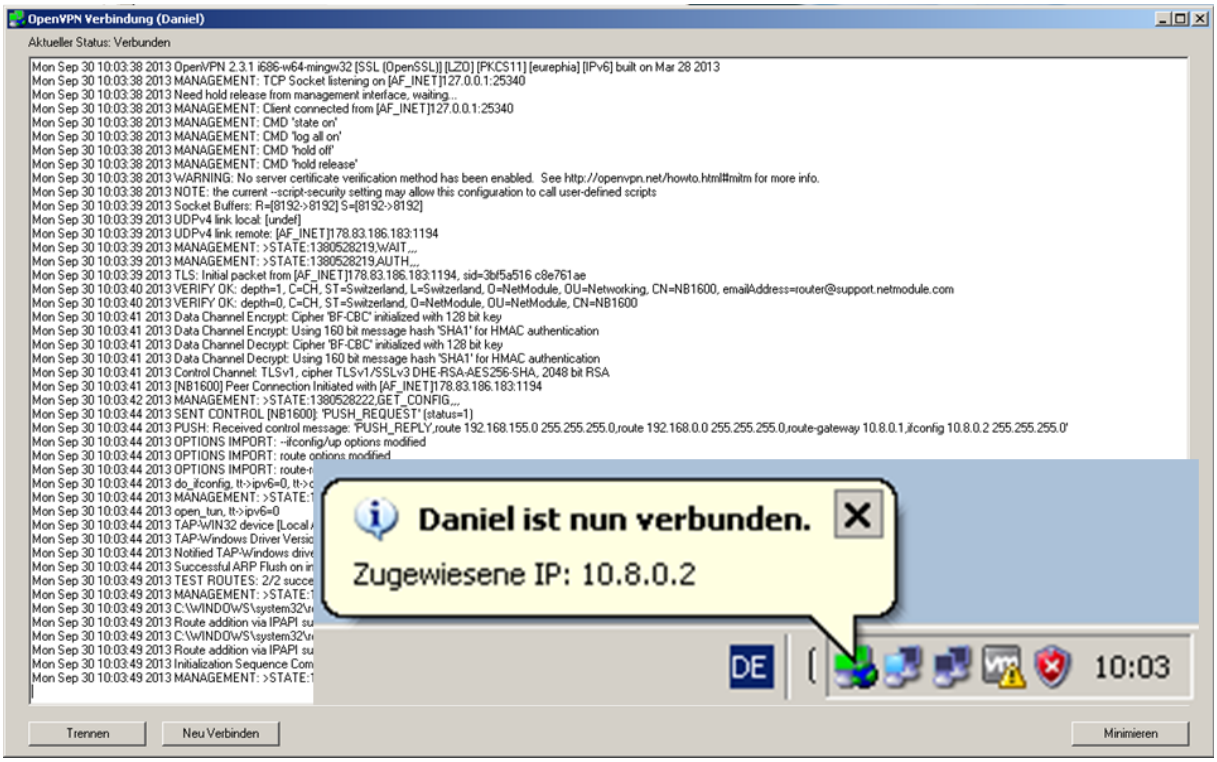


7.3 Establishing a connection

Starting the openVPN client. The openVPN client is displayed with a small icon in the status bar of the operating system. Connect to the openVPN server.

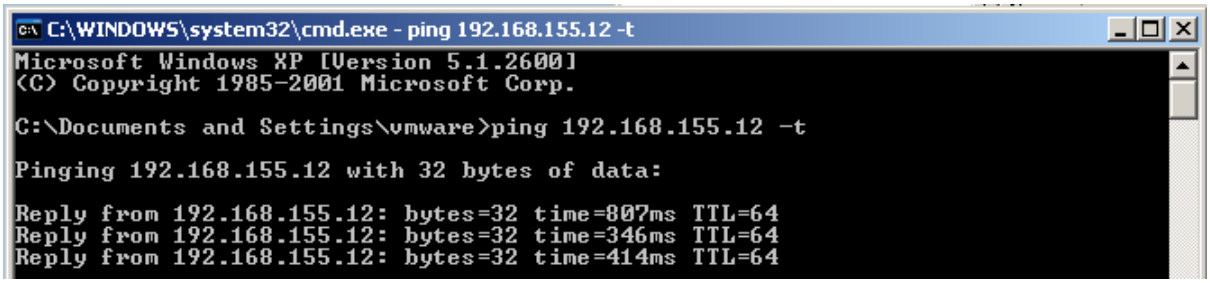






The routs stored in the VPN-server will be activated.

Attention: The logged Windows user needs to have the rights to create routing information bases.



8 Android openVPN client for Net Module Router

Download the application OpenVPN Connect or OpenVPN for Android via the Android Play Store.

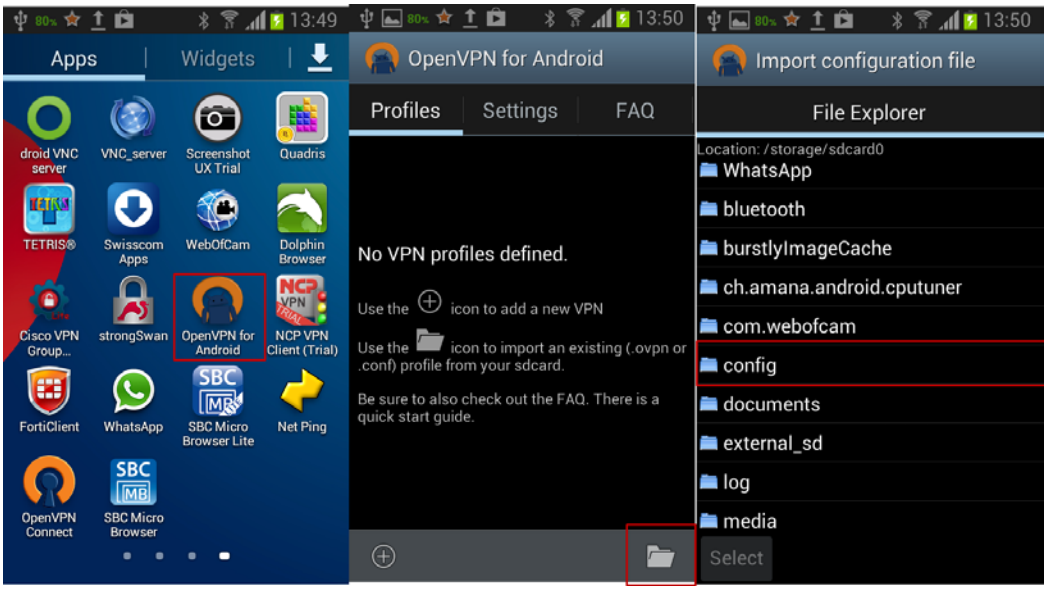
Connect the device, on which the configuration file downloaded from the router is stored, with your PC.

Attention: The openVPN-server must be configured in TUN mode for Android client systems.

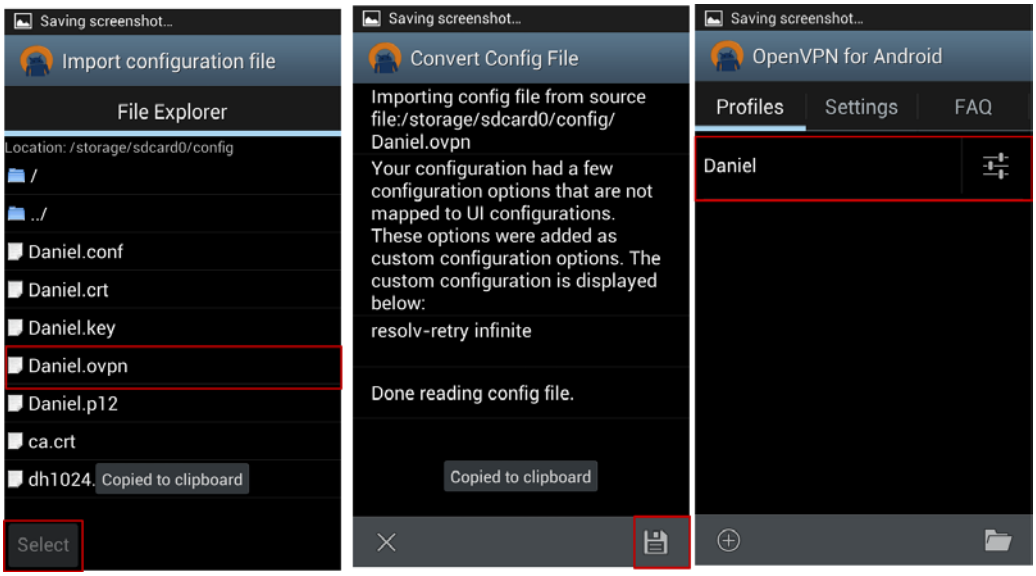
Copy the configuration files on the device in the register “config“.

Example: „Computer\GT-I9100\Phone\config“

Start the application OpenVPN for Android and open the configuration file downloaded from the PC.



The profile is now imported into the openVPN client for Android and is available.

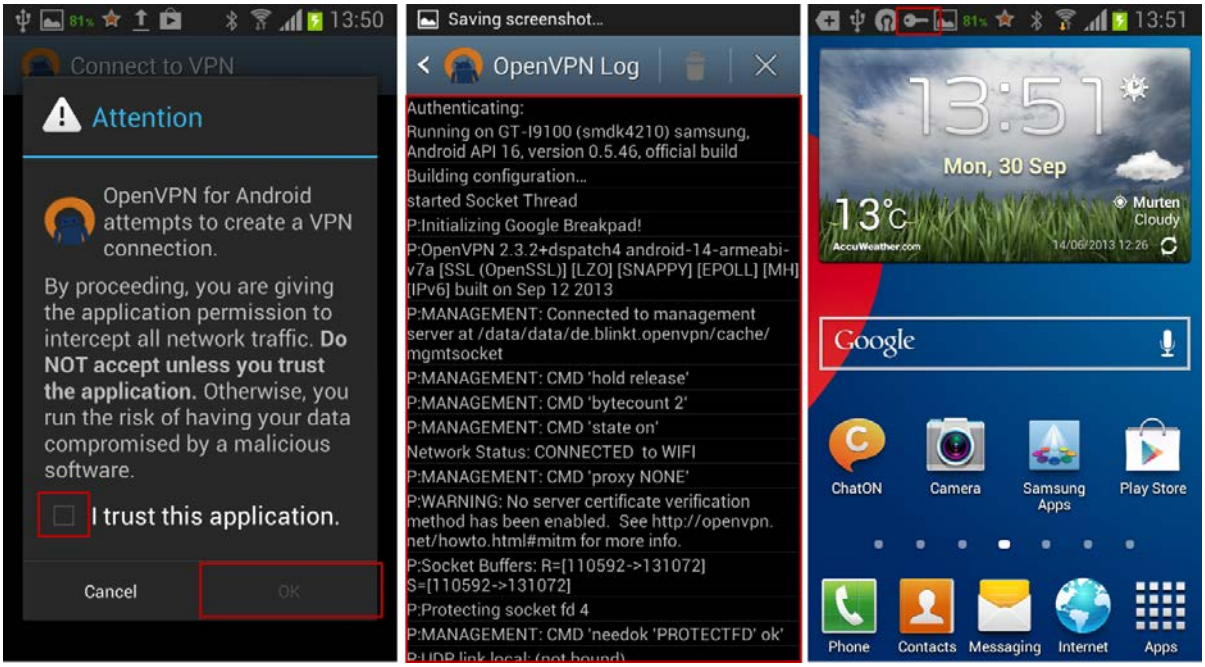


8.1 Establish a connection

Connect with the openVPN-server.

The operating system Android will ask you concerning the network configuration if you trust the application. In order to establish a connection you have to approve the dialog box.

As soon as the establishment of the connection was successful, the key icon is displayed in the status bar of Android.


13:50
Connect to VPN
Attention
OpenVPN for Android attempts to create a VPN connection.
By proceeding, you are giving the application permission to intercept all network traffic. Do NOT accept unless you trust the application. Otherwise, you run the risk of having your data compromised by a malicious software.
I trust this application.
Cancel
OK
Saving screenshot...
OpenVPN Log
Authenticating:
Running on GT-I9100 (smdk4210) samsung, Android API 16, version 0.5.46, official build
Building configuration...
started Socket Thread
P:Initializing Google Breakpad!
P:OpenVPN 2.3.2+dspatch4 android-14-armeabi-v7a [SSL (OpenSSL)] [LZO] [SNAPPY] [EPOLL] [MH] [IPv6] built on Sep 12 2013
P:MANAGEMENT: Connected to management server at /data/data/de.blinkt.openvpn/cache/mgmtsocket
P:MANAGEMENT: CMD 'hold release'
P:MANAGEMENT: CMD 'bytecount 2'
P:MANAGEMENT: CMD 'state on'
Network Status: CONNECTED to WIFI
P:MANAGEMENT: CMD 'proxy NONE'
P:WARNING: No server certificate verification method has been enabled. See http://openvpn.net/howto.html#mitm for more info.
P:Socket Buffers: R=[110592->131072] S=[110592->131072]
P:Protecting socket fd 4
P:MANAGEMENT: CMD 'needok 'PROTECTFD' ok'
13:51
Mon, 30 Sep
13°C
Murten
Cloudy
Google
ChatON
Camera
Samsung Apps
Play Store
Phone
Contacts
Messaging
Internet
Apps

9 I-OS openVPN client for Net Module Router

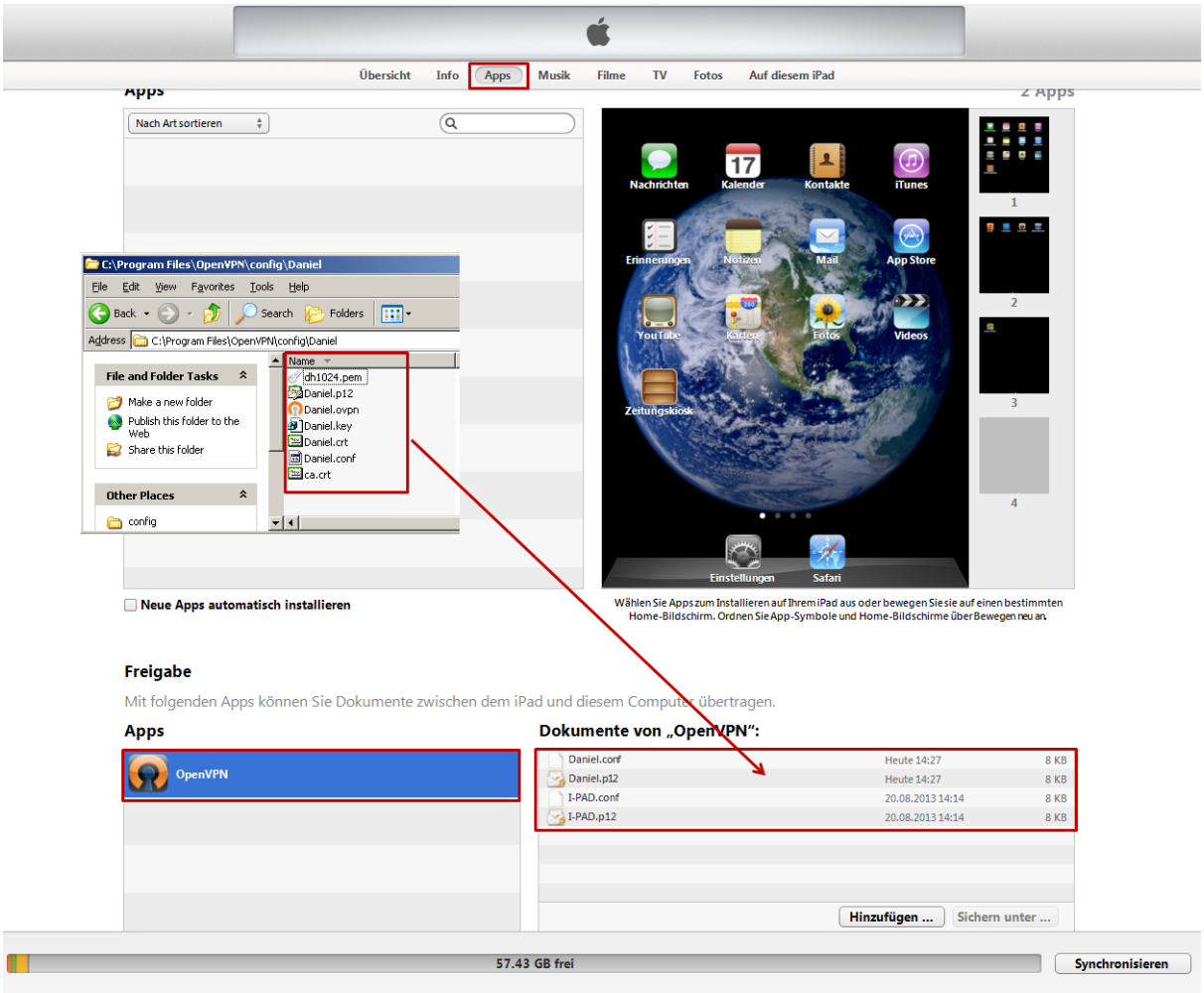
Install the application openVPN, which is available in the Apple App Store.

Install the application iTunes on your PC and connect the iPad with your PC.

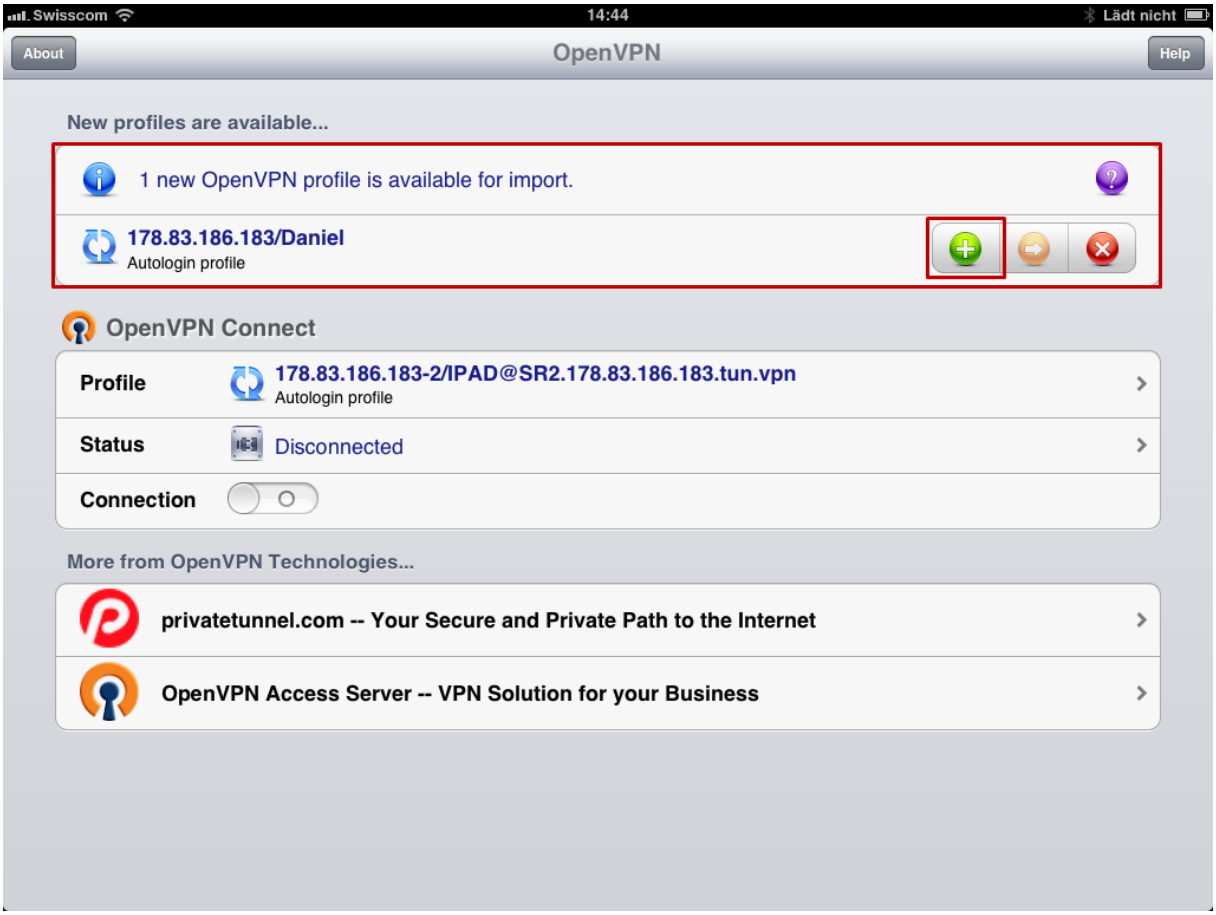
Attention: The openVPN-server must be configured in TUN mode for I-OS client systems.

Open the iPad or I-OS device in iTunes

Download the files, which were unpacked by the router, for the openVPN tunnle configuration via the tab „Apps“ → OpenVPN in the application



Open the App OpenVPN. The downloaded openVPN-server configuration is detected automatically and can be approved by clicking on add button.



9.1 Establishing of a connection

Connect with the OpenVPN-server by moving the roll bar.

If you see the status „connected“, then the VPN-tunnel is established.