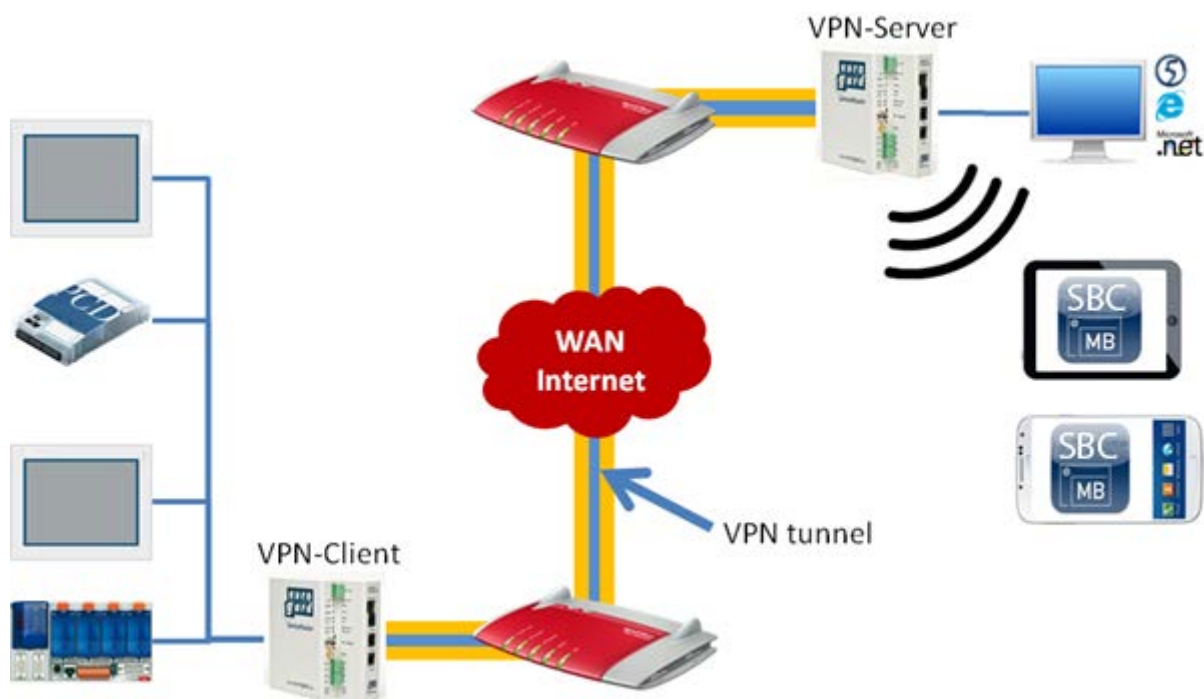


VPN Router



Dokument Historie

Version	Bearbeitung	Veröffentlichung	Bemerkungen
DE01	10.07.2013	11.07.2013	
DE02	30.09.2013	15.10.2013	Neu getesteter Router: → Net Module NB 1600 → Der Vigor 2920 ist in seiner Konfiguration identisch jedoch ohne ADSL/VDSL Modem
DE03	2014-02-20	2014-02-120	Neues Firmenlogo

Inhalt

1	Technische Daten: Vigor 2xx0Vn, EuroGard Service Router V2 und Net Module NB 1600.....	4
2	Nutzen eines bestehenden Internet Zugangspunktes	5
2.1	Vorbereitung	5
2.1.1	Explizite Port-Weiterleitung (Forwarding)	6
2.1.2	Konfiguration einer DMZ.....	7
3	Vigor 2xx0Vn DrayTek.....	10
3.1	Öffnen des Setup Menüs.....	10
3.2	Konfigurieren des WAN-Ports.....	11
3.3	WAN-Betrieb hinter einem Router/Firewall.....	11
3.4	Konfiguration des VPN-Servers.....	12
3.5	Client Android System 4.1.2.....	16
3.6	Client iPhone / iPad	18
3.7	Client Microsoft Windows XP.....	20
3.8	Client Microsoft Windows 7.....	27
3.9	Fehlerbehandlung Windows:	34
4	EuroGard Service Router 2.....	38
4.1	Öffnen des Setup Menüs.....	39
4.2	Konfigurieren des LAN-Ports (Local Area Network).....	40
4.3	Konfigurieren des WAN Ports (Wide Area Network).....	41
4.3.1	WAN over Ethernet.....	41
4.3.2	WAN over UMTS	42
4.4	Zeitkonfiguration	43
4.5	Server-Zertifikat erstellen	43
4.6	Aktivieren des openVPN-Servers.....	44
4.6.1	VPN-Modus Server.....	44
4.6.2	Zugänge erstellen.....	45
5	EuroGard Service Router 2 VPN-Client.....	46
5.1	Client Software EurogardSRConnect.....	48
5.2	IOS und Android Systeme.....	51
6	Net Module VPN Router NB 1600 und 1600-U.....	52
6.1	Technische Daten.....	53
6.2	Öffnen des Setup Menü.....	54

6.3	Konfigurieren der WAN und LAN Ports (Wide Area Network).....	55
6.4	Zeitkonfiguration	56
6.5	Erstellen der Server Zertifikate	57
6.6	Aktivieren des openVPN Servers.....	58
6.7	Anlegen eines Client Zuganges.....	59
7	Windows openVPN Client für Net Module Router	61
7.1	Installation.....	61
7.2	Entpacken des Konfigurationpakets	61
7.3	Herstellen einer Verbindung.....	62
8	Android openVPN Client für Net Module Router	63
8.1	Herstellen einer Verbindung.....	64
9	I-OS openVPN Client für Net Module Router	66
9.1	Herstellen einer Verbindung.....	67

Infos über dieses Dokument:

Ein sicherer Betrieb der PCD-Steuerungen am Internet ist nur mit zusätzlichen externen IT-Komponenten mit integrierten Schutzfunktionen wie VPN, Firewall, Proxy-Server, etc. gewährleistet.

Zu diesem Zweck haben wir mehrere VPN-Router evaluiert und mit unseren PCD-Steuerungen getestet. In diesem Dokument ist die detaillierte Beschreibung für die Konfiguration und Inbetriebnahme zu finden.

Getestete Geräte:

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

1 Technische Daten: Vigor 2xx0Vn, EuroGard Service Router V2 und Net Module NB 1600

Der Vigor 2xx0 der Firma DreyTec ist ein Business Router zum Erstellen von VPN-Verbindungen und dem Managen von kleineren bis mittleren Business / Home- Netzwerken. Seine Funktionalität und Benutzeroberfläche sind leicht zu bedienen.

Der EuroGard Service Router V2 ist ein industrieller Router zum Erstellen von sicheren Verbindungen auf industriellen Anlagen. Das Konfigurationsmenü ist in mehreren Sprachen verfügbar. Die Benutzerführung ist einfach verständlich und das Erstellen einer VPN-Verbindung leicht realisierbar.

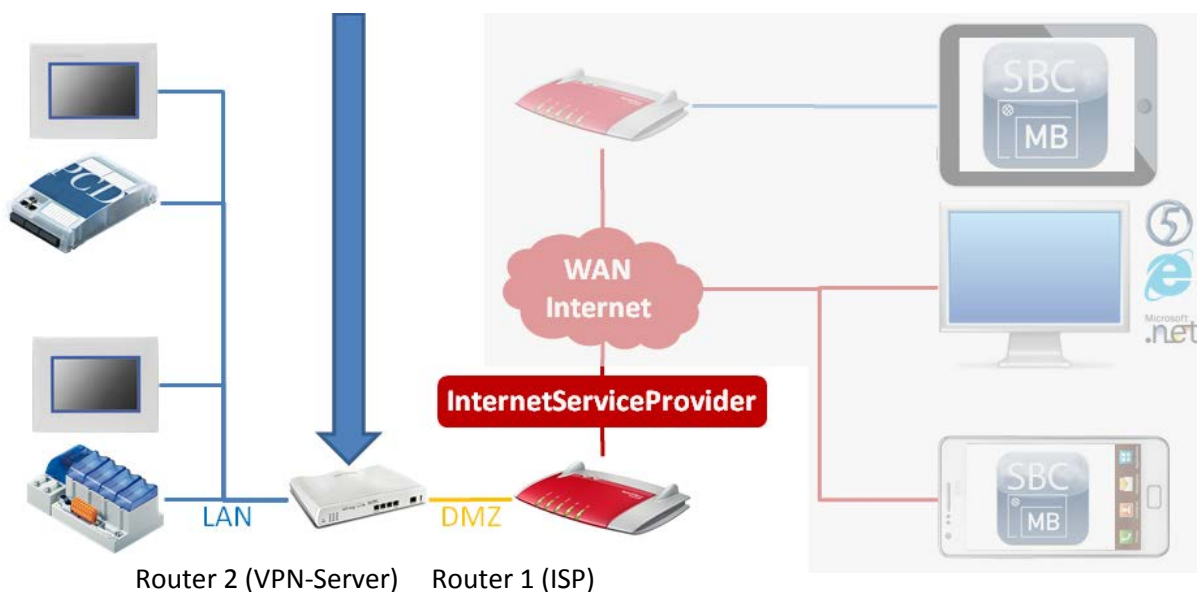
	DreyTek Vigor 2850Vn	DreyTek Vigor 2920Vn	EuroGard Service Router V2 (WLAN)	EuroGard Service Router V2 (UMTS)	Net Module NB 1600-U
Bestelldaten	2850Vn	2920VN	ER 1201-WLAN	ER 1201-UMTS	NB 1600-U
Weitere Informationen	http://www.draytek.de/produkte/modem-router/vigor2850-serie.html	http://www.draytek.de/produkte/dual-wan/vigor2920-serie.html	http://www.eurogard.de	http://www.eurogard.de	http://www.netmodule.de/products/industrial-routers/mobile-router.html
Einsatz/Bauform	Business / Home	Business / Home	Industriell	Industriell	Industriell
Hutschienmontage	Nein	Nein	Ja	Ja	Ja
Spannungsversorgung	230 VAC	230 VAC	24 VDC	24 VDC	24 V DC (-15% +20%)
VPN Eigenschaften					
Anzahl WAN Interfaces	3: LAN/Modem/USB	3: LAN/LAN/USB	1: LAN	2: LAN/UMTS	2; LAN, UMTS
Integriertes ADSL/VDSL Modem	Ja	Nein	Nein	Nein	Nein
VPN PPTP	Ja	Ja	Nein	Nein	Ja
VPN L2TP/IPSec	Ja	Ja	Nein	Nein	Nein
openVPN	Nein	Nein	Ja	Ja	Ja
Anz. VPN Clients	32 Verbindungen	32 Verbindungen	30 Verbindungen	30 Verbindungen	10
Windows Client	Ja (in Windows integriert)	Ja (in Windows integriert)	Ja (EurogardSRC connect)	Ja (EurogardSRC connect)	Ja openVPN
IOS Client	Ja (IPSec/L2TP, integriert in IOS)	Ja (IPSec/L2TP, integriert in IOS)	Nein *	Nein *	Ja openVPN
Android Client	Ja (IPSec/L2TP, integriert in Android)	Ja (IPSec/L2TP, integriert in Android)	Nein *	Nein *	Ja openVPN
Erweiterungen					
3G / 4G Modem	Ja, mit USB-Stick	Ja, mit USB-Stick	Nein	Ja, mit integriertem UMTS Modem	3G (UMTS 7.2 Mbps)

* IOS oder Android Systeme können heute via WLAN an den Router angebunden werden. Dafür werden jeweils 2 Router benötigt. Ein VPN-Server sowie ein VPN-Client. Unterstützung von VPN auf mobilen Geräten ist in Vorbereitung.

2 Nutzen eines bestehenden Internet Zugangspunktes

2.1 Vorbereitung

Einrichten einer Verbindung in eine bestehende Ethernet-Infrastruktur: Die Internetverbindung zum InternetServiceProvider (ISP) wird dabei von einem bestehenden Gerät (in der unteren Grafik von Router 1) zur Verfügung gestellt.



Im oben gezeigten Fall wird die Internetverbindung zum ISP **über den** Router 1 hergestellt. Die bestehende Ethernet-Infrastruktur, soll oder kann nicht verändert werden. Der Router 2, welcher den VPN-Server beinhaltet, wird hinter **dem** Router 1 im bestehenden LAN installiert. Der Router 1 muss in diesem Fall so konfiguriert werden, dass alle relevanten VPN-Ports an die IP-Adresse des Router 2 übermittelt werden, oder die DMZ wird auf die IP-Adresse des Router 2 konfiguriert.

Je nach Konfiguration der VPN-Verbindung [Die Konfiguration der VPN-Verbindung kann z.B. das Point-to-Point Tunneling Protocol (PPTP) oder das Layer 2 Tunneling Protocol (L2TP) sein, welches meist in Kombination mit dem Internet Protocol Security (IPSec) angewendet wird] werden unterschiedliche Ports vom öffentlichen Netzwerk an der WAN-Schnittstelle des VPN-Servers benötigt. Ein Port stellt ein Tor zur Kommunikation mit einer Applikation, in diesem Fall der VPN-Server, über TCP/IP dar.

	Protokoll	Port
PPTP Standard	TCP	1723
L2TP Standard	UDP	1701
IPSec Standard	UDP	500, 4500

In einer normalen Konfiguration werden die meisten Ports am Router, der die ISP-Verbindung verwaltet, von der internen Firewall geblockt. Daher ist es **nicht** möglich, ohne

kleine Änderungen an der bestehenden Ethernet-Infrastruktur, einen VPN-Server zu betreiben.

Firewall bedeutet grundsätzlich, dass alle Datenpakete die über nicht definierte Ports auf das LAN zugreifen wollen, vom ISP verwaltenden Router 1 verworfen werden. Somit kann der undefinierte Port keine Kommunikation mit den Geräten hinter der Firewall herstellen.

Damit eine Verbindung zum VPN-Server (Gerät hinter der Firewall) des ISP verwaltenden Routers 1 hergestellt werden kann, müssen die VPN-Verbindungsrelevanten Ports im ISP verwaltenden Router 1 in einer Firewall-Regel definiert werden

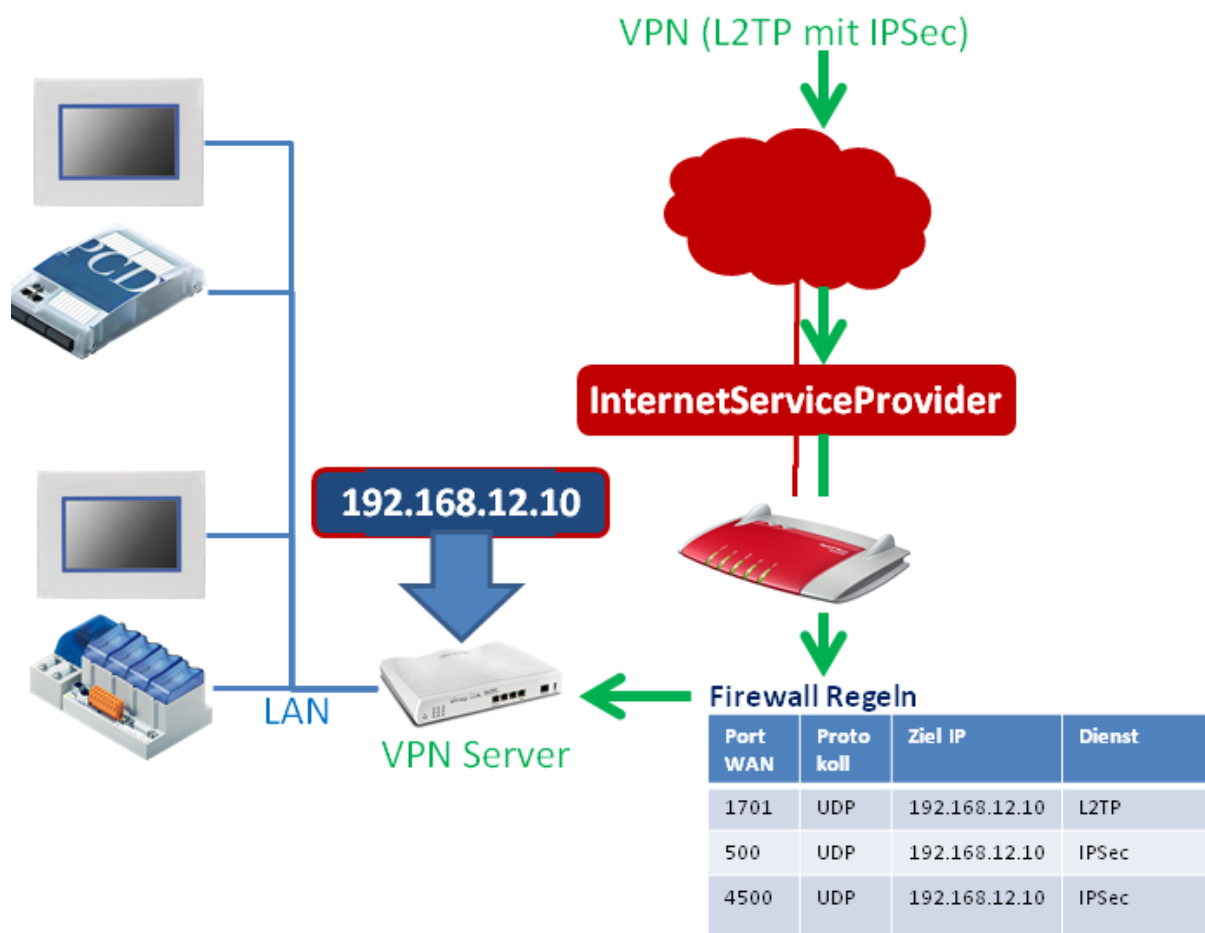
Die Konfiguration des 1 Routers zum Weiterleiten der Ports ist abhängig vom Fabrikat und Softwarestand des eingesetzten Gerätes. Grundsätzlich gibt es 2 Wege diese Ports an den VPN-Server weiterzuleiten.

2.1.1 Explizite Port-Weiterleitung (Forwarding)

Die Ports für das Herstellen einer VPN-Verbindung vom Client zum Server müssen vom ersten Router durch eine Firewall-Regel an den VPN-Server weitergereicht werden.

Ports:

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



Vorteil dieser Konfiguration:

Sehr sicher, da lediglich die oben genannten Ports am VPN-Server zur Verfügung stehen.

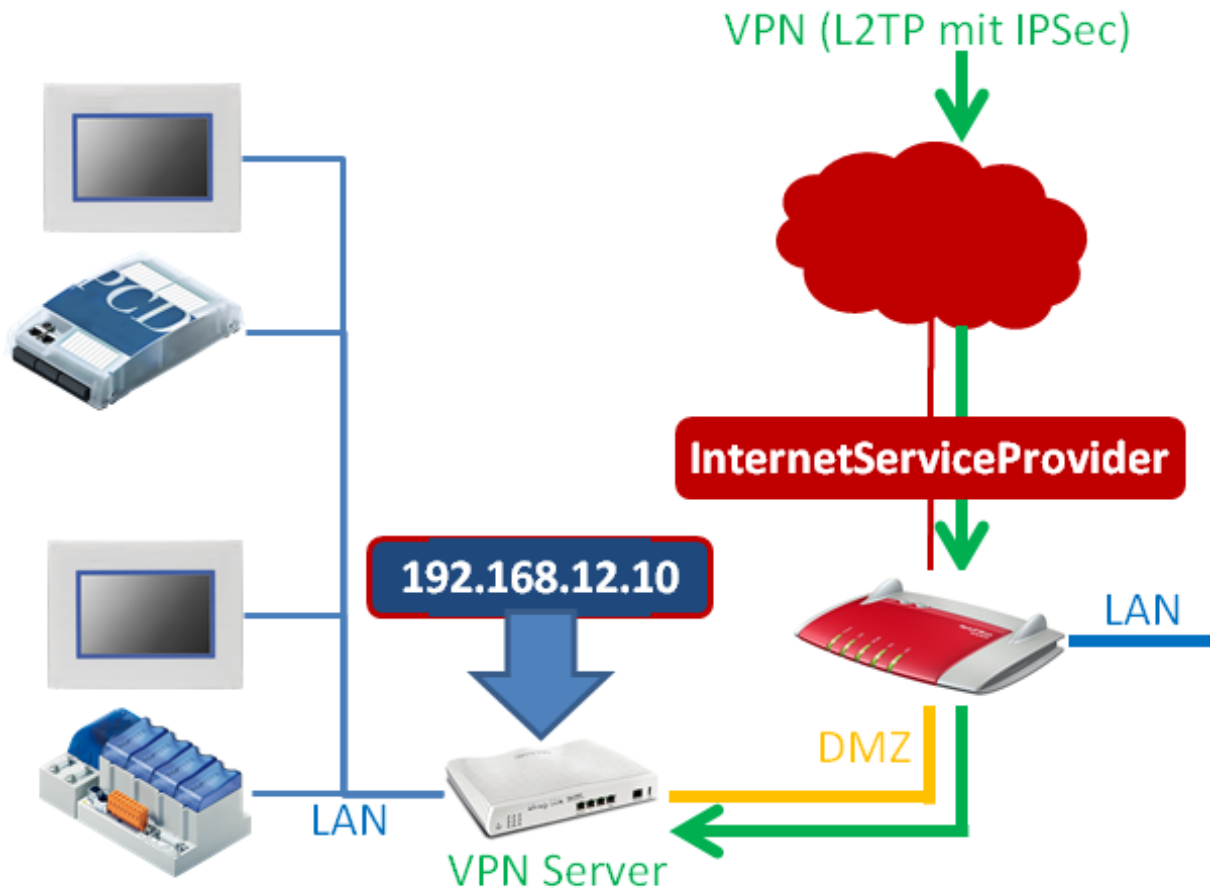
Nachteil dieser Konfiguration:

Die VPN-Ports sind standardmässig mit den oben beschriebenen Ports definiert. Diese sind jedoch nicht fest definiert, sondern können im Setup des VPN-Servers verändert werden. Ist die Portweiterleitung nicht vollständig identisch mit der Konfiguration des VPN-Servers, so kann keine Verbindung hergestellt werden.

Weitere Möglichkeiten bietet der Einsatz einer DMZ.

2.1.2 Konfiguration einer DMZ

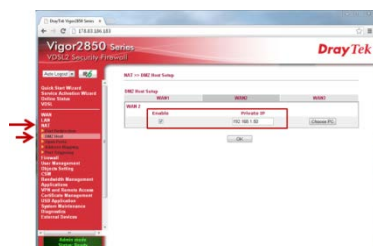
Eine DMZ erlaubt es, alle Ports die auf der WAN-Schnittstelle angefragt werden und der erste Router keine Regel kennt, an eine bestimmte IP-Adresse weiter zu leiten.



Vorbereitung des bestehenden Routers DMZ/NAT:

Damit der bestehende Router, der mit dem ISP verbunden ist, Anfragen auf nicht bekannten Port`s verteilt, muss eine DMZ eingerichtet werden. Diese Konfiguration kann von Router zu Router unterschiedlich sein, sie wird jedoch meistens in der Hilfe des Setups oder im Handbuch des Routers gut beschrieben.

DMZ stellt eine „Demilitarized Zone“ dar. Sie ist für Geräte die selbst keine Sicherheitseinrichtungen besitzen, ein ungeschützter und nicht sicherer Bereich. In der DMZ besitzt jedes Gerät vergleichbare Eigenschaften, als ob es tatsächlich am Internet



angeschlossen ist. Grund ist, dass der mit dem Internet physikalisch verbundene Router, alle ihm nicht bekannten Datenpakete an oder in die DMZ weiterleitet. In den meisten Fällen wird die DMZ durch das Angeben einer bestimmten IP-Adresse konfiguriert.

Achtung:

Ports für die der erste Router eine Regel kennt, werden meist nicht in die DMZ weitergeleitet.

Nachteil:

Der VPN-Server benötigt eine eigene Schutzeinrichtung (Firewall usw...)

Vorteil:

Sehr leicht zu konfigurieren und zu administrieren.

3 Vigor 2xx0Vn DrayTek

Im Dokument werden die Konfiguration des DreyTec Routers Vigor 2850 und 2920 beschreiben. Beide besitzen dieselbe Konfigurationsoberfläche zur Konfiguration der Grundeinstellungen und VPN. Im Gegensatz zum Vigor 2850 besitzt der Vigor 2920 kein integriertes ADLS/VDSL Modem.

3.1 Öffnen des Setup Menüs

Zum Einrichten des Vigor 2xx0 muss der PC mit einer LAN-Schnittstelle verbunden werden. Der Router wird mit einem aktivierten DHCP-Server ausgeliefert. Es sollte deshalb vermieden werden, den Vigor 2xx0 mit Werkskonfiguration in eine Ethernet-Infrastruktur mit bereits vorhandenem DHCP-Server zu konfigurieren.

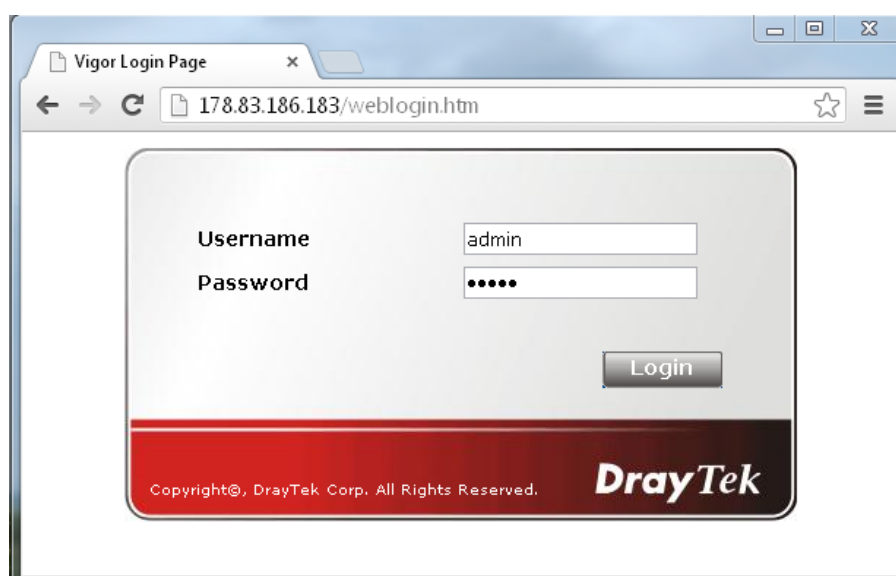
Empfohlen:

Trennen Sie ihren PC von allen bestehenden Netzwerkverbindungen.
Verbinden Sie ihren PC direkt mit dem Router.

Die IP-Adresse des Routers ist standartmässig auf „192.168.1.1“ konfiguriert. Der DHCP-Server des Routers wird dem angeschlossenen PC eine Adresse im Adressraum des DHCP-Servers zur Verfügung stellen (erstes Gerät normalerweise „192.168.1.10“).

Der Router wird in einem Browser konfiguriert.
Damit die Konfigurationsoberfläche im Browser geladen wird, muss die IP-Adresse des Routers im Browser aufgerufen werden.

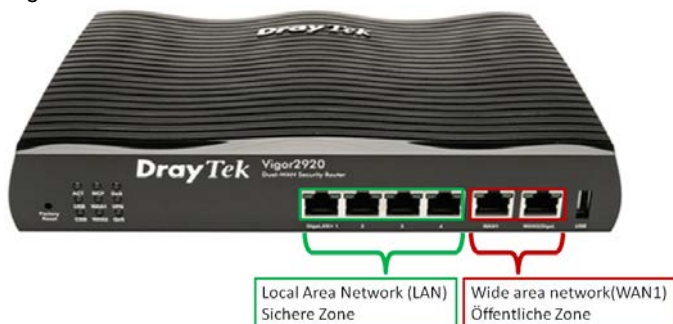
Standartmässig wird der Vigor 2xx0 mit dem Benutzer „admin“ und dem dazugehörigem Passwort „admin“ ausgeliefert. Sie finden die Benutzer und Passwörter auch im Handbuch des Routers.



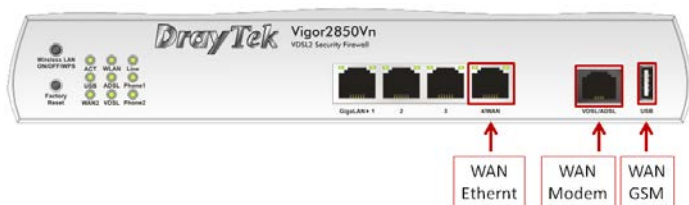
3.2 Konfigurieren des WAN-Ports

WAN steht für „Wide Area Network“. Dies ist bei einem Router immer die öffentliche Schnittstelle in einen öffentlichen, ungeschützten Bereich.

Vigor 2920



Vigor 2850



3.3 WAN-Betrieb hinter einem Router/Firewall

Der Vigor 2xx0 ermöglicht das Konfigurieren von 3 unterschiedlichen WAN Ports.

Achtung: Der Vigor 2920 besitzt kein integriertes ADSL/VDSL Modem

Übersicht der möglichen Verbindungsarten:

- 1) ADSL/VDSL Modem → (Nur Vigor 2850)
diese Konfiguration erlaubt es, den Router direkt an einen ADSL/VDSL-Anschluss eines ISP (Internet Service Provider) mit dem integrierten Modem zu verbinden. Für diese Anschlussart werden die Konfigurationsparameter des ISP benötigt.
- 2) Ethernet →
diese Konfiguration erlaubt es, den Router hinter einem bestehenden Router oder ADSL/VDSL Modem zu betreiben. Dabei stellt der bestehende Router die Verbindung zum ISP zur Verfügung.
- 3) USB →
diese Konfiguration erlaubt es, ein angeschlossenes Modem (3G/4G) für den Verbindungsaufbau zu einem ISP zu verwenden. Für diese Anschlussart werden die Konfigurationsparameter des ISP benötigt.

In diesem Dokument wird die Verbindungsart 2 beschrieben. Bei dieser Verbindungsart wird der Router mit VPN-Server hinter einem bestehenden Router positioniert. Der bestehende Router verwaltet in diesem Fall die Internetverbindung zum Internet Service Provider (ISP) und besitzt die öffentliche IP-Adresse des Systems.

3.4 Konfiguration des VPN-Servers

Der Vigor 2xx0 unterstützt die folgenden Remote Access Möglichkeiten:

1) Tunneling Protokolle:

a. PPTP VPN-Service (Point-to-Point Tunneling Protocol)

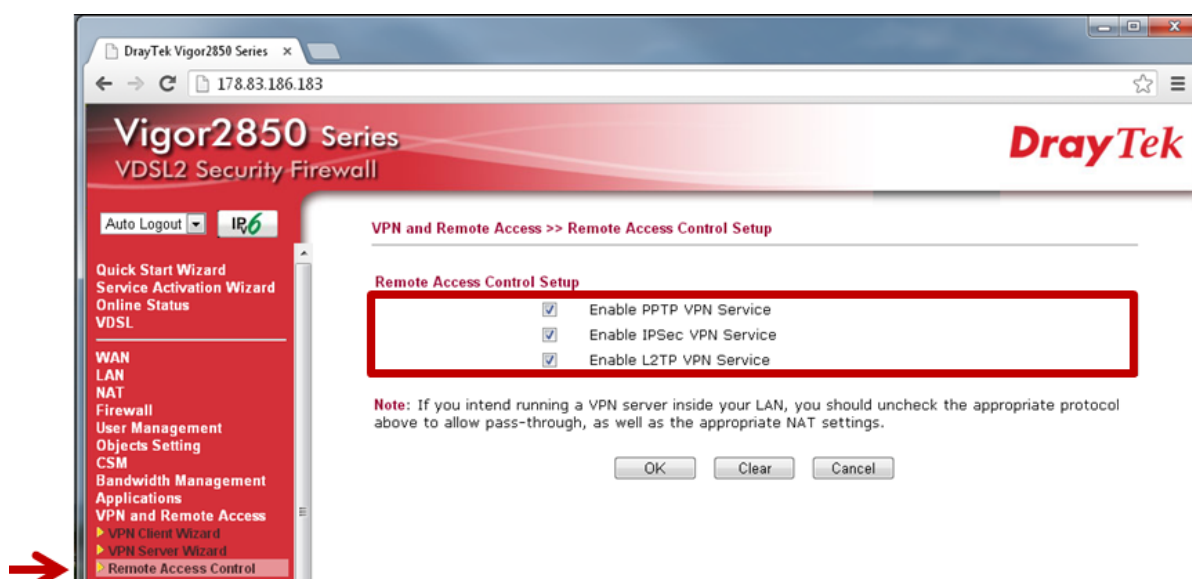
Mittels PPTP wird ein VPN geschaffen, indem ein Tunnel für das Point-to-Point Protocol gebildet wird. Es lässt Raum für jede denkbare Form der Authentifizierung und Verschlüsselung. Meist wird der TCP-Port 1723 verwendet.

b. IPSec VPN-Service (Internet Protocol Security)

IPsec ist eine Protokoll-Suite, die eine gesicherte Kommunikation über potentiell unsichere IP-Netze ermöglicht, wie beispielsweise dem Internet.

c. L2TP VPN-Service (Layer 2 Tunneling Protocol)

Tunneling auf der Layer 2 Ebene des OSI Schichtenmodells (Sicherheitsschicht). Eine Verschlüsselung ist in L2TP nicht direkt enthalten und wird daher meist in Kombination mit IPSec betrieben.



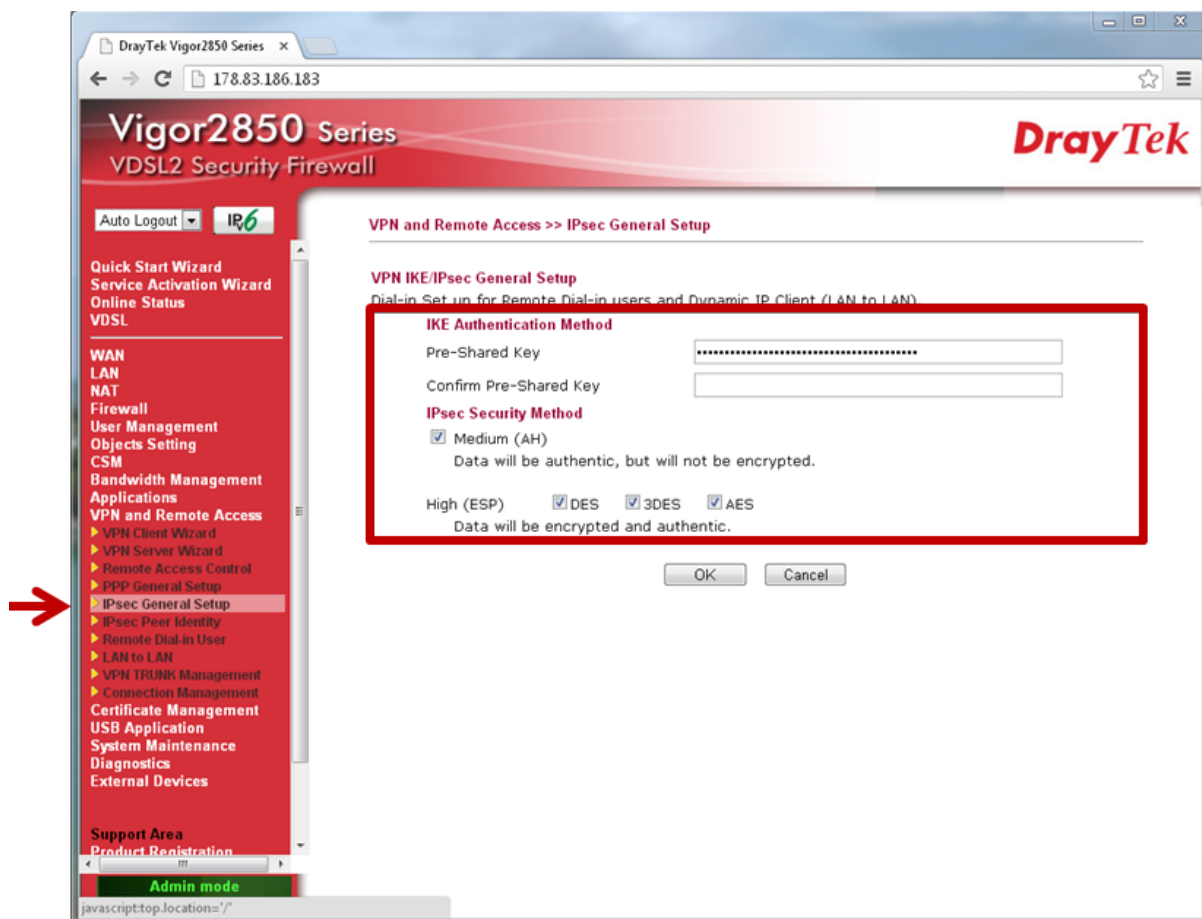
Remote Access Control Setup

Für den Aufbau der VPN-Verbindung wird in diesem Dokument L2TP beschrieben: Aktivieren Sie den Service für IPSec und L2TP.

L2TP erlaubt das Routen von Netzwerken NAT (Network Address Translation). Der VPN-Tunnel wird dabei über IPSec hergestellt.

2) IPSec Einstellungen Pre-Shared Key (PSK)

Der PSK wird beim Einstellen der Verbindungsoptionen des Clients benötigt, falls eine Verbindungsart mit IPSec gewählt wurde.

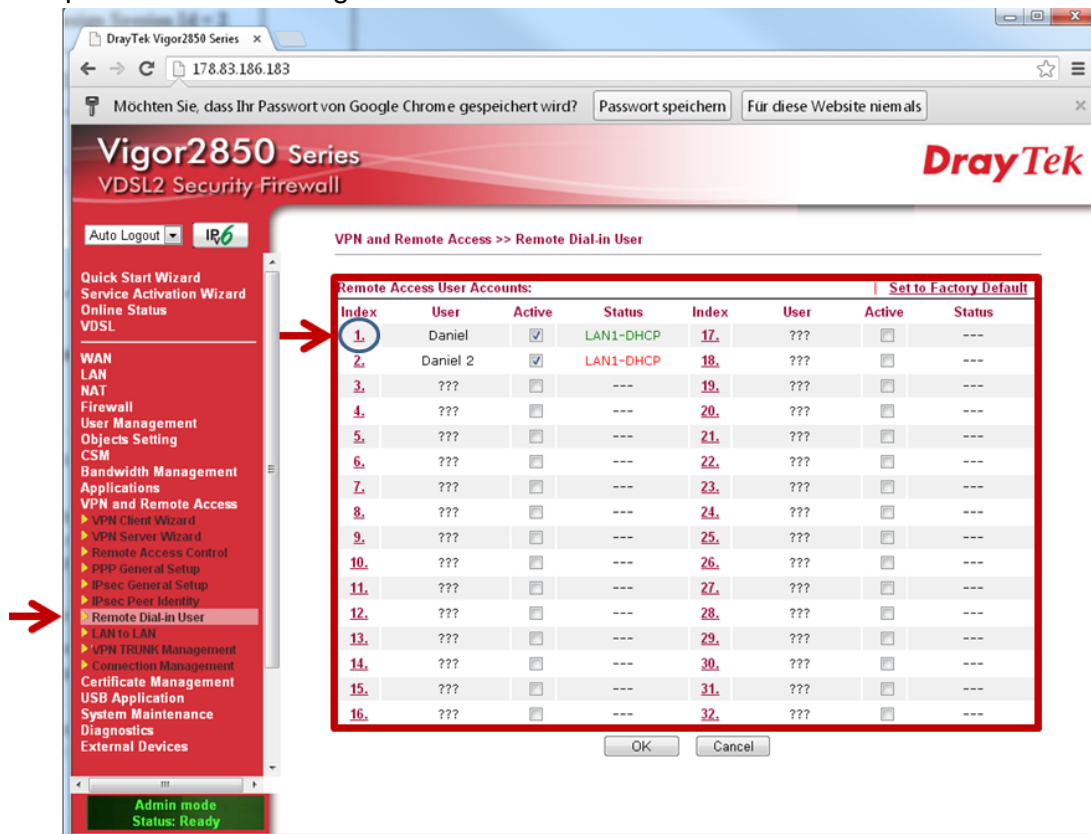


IPSec General Setup

Der PSK sollte auf keinen Fall ein Wort aus einem Wörterbuch sein.
Es wird empfohlen das Passwort mit Sonderzeichen, Zahlenkombinationen sowie eine Mindestlänge von 12 Zeichen zu definieren.

3) Remote Dial-in User

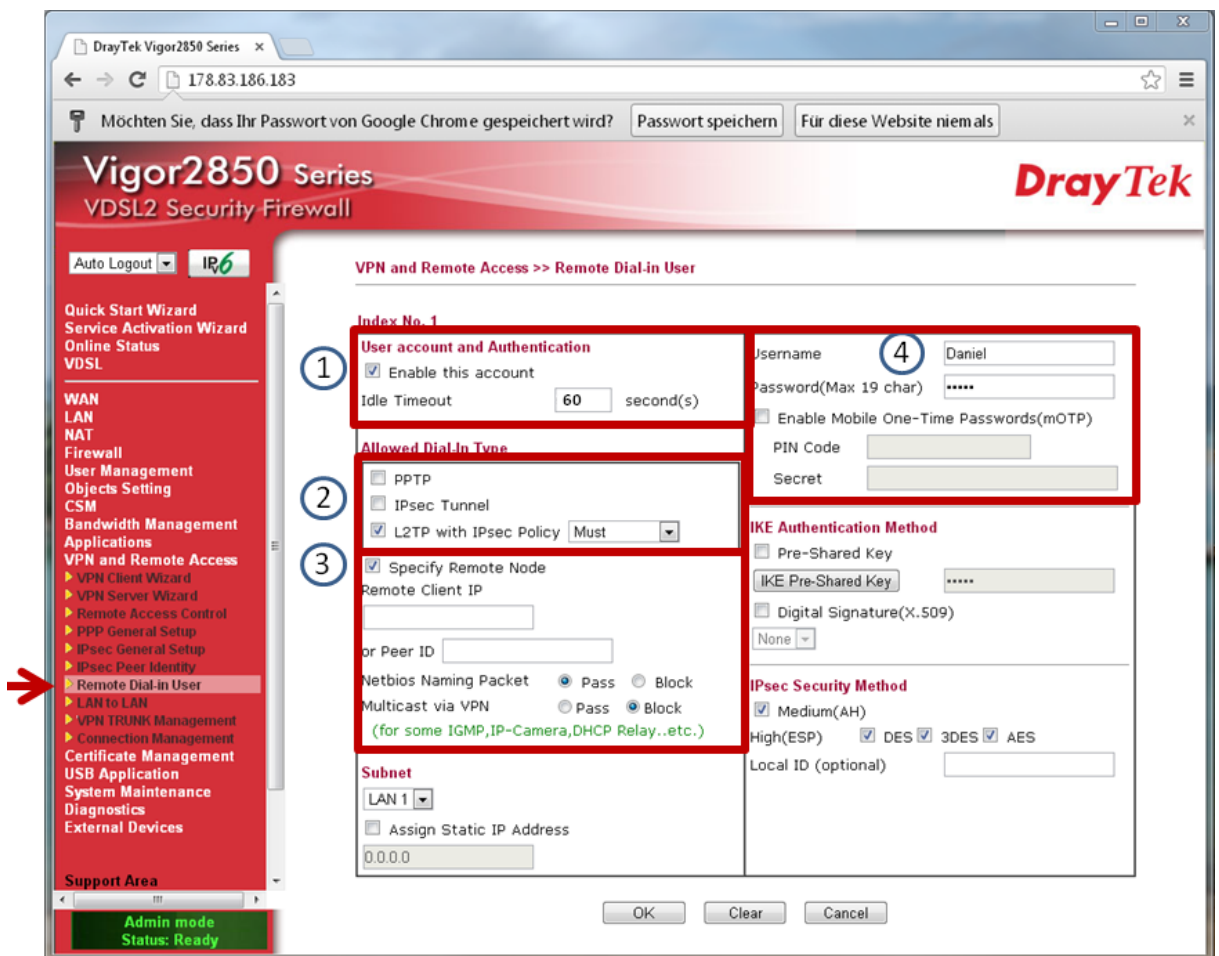
Hier können bis zu 32 Benutzer konfiguriert werden. Jeder dieser Benutzer kann sich am VPN-Server anmelden. Zum Anlegen eines neuen Benutzers muss der Index der entsprechenden Zeile angeklickt werden.



32 Remote Dial-in User

4) Remote Dial-in User Konfiguration

- 1) Den aktuell selektierten Benutzer auf aktiven Benutzer setzen:
Das Timeout auf den Wert „60“ Sekunden setzen.
- 2) Dial-in Möglichkeiten des aktuell selektierten Benutzers:
Bevorzugte Einstellung ist L2TP with IPsec Policy (Must).
In diesem Fall wird ein geschützter IPsec Tunnel zum Server hergestellt. In diesem Tunnel wiederum wird ein weiterer L2TP Tunnel aufgebaut, der erlaubt das Netzwerk zwischen Server und Client zu routen.
- 3) Specify Remote Node aktivieren.
- 4) Definition eines Benutzernamens und Passwort für die Authentifizierung.

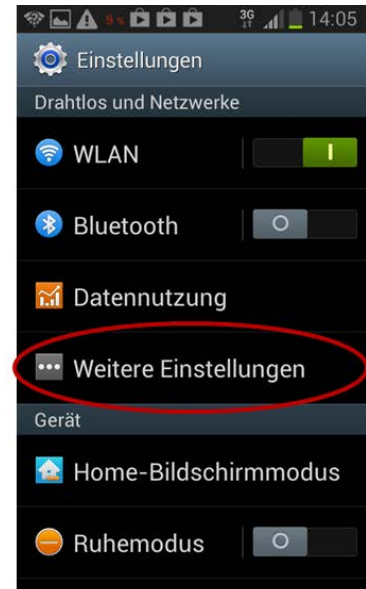


- 5) Der VPN-Server ist nun vollständig konfiguriert und wartet auf die Verbindungen von Clients.
- 6) Wenn der Client verbunden ist, kann einfach durch das Aufrufen der IP und .html Datei im Micro-Browser eine Verbindung zu Applikation hergestellt werden.

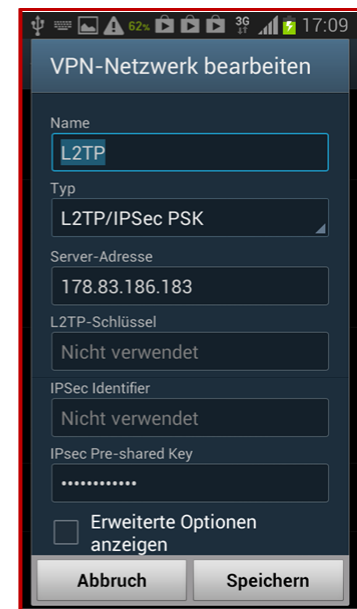
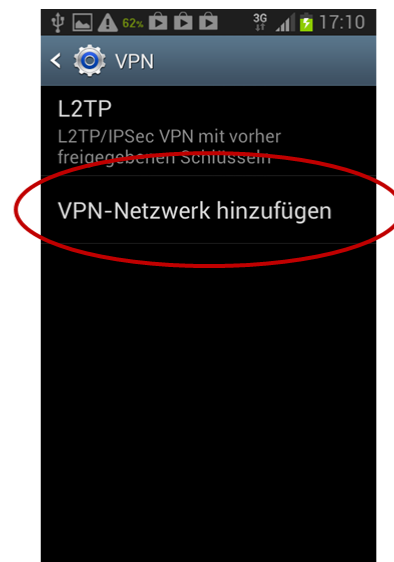
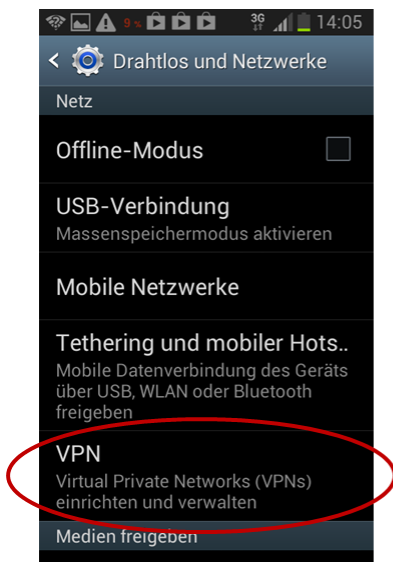
7)

3.5 Client Android System 4.1.2

Öffnen des Menüs → Einstellungen → Weiter Einstellungen:



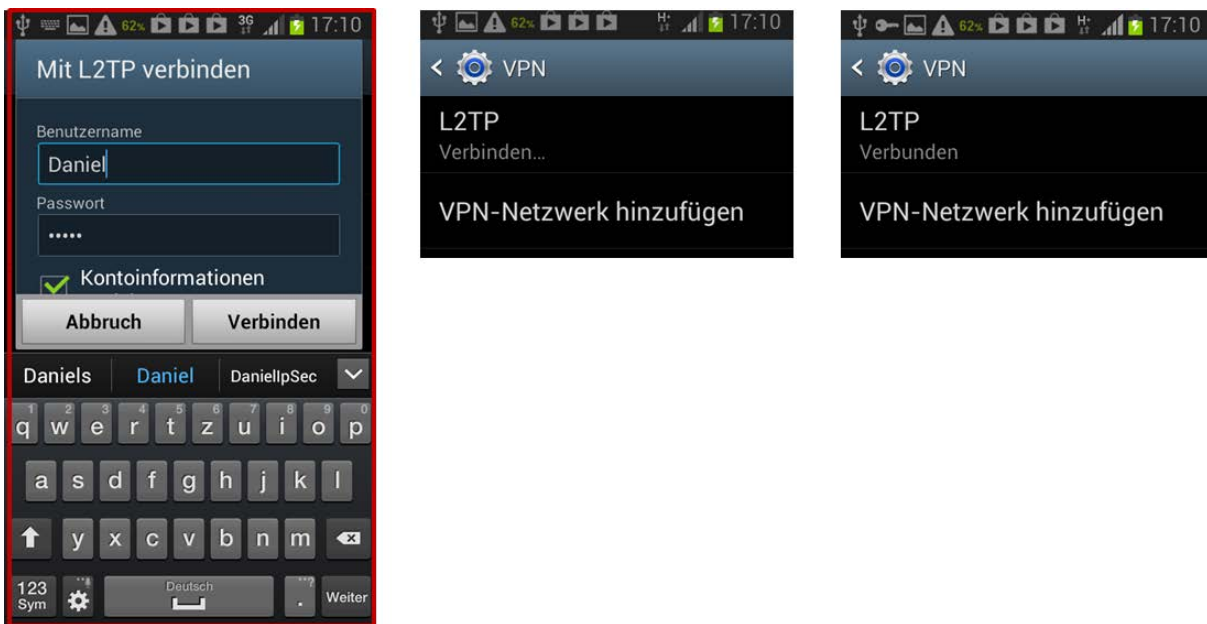
Im Untermenü befindet sich der Eintrag VPN (Virtual Private Networks), welcher es ermöglicht den Client zu konfigurieren:



Hinzufügen einer VPN-Netzwerkverbindung:

- Name = Frei definierbar
- Server-Adresse = Öffentliche IP-Adresse oder DNS-Name des DSL-Routers
- L2TP-Schlüssel = wird bei aktueller Router-Konfiguration nicht verwendet
- IPsec Pre-shared Key = Schlüssel, welcher im Router IPsec General Setup hinterlegt wurde
- Speichern

Öffnen der angelegten VPN-Netzwerkverbindung:



- Benutzername und Passwort, die in der Remote Dial-in User Konfiguration hinterlegt wurden:

Username	<input type="text" value="Daniel"/>
Password(Max 19 char)	<input type="password" value="....."/>
<input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)	
PIN Code	<input type="text"/>
Secret	<input type="text"/>

3.6 Client iPhone / iPad

Zum Erstellen einer L2TP/IPSec Verbindung, sind mit einem I-OS Gerät folgende Schritte notwendig:

- 1) Öffnen der „Einstellungen“ . Unter dem Menü Punkt „Allgemein“ „VPN“ wählen:



- 2) Hinzufügen einer neuen VPN Verbindung:



- 3) Erstellen einer L2TP-IPSec Verbindung mit einem entfernten VPN-Server.
Benötigte Einstellungen oder Angaben:
- ➔ Beschreibung: Frei definierbar
 - ➔ Server: IP-Adresse oder DNS des VPN-Servers
 - ➔ Account: User Profil mit VPN-Zugriffsrechte auf den VPN-Server
 - ➔ Kennwort: Das für dieses User Profil hinterlegte Passwort
 - ➔ Shared Secret: Der für den VPN-Tunnel hinterlegte Pre-Shared Key (PSK)

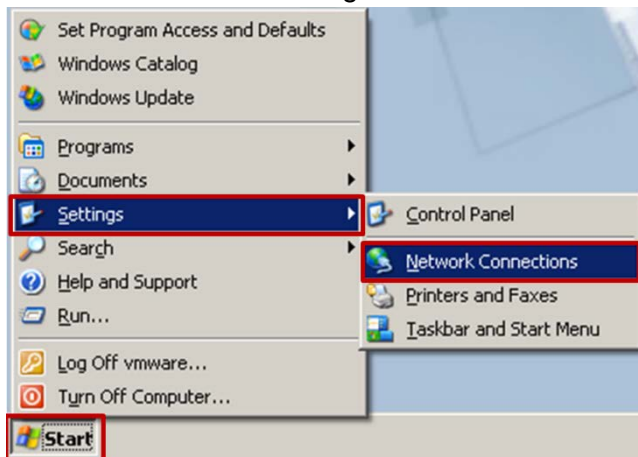


- 4) Selektieren des für den VPN-Zugriff verwendeten Tunnels und aktivieren dieses Tunnels. Es ist im Statusfeld ersichtlich, dass der Tunnel erfolgreich aufgebaut wurde:

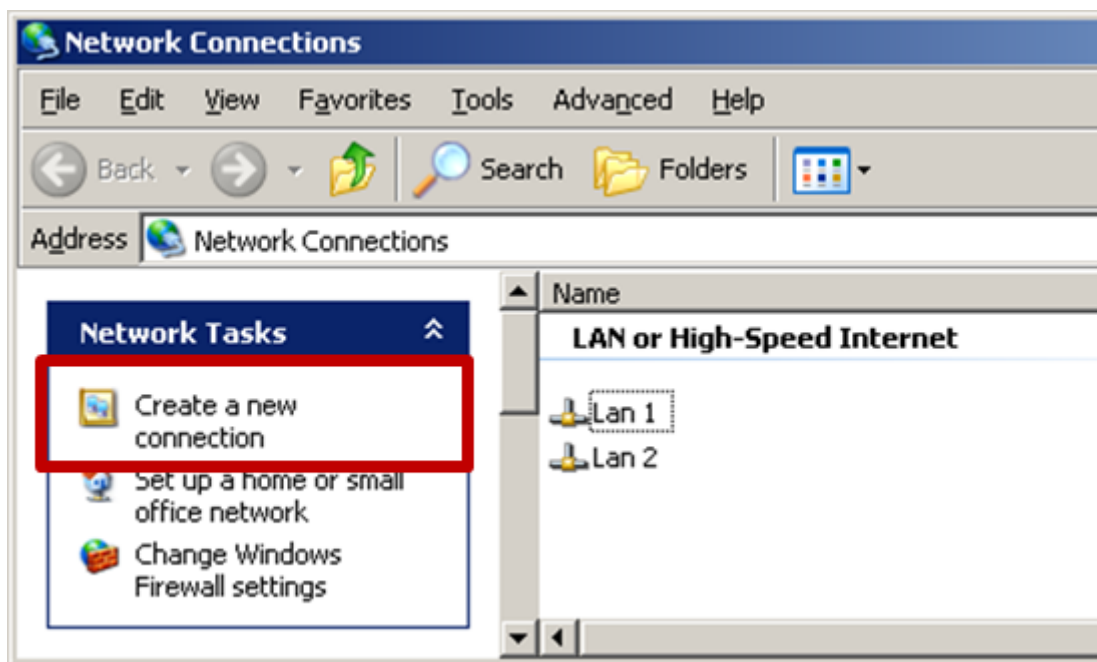


3.7 Client Microsoft Windows XP

1) Öffnen der Netzwerk-Konfiguration:



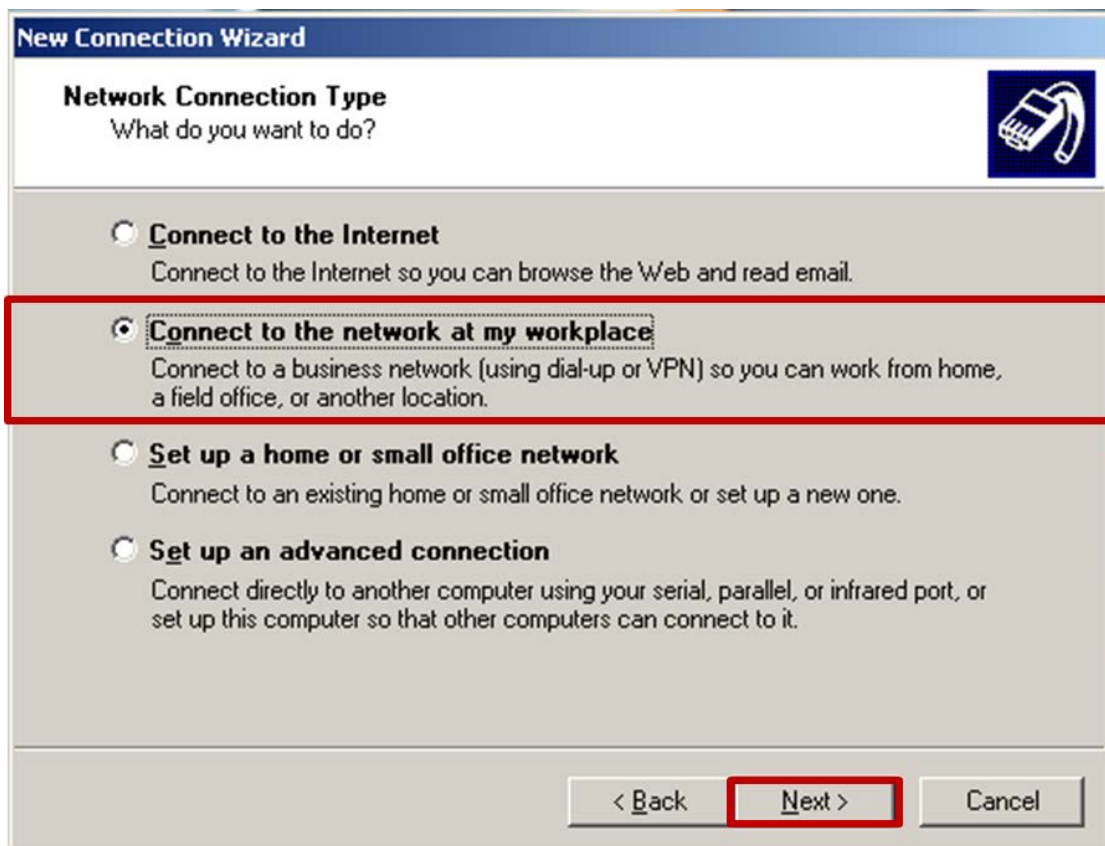
2) Neue Verbindung erstellen:



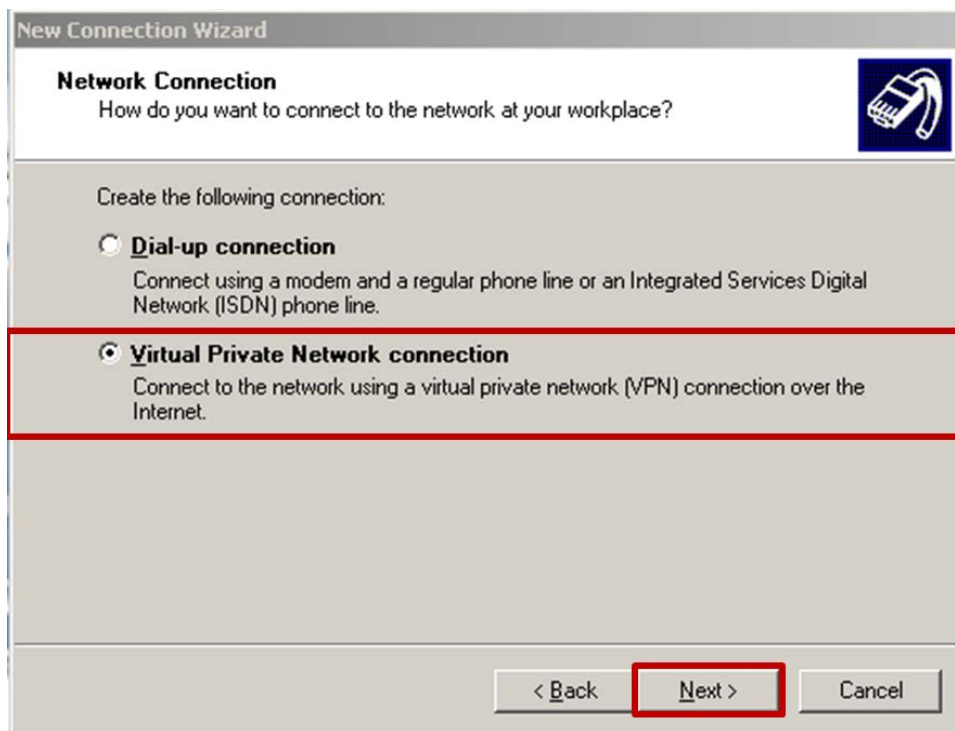
3) Wizard zum Erstellen einer neuen Verbindung wird geladen:



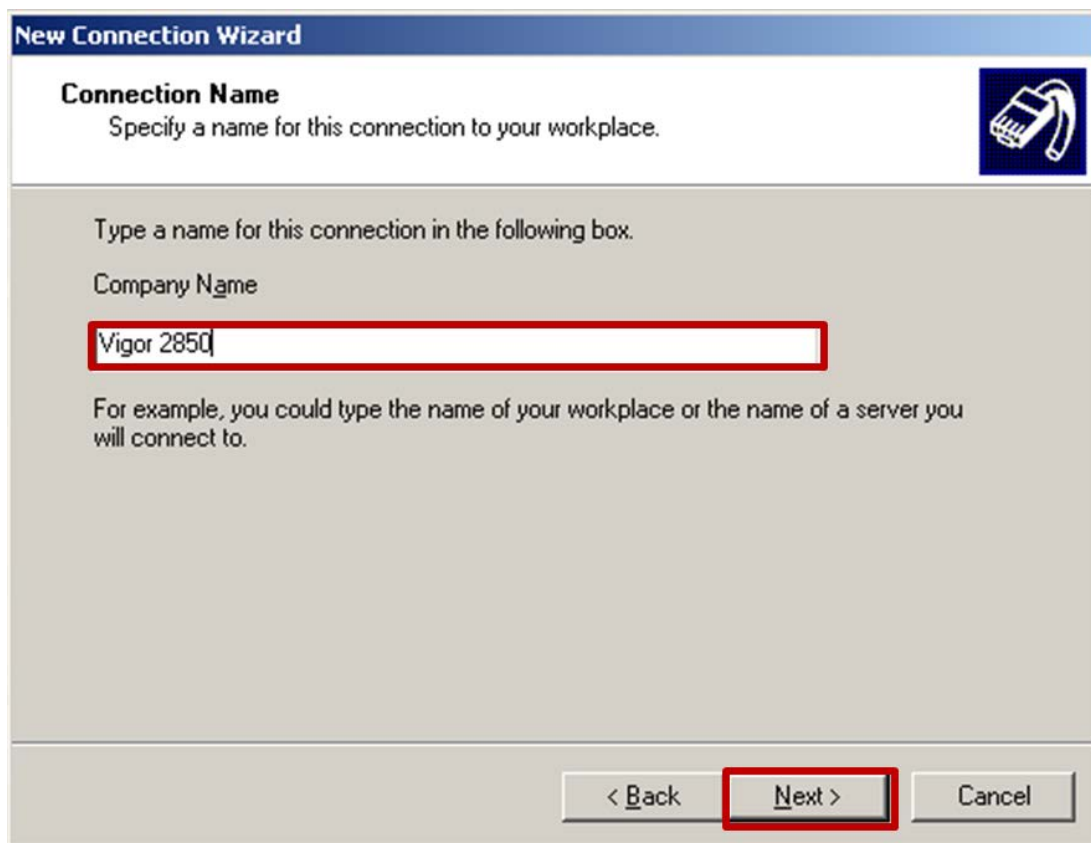
4) Verbindung mit Arbeitsplatz herstellen (VPN):



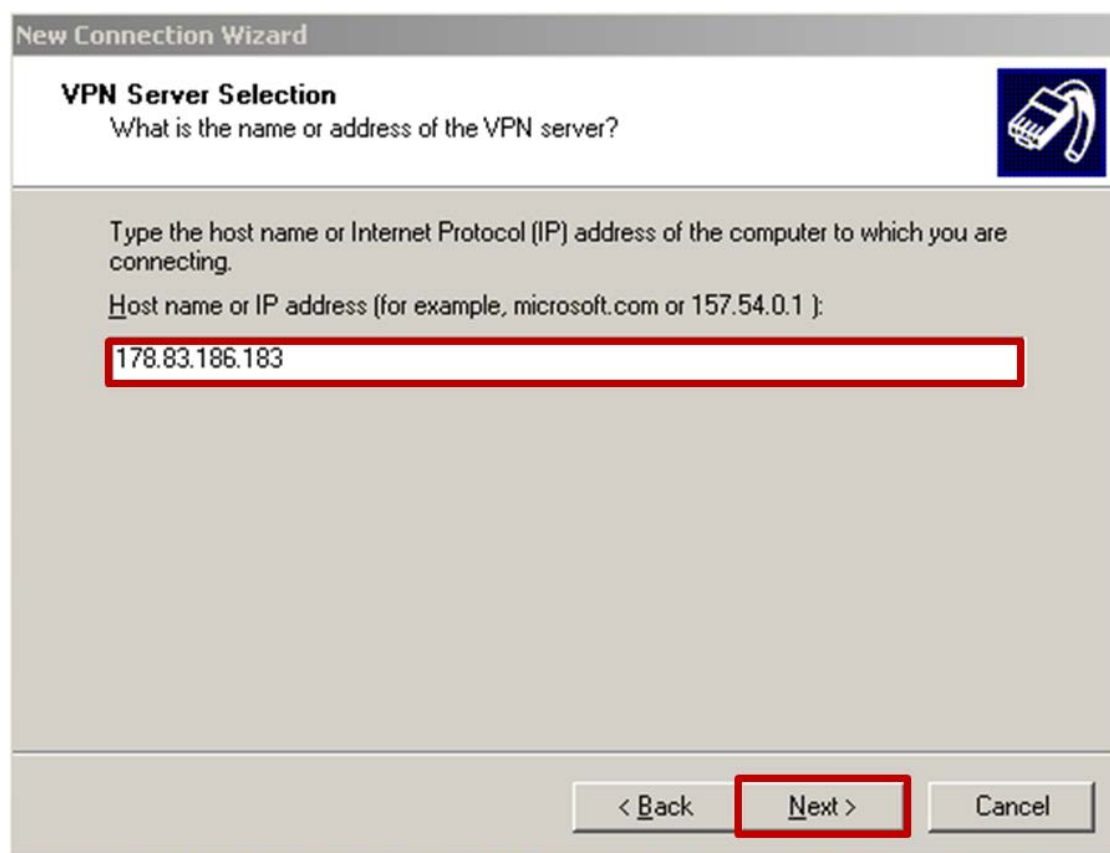
5) Virtual Private Network Verbindung (VPN):



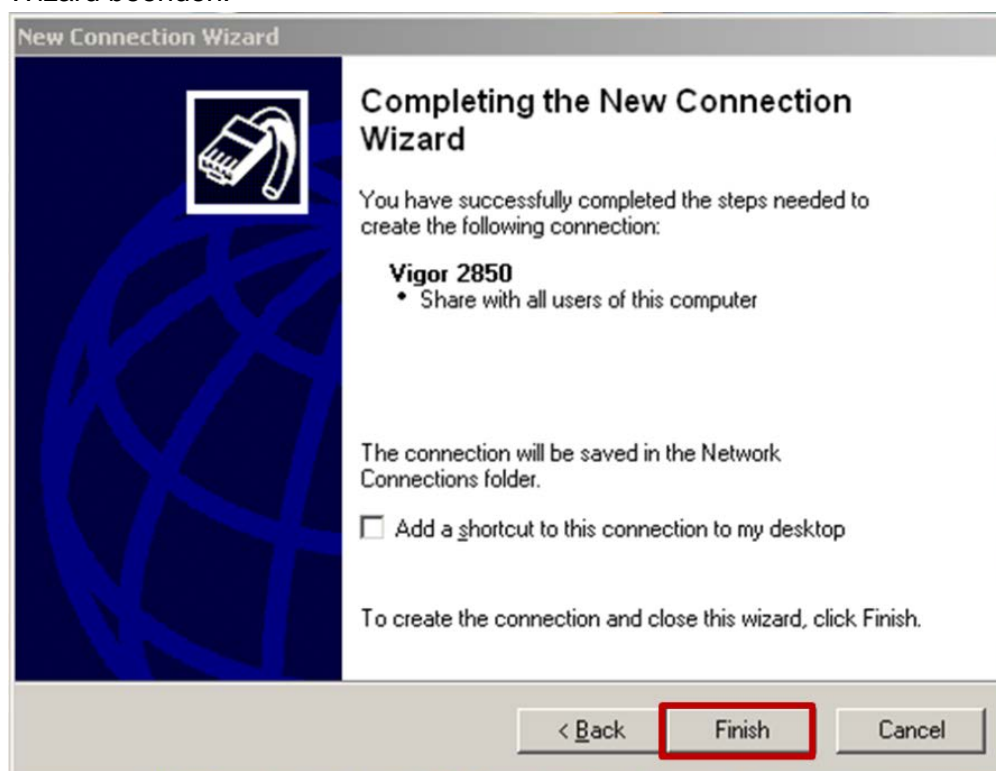
6) Name des VPN:



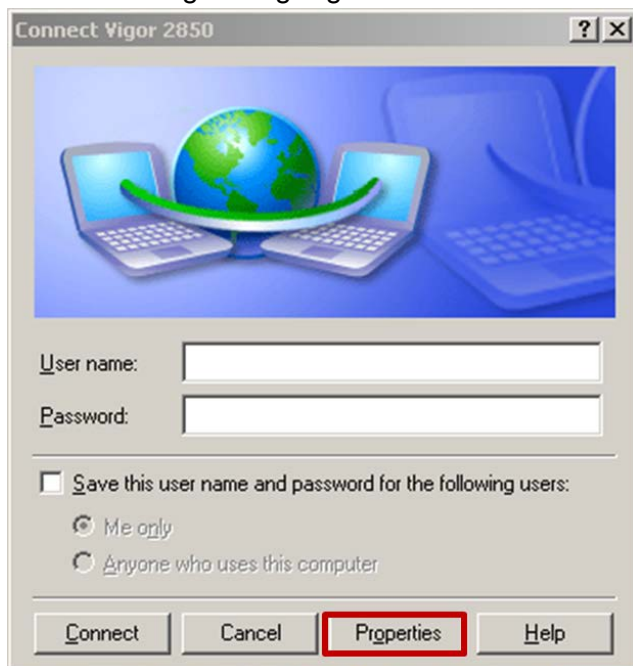
7) VPN-Server Adresse:



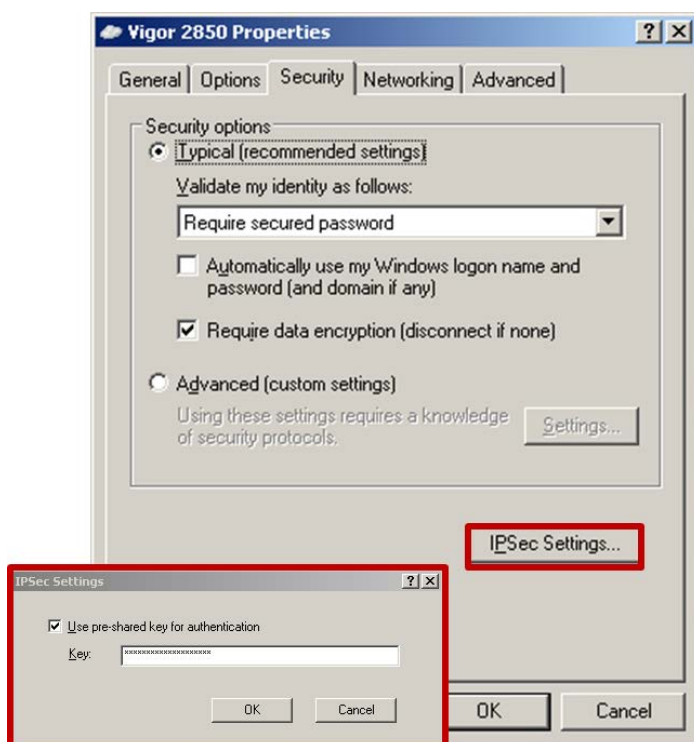
8) Wizard beenden:



9) Im Verbindungsdialog Eigenschaften selektieren:



10) Tab Sicherheit → IPSec Einstellungen → IPSec Schlüssel eingeben:



11) Benutzername und Passwort des VPN-Benutzers eingeben:



12) Verbindung wurde Hergestellt:



13) Der PC ist nun ein Teilnehmer des gegenüberliegenden Netzwerkes. Der Zugriff auf die Geräte ist mit allen Applikationen die Ethernet unterstützen möglich:

- Browser
- PG5



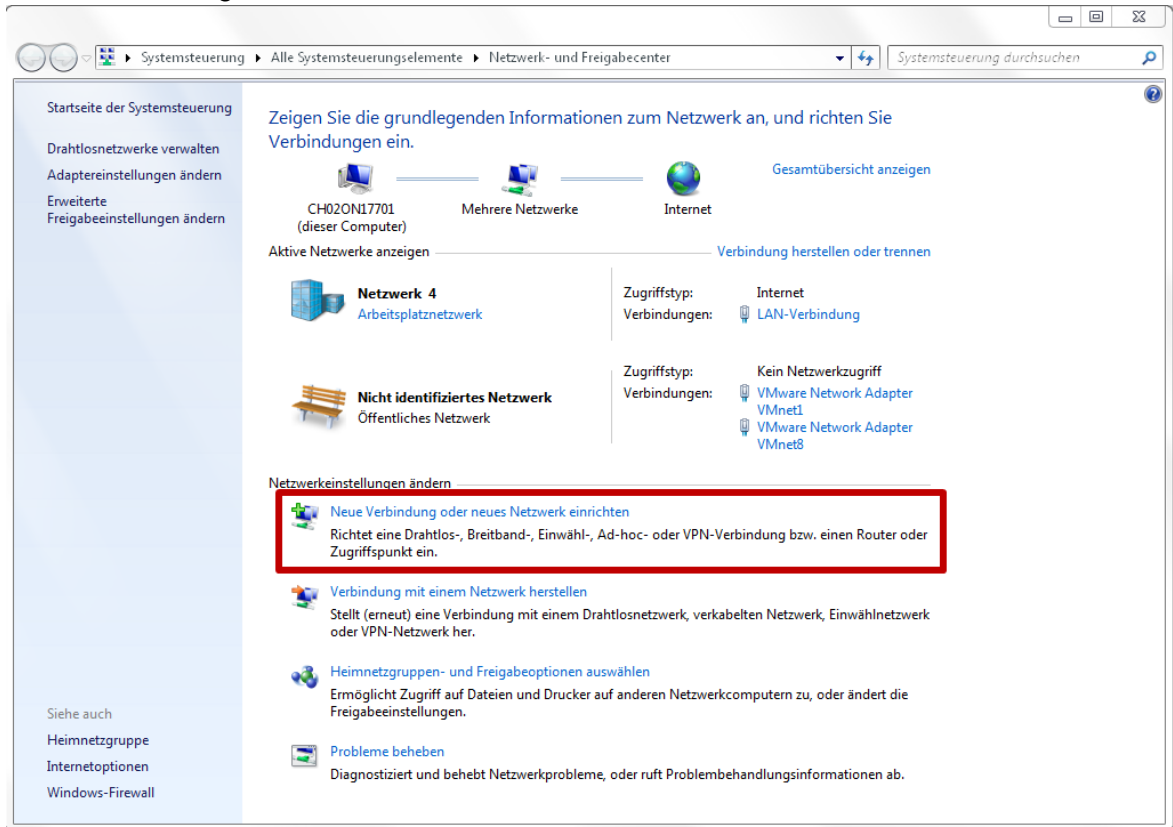
3.8 Client Microsoft Windows 7

Einrichten einer VPN-Verbindung in einem Windows 7 System. Für das Einrichten einer VPN-Verbindung werden Administrationsrechte benötigt.

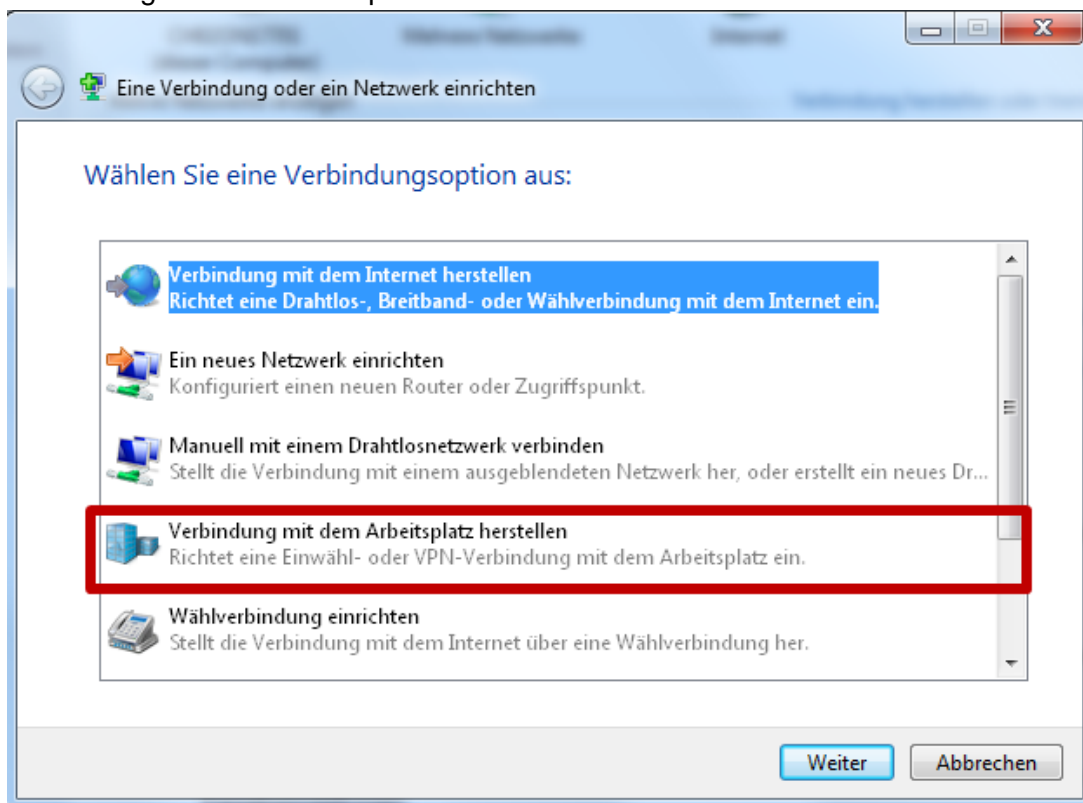
- 1) Öffnen des Netzwerk und Freigabecenters:



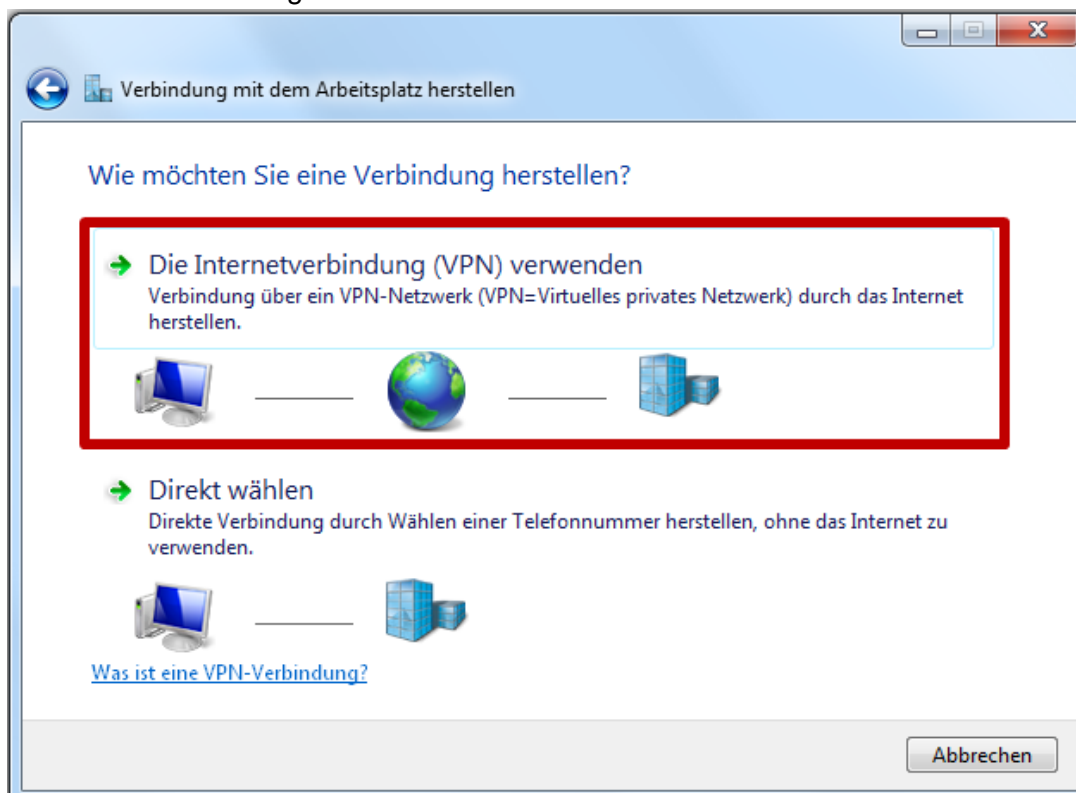
- 2) Neue Verbindung zu einem Netzwerk einrichten:



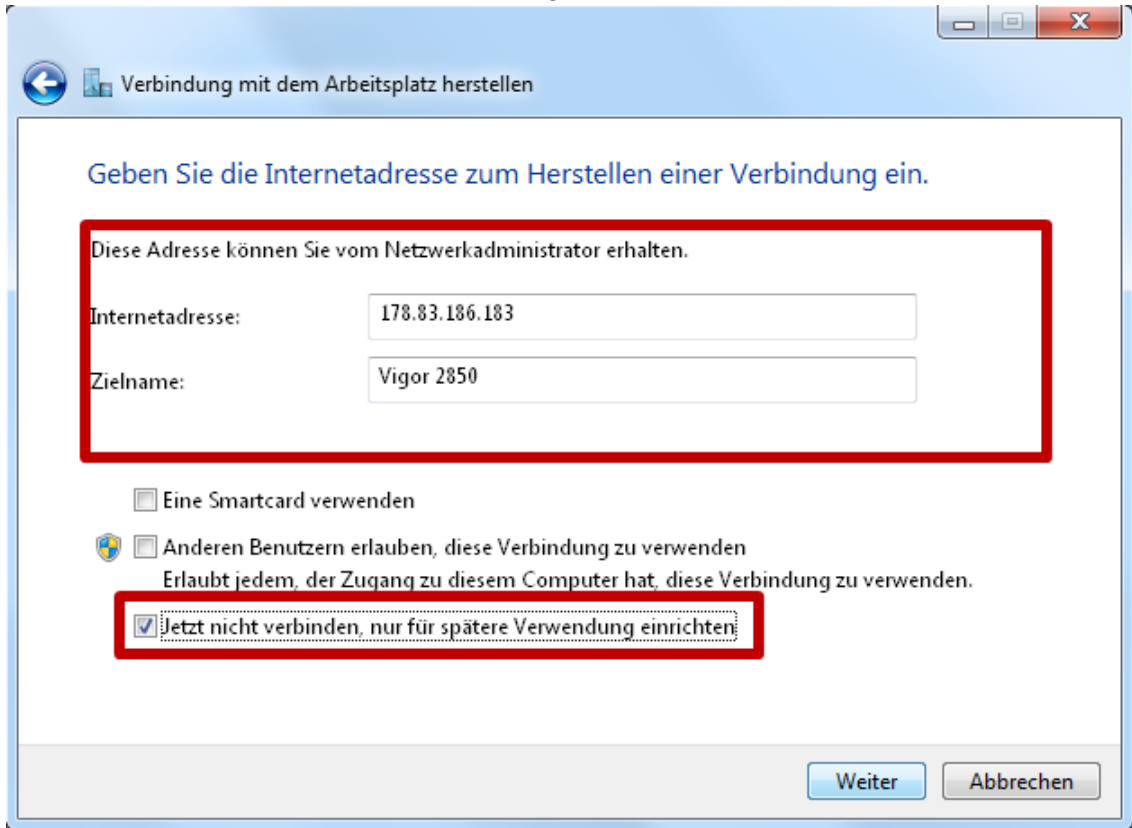
3) Verbindung mit dem Arbeitsplatz herstellen:



4) Die Internetverbindung verwenden:



5) Internetadresse und Name der Verbindung definieren:



Verbindung mit dem Arbeitsplatz herstellen

Geben Sie die Internetadresse zum Herstellen einer Verbindung ein.

Diese Adresse können Sie vom Netzwerkadministrator erhalten.

Internetadresse: 178.83.186.183

Zielname: Vigor 2850

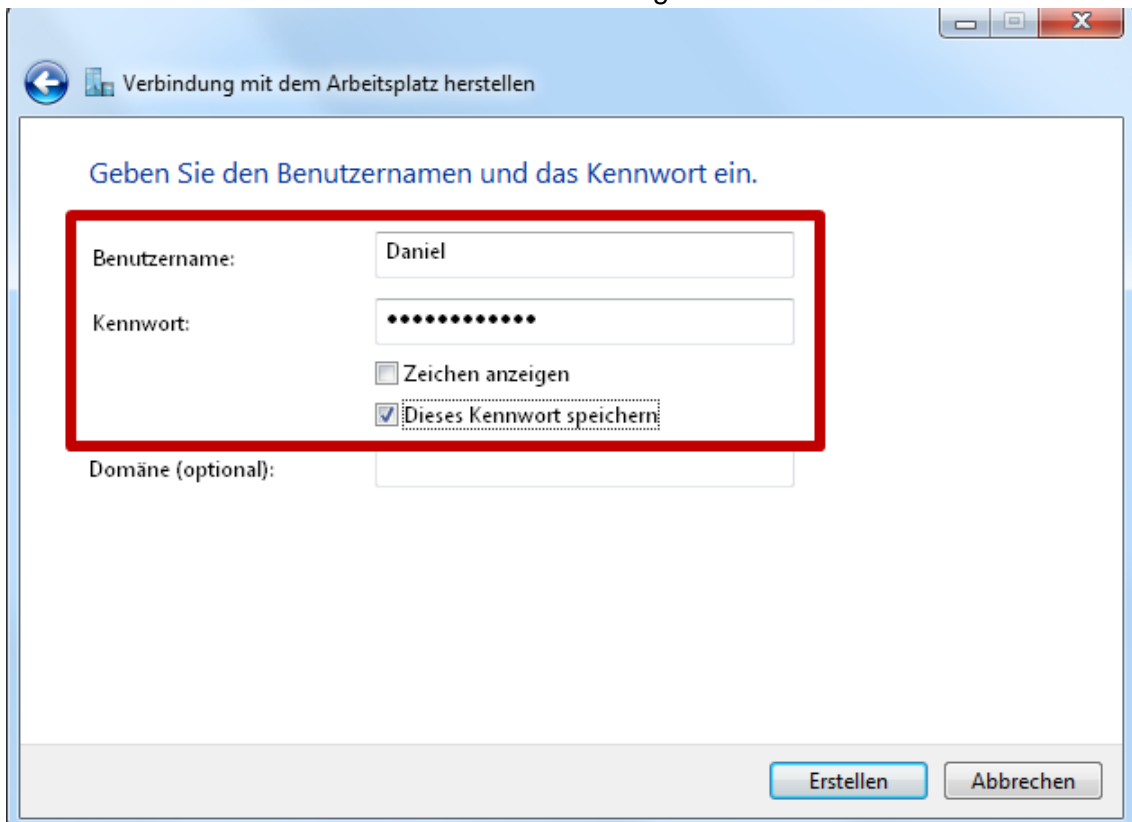
Eine Smartcard verwenden

Anderen Benutzern erlauben, diese Verbindung zu verwenden
Erlaubt jedem, der Zugang zu diesem Computer hat, diese Verbindung zu verwenden.

Jetzt nicht verbinden, nur für spätere Verwendung einrichten

Weiter Abbrechen

6) Benutzername und Kennwort des VPN-Server eingeben:



Verbindung mit dem Arbeitsplatz herstellen

Geben Sie den Benutzernamen und das Kennwort ein.

Benutzername: Daniel

Kennwort: [masked]

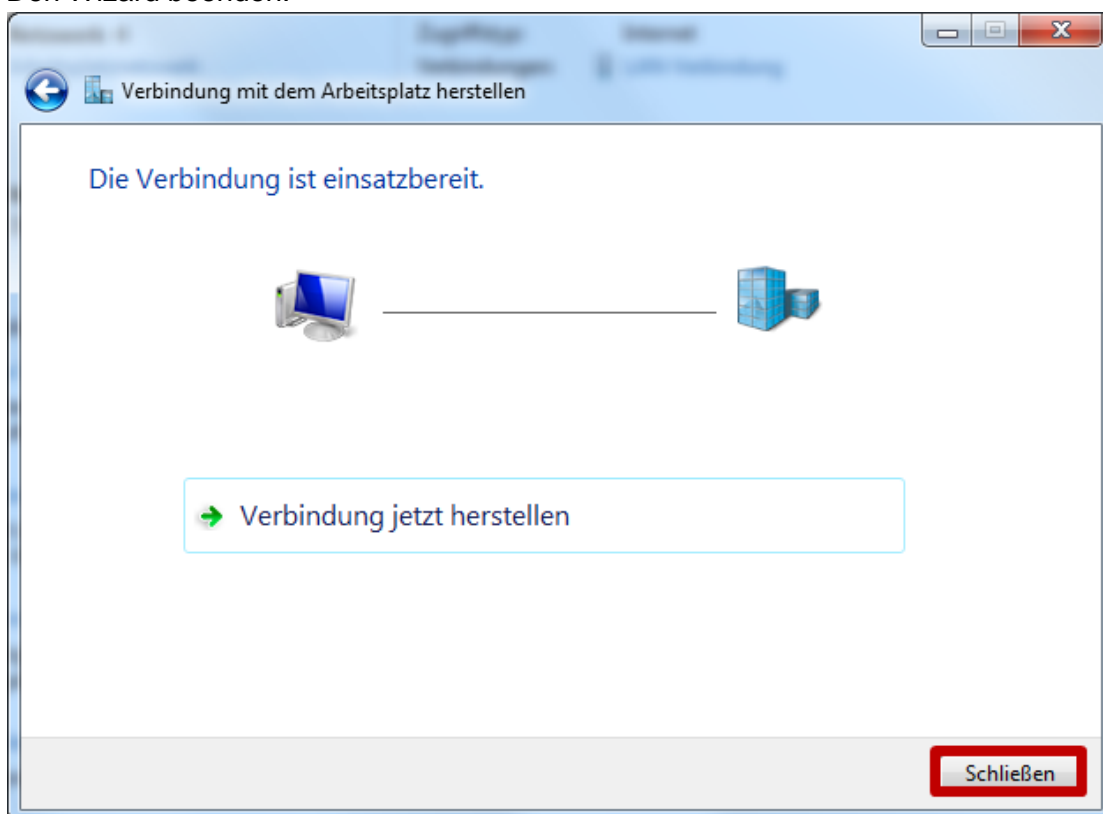
Zeichen anzeigen

Dieses Kennwort speichern

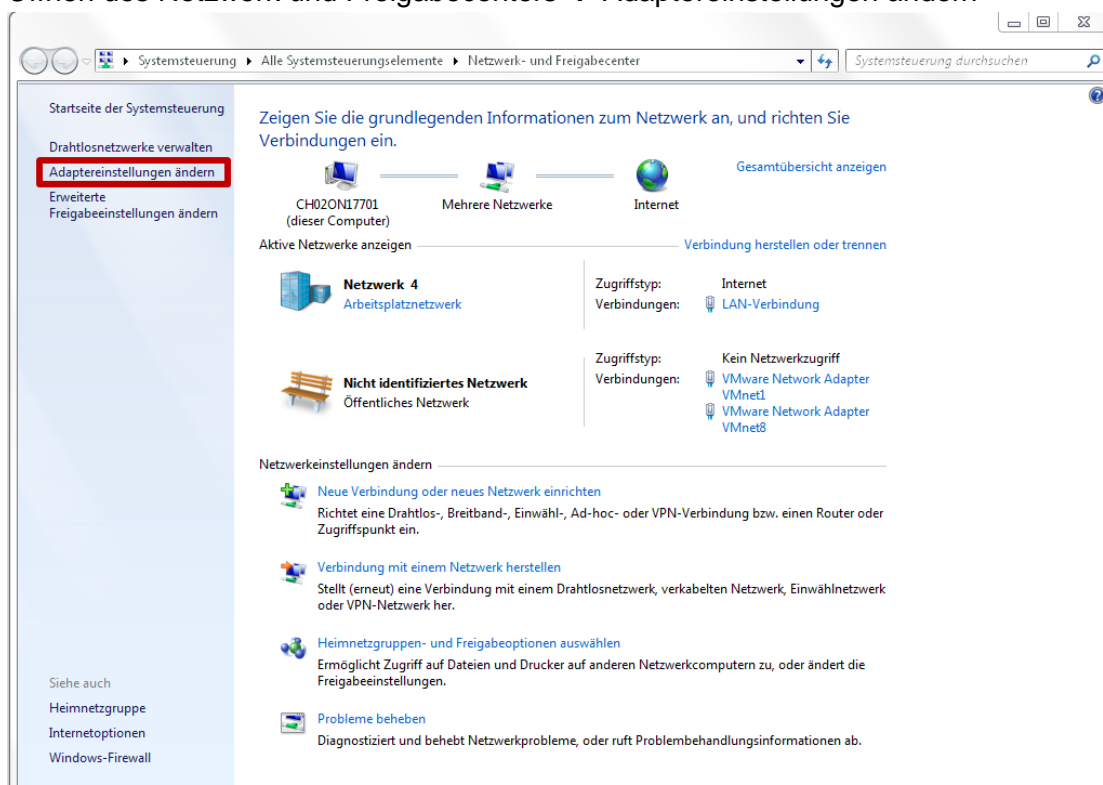
Domäne (optional):

Erstellen Abbrechen

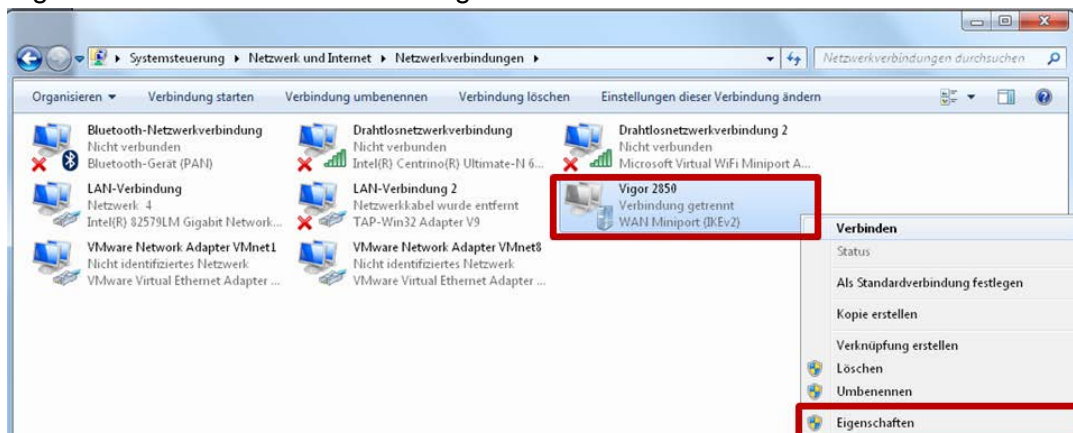
7) Den Wizard beenden:



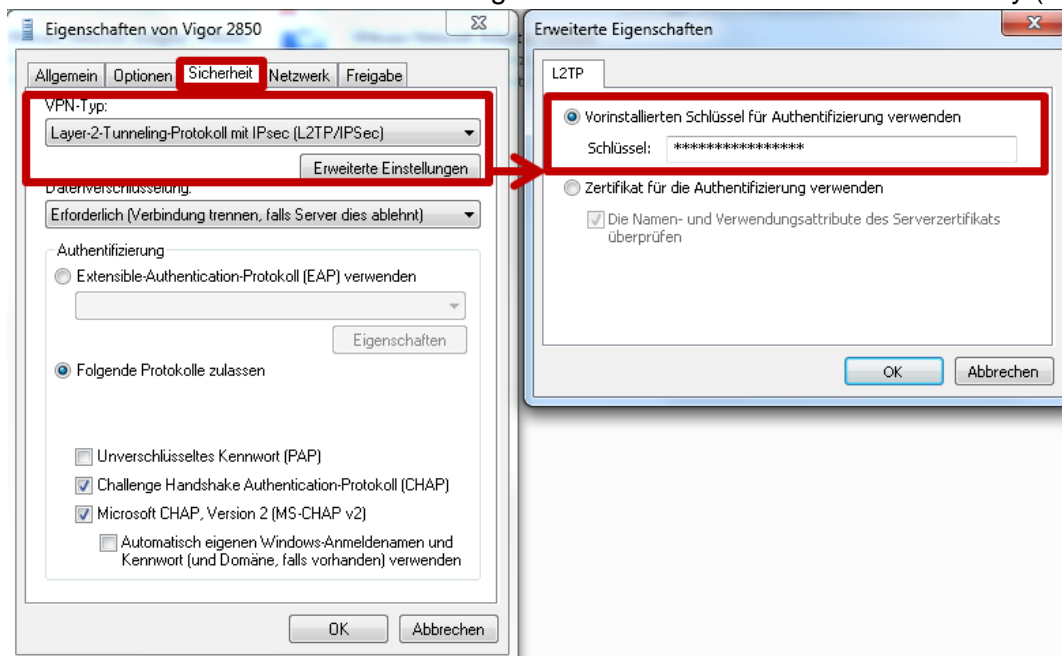
8) Öffnen des Netzwerk und Freigabecenters → Adaptereinstellungen ändern



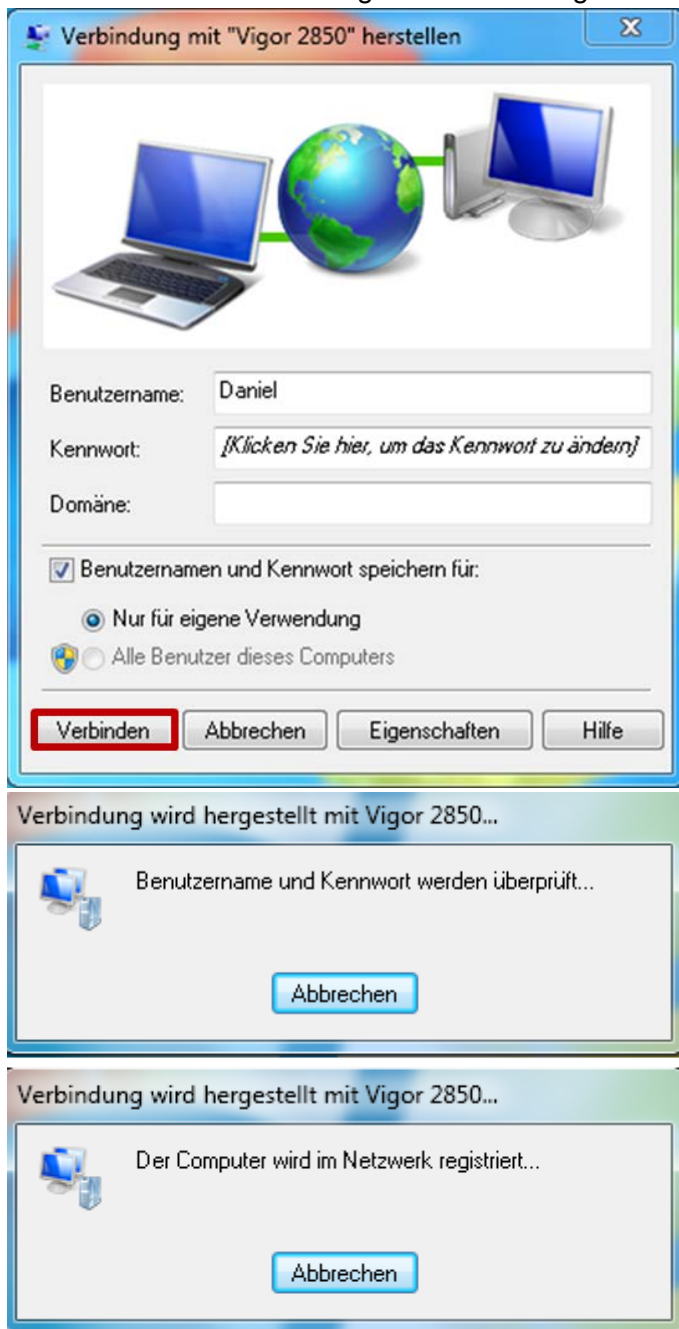
9) Eigenschaften der VPN-Verbindung öffnen:



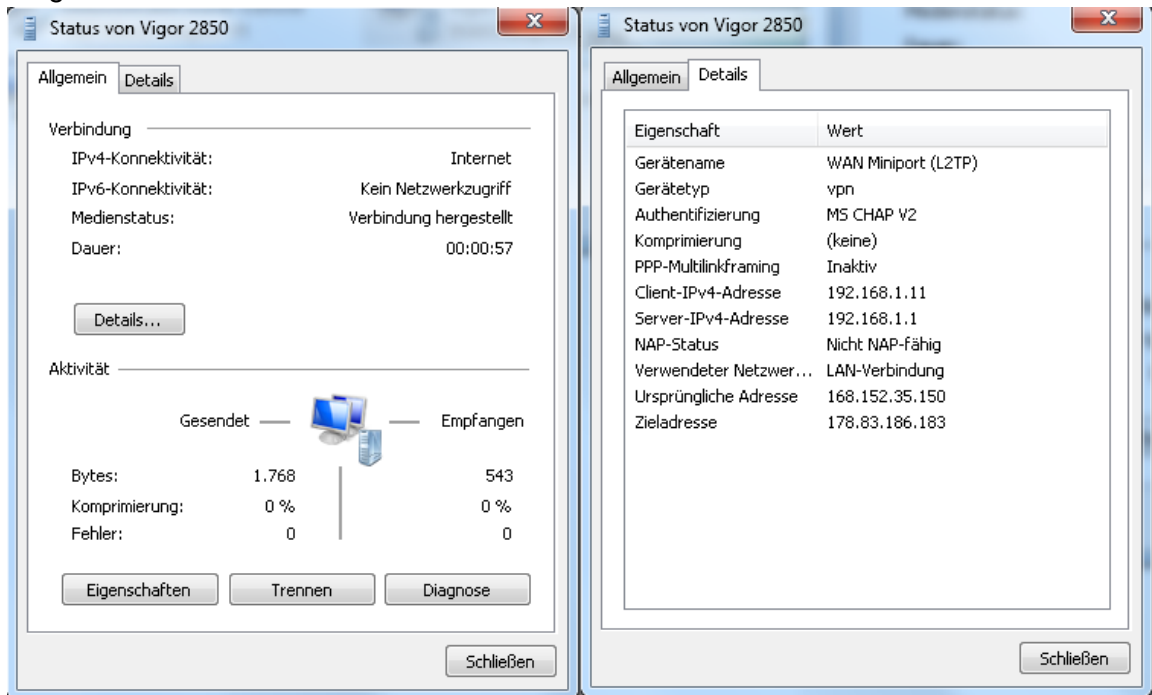
10) Einstellen der L2TP/IPSec Verbindung und setzen des IPSec Pre-Shared Key (PSK):



11) Öffnen der VPN-Verbindung und Verbindung herstellen



12) Verbindung wurde aufgebaut, IP-Adressen vom DHCP-Servers des Routers wurden vergeben



13) Der PC ist nun ein Teilnehmer des gegenüberliegenden Netzwerkes. Der Zugriff auf die Geräte ist mit allen Applikationen die Ethernet unterstützen möglich.

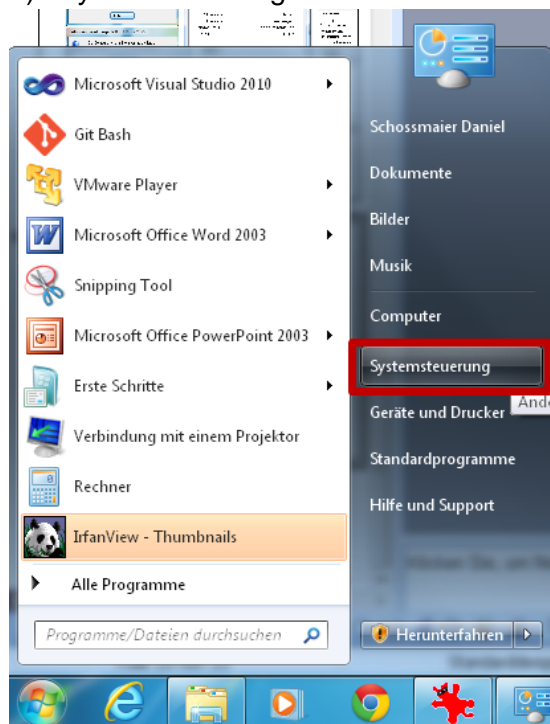
- ➔ Browser
- ➔ PG5



3.9 Fehlerbehandlung Windows:

Im Fall, dass die Verbindung nicht erfolgreich hergestellt wurde, überprüfen Sie bitte die folgenden Punkte und wiederholen Sie den Vorgang ab Punkt 15 erneut.
Aktivieren des IPsec Policy Agent und des IKE and AuthIP IPsec Keying Modules.

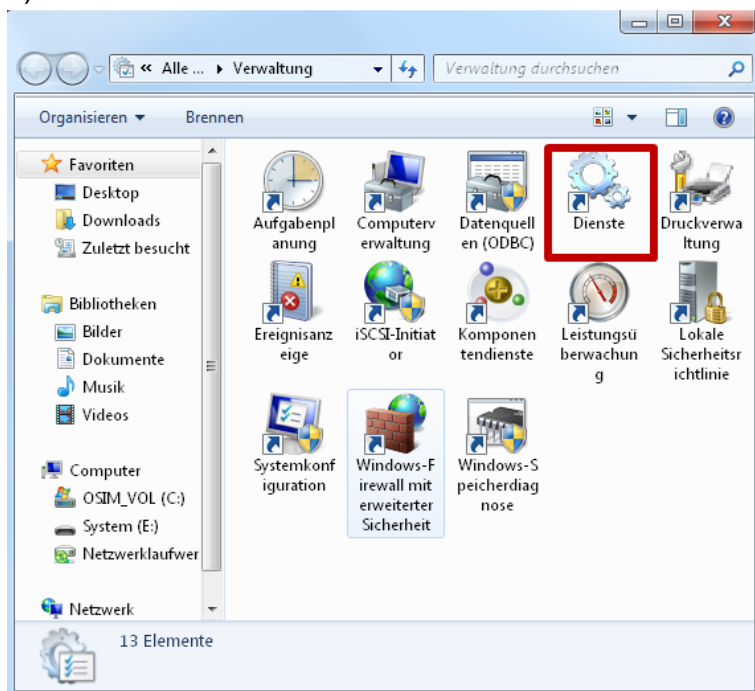
1) Systemsteuerung öffnen:



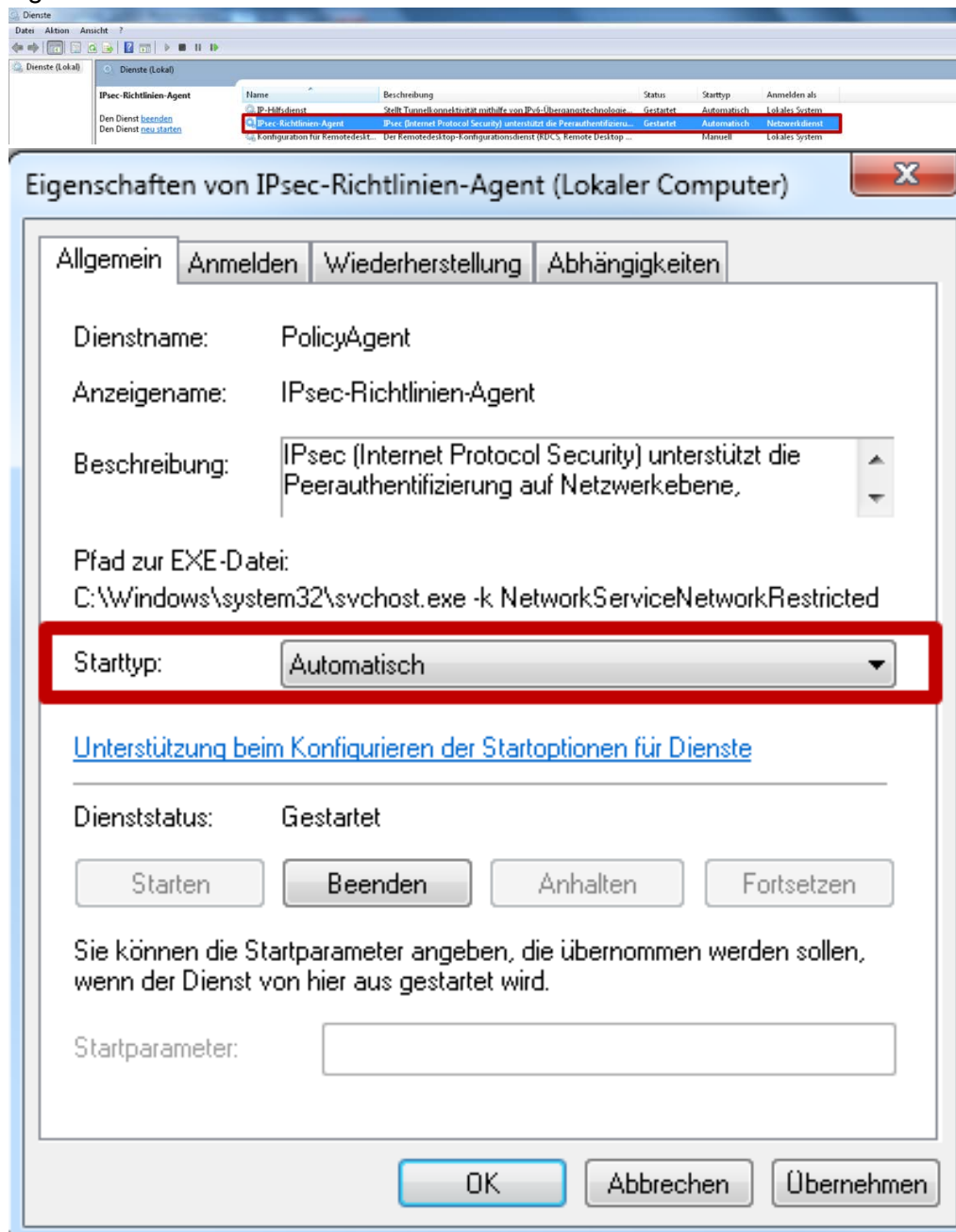
2) Verwaltung öffnen:



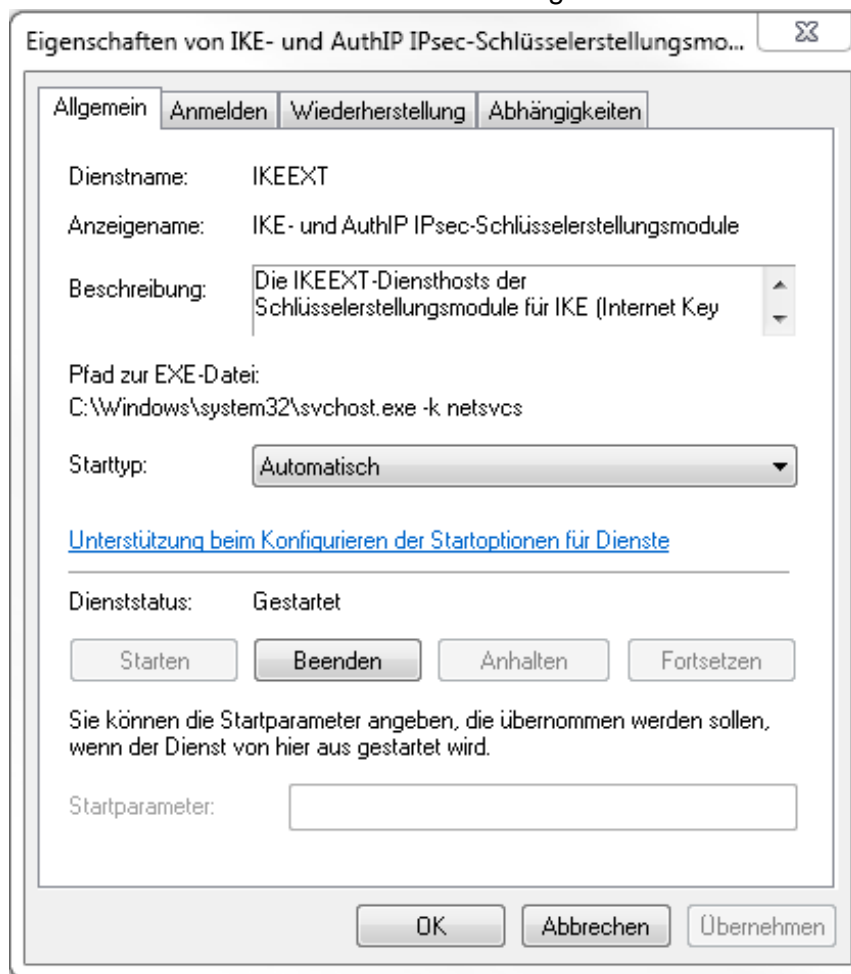
3) Fenster der Dienste öffnen:



- 4) Dienste starten
(IPsec-Richtlinien-Agent und IKE und AuthIP IPsec-Schlüsselerstellungsmodule)
 - a. IPsec-Richtlinien-Agent

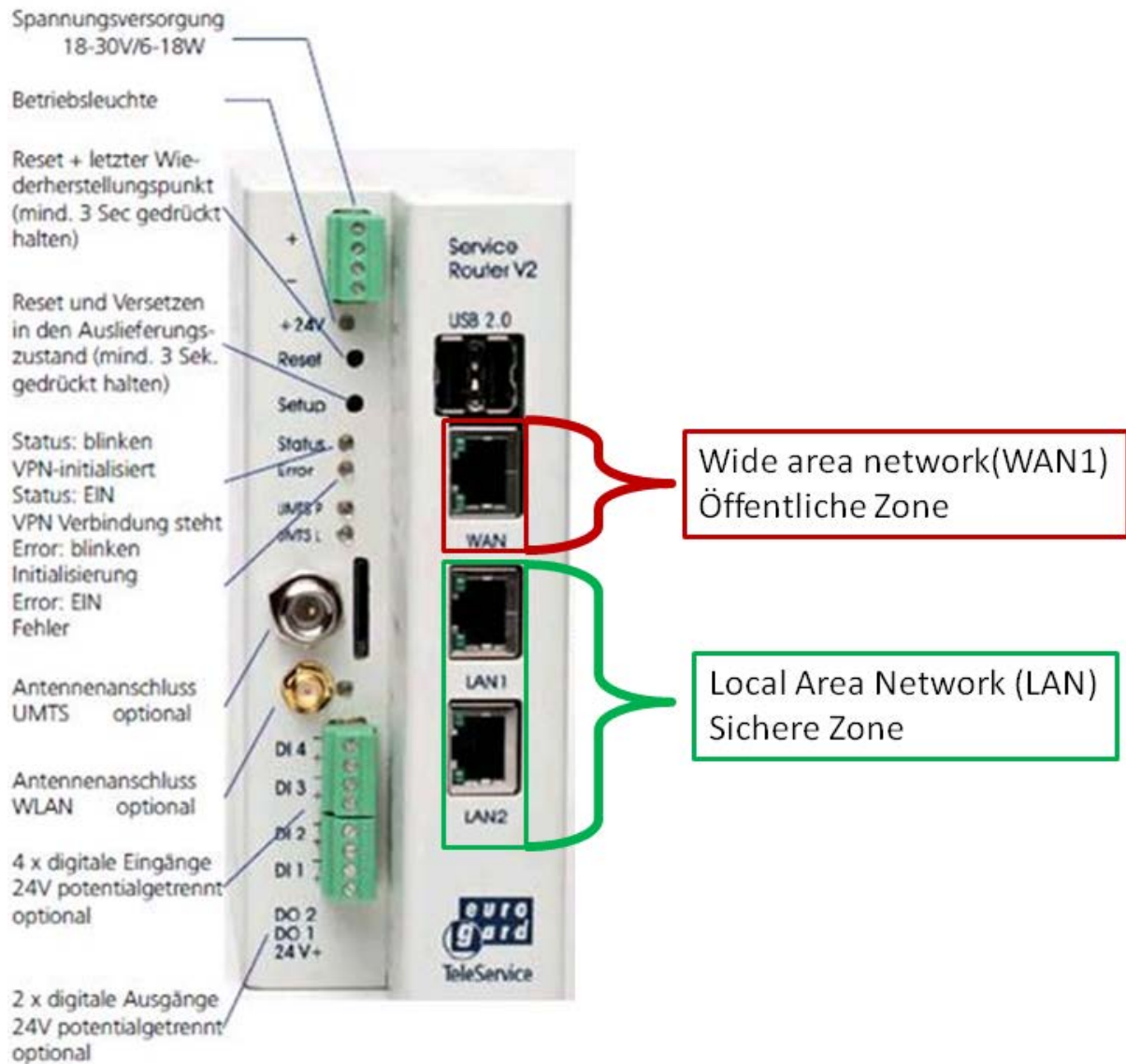


b. IKE- und AuthIP IPsec-Schlüsselerstellungsmodule:



4 EuroGard Service Router 2

Der Router sollte immer beginnend mit den Einstellungen für das lokalen Netzwerk (LAN) und anschließend für den VPN-Server konfiguriert werden. Grund hierfür ist, dass Parameter der lokalen Konfiguration und die Systemzeit beim Generieren des Server-Zertifikates im Router verwendet werden.



Wide Area Network (WAN) → Verbindung zum Router mit öffentlichen IP-Adresse

Local Area Network (LAN) → Verbindung zum lokalen Netzwerk

4.1 Öffnen des Setup Menüs

Zum Einrichten des Eurogard Service Router V2 muss der PC mit einer LAN-Schnittstelle des Routers verbunden werden. Der Router wird mit einem aktivierten DHCP-Server ausgeliefert. Es sollte deshalb vermieden werden, den Eurogard Service Router V2 zu mit Werkskonfiguration in eine Ethernet-Infrastruktur mit bereits vorhandenem DHCP-Server zu konfigurieren.

Empfohlen:

Trennen Sie ihren PC von allen bestehenden Netzwerkverbindungen.

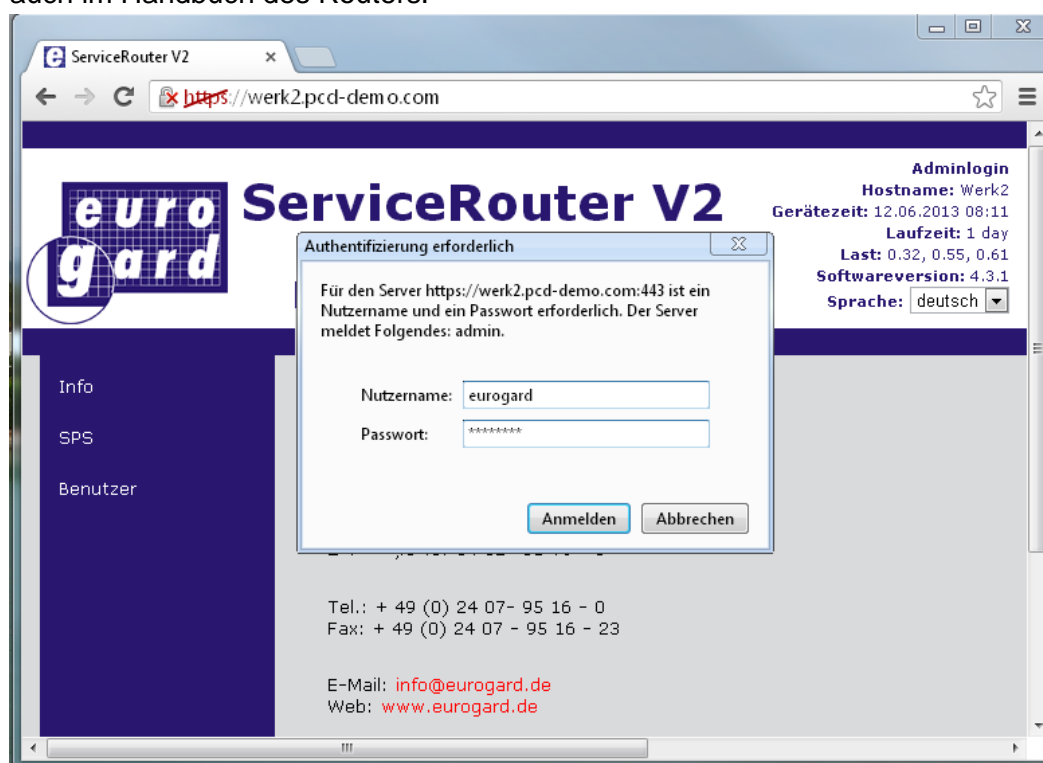
Verbinden Sie ihren PC direkt mit dem Router.

Die Standard IP-Adresse des Routers ist von Werk auf „192.168.155.1“ eingestellt. Der DHCP-Server des Routers wird dem angeschlossenen PC eine Adresse im Adressraum des DHCP-Servers zur Verfügung stellen.

Die Konfiguration des Routers wird mit Hilfe eines Browsers erstellt.

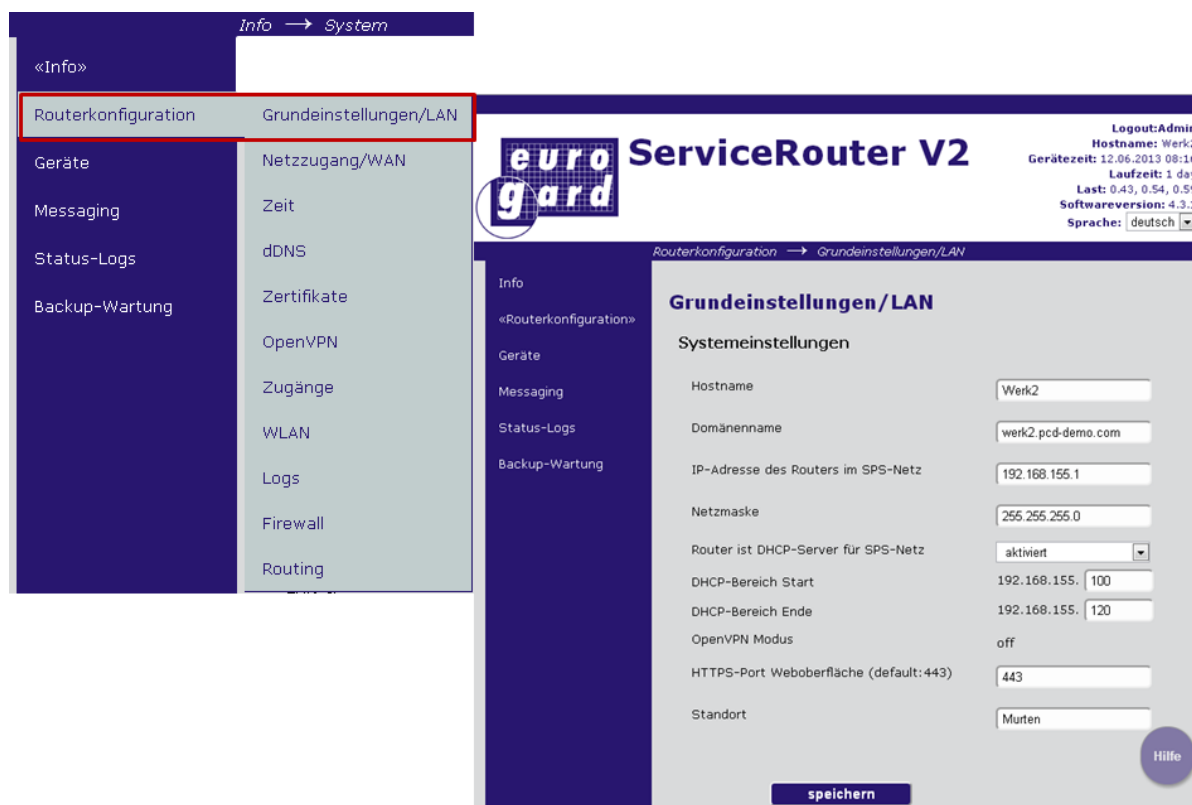
Damit die Konfigurationsoberfläche im Browser geladen wird, muss die IP-Adresse des Routers im Browser aufgerufen werden.

Ab Werk wird der Eurogard Service Router V2 mit dem Benutzer „eurogard“ und dem dazugehörigem Passwort „eurogard“ ausgeliefert. Sie finden die Benutzer und Passwörter auch im Handbuch des Routers.



4.2 Konfigurieren des LAN-Ports (Local Area Network)

Öffnen der Router Konfiguration und setzen der Grundeinstellungen des lokalen Netzwerkes: Verwenden Sie die Adressen im Adressraum Ihrer bestehenden Applikation oder definieren Sie einen neuen Adressraum für eine neue Anlage. Es sollten mindestens der Hostname, Domänenname sowie der Standort geändert werden. Grund hierfür ist, dass diese für das später generierte Server-Zertifikat verwendet werden. Der Domänenname wird im später generierten Zertifikat als Verbindungsname zum VPN-Server eingetragen.



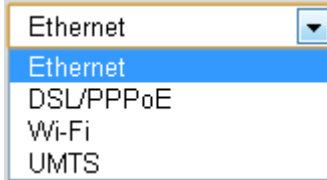
The screenshot displays the web interface of a ServiceRouter V2. On the left, a navigation menu is visible with 'Routerkonfiguration' and 'Grundeinstellungen/LAN' highlighted. The main content area shows the 'Grundeinstellungen / LAN' configuration page. The 'Systemeinstellungen' section includes the following fields:

Parameter	Value
Hostname	Werk2
Domänenname	werk2.pcd-demo.com
IP-Adresse des Routers im SPS-Netz	192.168.155.1
Netzmaske	255.255.255.0
Router ist DHCP-Server für SPS-Netz	aktiviert
DHCP-Bereich Start	192.168.155.100
DHCP-Bereich Ende	192.168.155.120
OpenVPN Modus	off
HTTPS-Port Weboberfläche (default:443)	443
Standort	Murten

At the bottom of the configuration page, there is a 'speichern' (save) button and a 'Hilfe' (help) button. The top right corner of the interface shows system information: 'Logout:Admin', 'Hostname: Werk2', 'Gerätezeit: 12.06.2013 08:16', 'Laufzeit: 1 day', 'Last: 0.43, 0.54, 0.59', 'Softwareversion: 4.3.1', and 'Sprache: deutsch'.

4.3 Konfigurieren des WAN Ports (Wide Area Network)

Der Eurogard Service Router V2 ermöglicht das Konfigurieren von 4 unterschiedlichen WAN Ports:



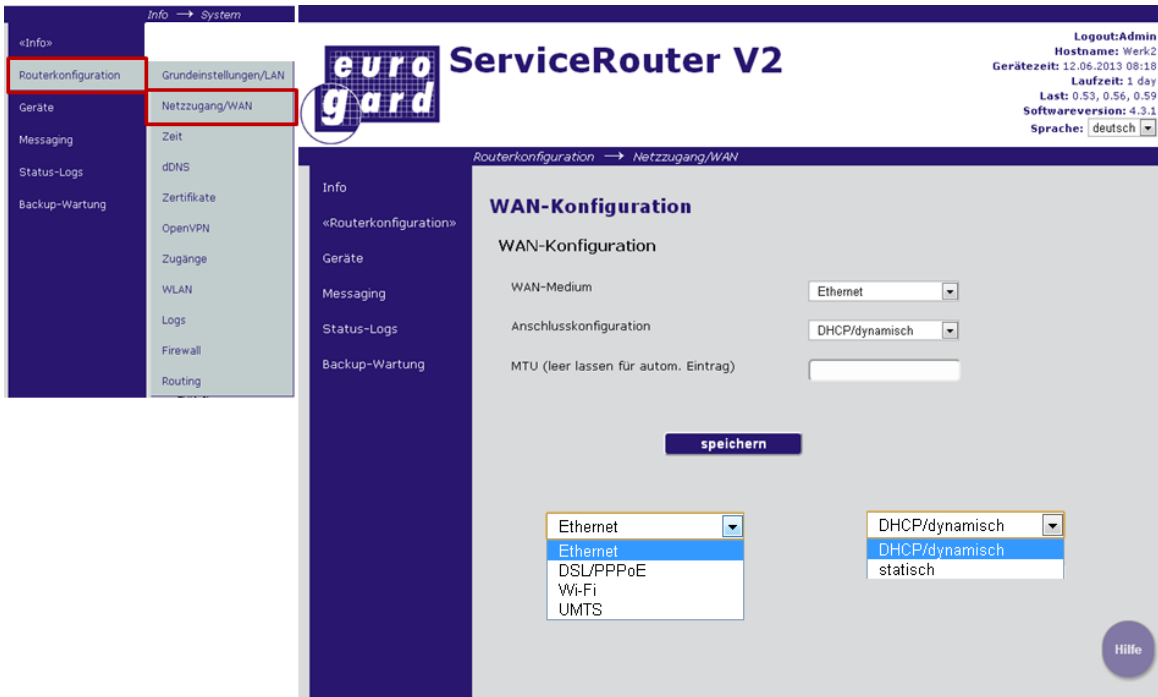
- 1) Ethernet →
diese Konfiguration erlaubt es, den Router hinter einem bestehenden Router zu betreiben. Dabei stellt der bestehende Router die Verbindung zum ISP zur Verfügung.
- 2) DSL/PPPoE → (ein externes ADSL/VDSL Modem wird benötigt)
diese Konfiguration erlaubt es, den Router direkt an ein ADSL/VDSL Modem zu verbinden. Für diese Anschlussart werden die Konfigurationsparameter des ISP benötigt.
- 3) UMTS →
diese Konfiguration erlaubt es, das integrierte UMTS-Modem für den Verbindungsaufbau zu einem ISP zu verwenden. Für diese Anschlussart werden die Konfigurationsparameter des ISP benötigt.
ACHTUNG: In dieser Konfiguration (UMTS) kann der Router nur als VPN-Client betrieben werden.

4.3.1 WAN over Ethernet

Wenn Sie eine bereits bestehende Internetverbindung verwenden.

DHCP: Die IP-Adresse des Gerätes wird vom DHCP-Server der WAN-Schnittstelle bezogen.

Statisch: Die IP-Adresse wird fest definiert.



4.3.2 WAN over UMTS

Wenn der Router mit einem integrierten UMTS Modem ausgestattet ist, kann das UMTS-Modem als WAN-Schnittstelle verwendet werden.

Achtung, eine Verbindung via UMTS unterstützt nur VPN-Client Funktionalitäten. Der Router kann dabei nicht als VPN-Server verwendet werden.

Die für die Einwahl erforderlichen Parameter werden von Ihrem ISP zur Verfügung gestellt.



The screenshot shows the configuration page for the WAN interface on a ServiceRouter V2. The breadcrumb trail is "Routerkonfiguration" → "Netzzugang/WAN". The left sidebar contains navigation options: Info, «Routerkonfiguration», Geräte, Messaging, Status-Logs, and Backup-Wartung. The main content area is titled "WAN-Konfiguration" and contains the following fields:

Parameter	Value
WAN-Medium	UMTS
APN	gprs.swisscom.ch
PIN	
Benutzername	any
Passwort	...
Datenzähler	an
Monatliches Rücksetzen am:	1
Logdatei führen	aktiviert

A "speichern" button is located at the bottom right of the configuration area.

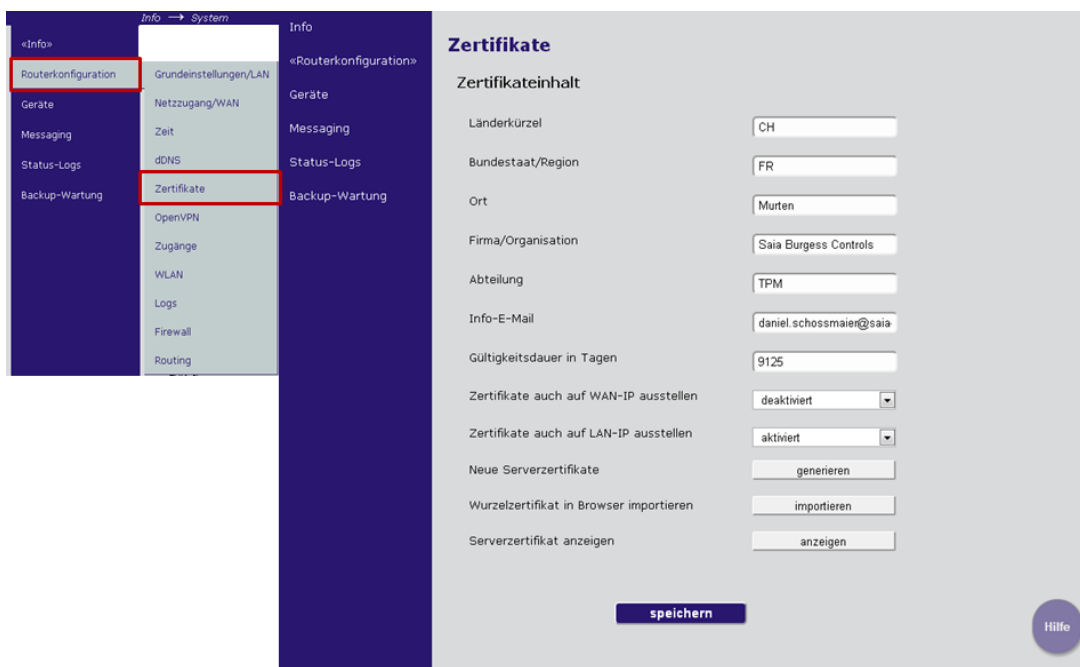
4.4 Zeitkonfiguration

Bevor das Zertifikat generiert wird, ist es notwendig die Uhrzeit des Routers zu prüfen und gegebenenfalls den Zeitserver zu aktivieren oder die Zeit manuell zu setzen.



4.5 Server-Zertifikat erstellen

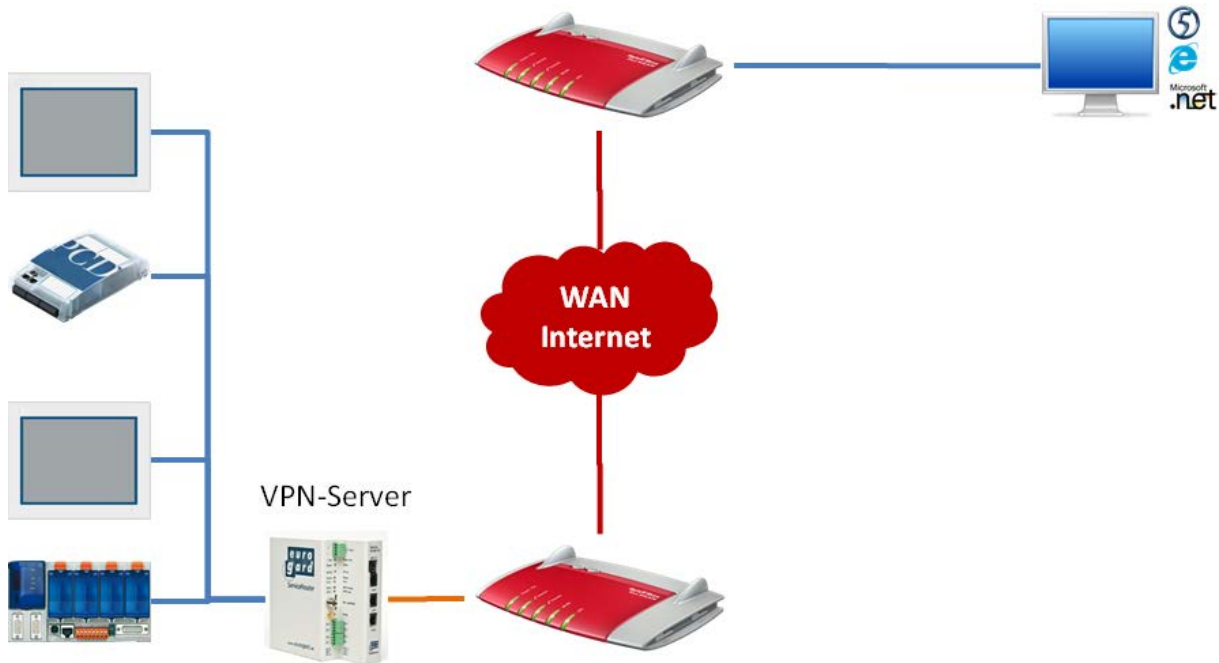
Zum Erstellen des Server-Zertifikates werden die in den oberen Schritten hinterlegten Informationen als auch zusätzliche Parameter verwendet, welche Sie auf der Seite „Zertifikat“ hinzufügen müssen. Daher ist es wichtig, dass vor der Erstellung des Zertifikates die oberen Schritte abgeschlossen sind.



4.6 Aktivieren des openVPN-Servers

4.6.1 VPN-Modus Server

Zum Aktivieren der VPN Funktionalität muss der Server aktiviert werden. Zusätzlich sollten der IP-Adressen-Bereich definiert werden, innerhalb welchem der VPN Client vom DHCP-Server eine IP-Adresse erhält.



Achtung:

Es sollte keine IP-Adresse statisch im Bereich der VPN-Client IP Adressen konfiguriert sein.

The screenshot shows the 'ServiceRouter V2' web interface. The left sidebar has 'Routerkonfiguration' and 'OpenVPN' highlighted. The main area is titled 'OpenVPN' and shows 'Grundeinstellungen OpenVPN'. The configuration includes:

- VPN-Modus: Server
- Erste IP des DHCP-Bereichs für VPN-Teilnehmer: 192.168.155.130
- Letzte IP des DHCP-Bereichs für VPN-Teilnehmer: 192.168.155.140
- VPN-Transportprotokoll: UDP
- Port: 1194
- Client-zu-Clientverbindungen erlauben: ein
- VPN-Paketgröße limitieren auf: 1400 Byte
- Logdatei führen: aus
- Intervall für Keepalive-Pakete in Sekunden: 60
- VPN-Neustart nach wieviel erfolglosen Pings (min. 2): 4
- Kryptoalgorithmus: Kompatibilitätsmodus
- VPN-Netz übersetzen (wird üblicherweise nicht benötigt):

At the bottom right, there is a 'speichern' button and a 'Hilfe' button. The top right corner shows system information: Logout:Admin, Hostname: Werk2, Gerätezeit: 12.06.2013 09:22, Laufzeit: 1 day, Last: 0.40, 0.55, 0.58, Softwareversion: 4.3.1, Sprache: deutsch.

In den meisten Fällen müssen die Default Werte nicht verändert werden.

4.6.2 Zugänge erstellen

Erstellen eines neuen Zuganges. Jeder Client benötigt einen Zugang und das damit verbundene Zertifikat. Der „Bereich“ (siehe Bild unten) stellt dabei die Berechtigung des Zuganges dar. Der Bereich „user“ hat keine Rechte, die Router Konfiguration zu ändern. Er kann sich jedoch als VPN-Client oder über den SSL Proxy Server verbinden. „Admin“ hingegen berechtigt den Zugang zum Bearbeiten der Router Konfiguration.

- ➔ Neuer Zugang (Eingabe von Benutzername, Bereich und Passwort)
- ➔ Neues Zertifikat → Client Zertifikat erstellen.
- ➔ Download des für den Zugang benötigten Zertifikates.

The screenshot shows the 'Zugänge' (Access) configuration page in the Gard VPN interface. The left sidebar has 'Routerkonfiguration' and 'Zugänge' highlighted. The main area shows a table of existing access points and a form to add a new one.

Account-Name	Servicenet	Zertifikat	Online-Status	Aktion
Admin	admin	gültig bis Jun 4 11:17:00 2038 GMT	offline	download Passwort ändern Zugang löschen neues Nutzerzertifikat
Daniel	admin	gültig bis Jun 4 11:18:20 2038 GMT	offline	download Passwort ändern Zugang löschen neues Nutzerzertifikat
Android	user	gültig bis Jun 4 16:12:16 2038 GMT	offline	download Passwort ändern Zugang löschen neues Nutzerzertifikat

Buttons: Status aktualisieren, [neuen Zugang hinzufügen](#)

Form fields: Zugangsname, Bereich, Passwort, Passwort wiederholen, [speichern](#)

Account-Name	Servicenet	Zertifikat	Online-Status	Aktion
Admin	admin	gültig bis Jun 4 11:17:00 2038 GMT	offline	download Passwort ändern Zugang löschen neues Nutzerzertifikat
Daniel	admin	gültig bis Jun 4 11:18:20 2038 GMT	offline	download Passwort ändern Zugang löschen neues Nutzerzertifikat
Android	user	gültig bis Jun 4 16:12:16 2038 GMT	offline	download Passwort ändern Zugang löschen neues Nutzerzertifikat
User	user	nicht vorhanden	offline	download Passwort ändern Zugang löschen neues Nutzerzertifikat

User | user | **gültig bis Jun 6 06:28:09 2038 GMT** | offline | download | Passwort ändern | Zugang löschen | [neues Nutzerzertifikat](#)

[download](#) | Passwort ändern | Zugang löschen | neues Nutzerzertifikat

↓

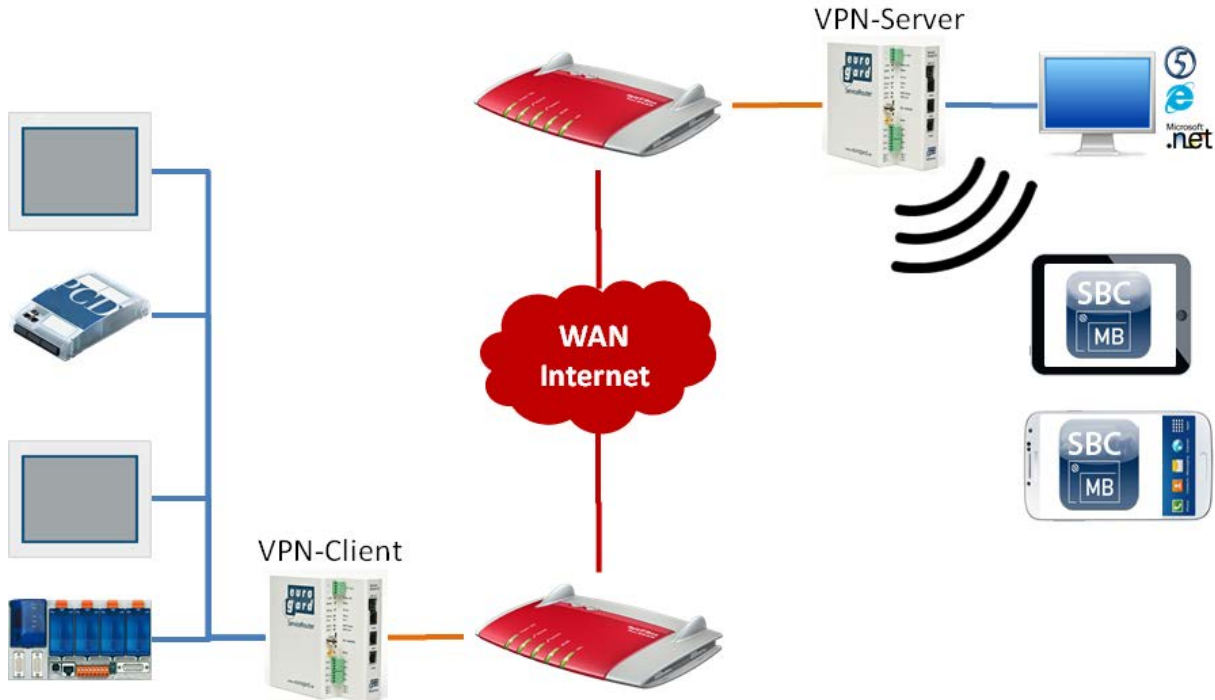
User@Werk2.wei2.p...tar

Achtung:

Beim erstellen eines neuen Server Zertifikates müssen alle Client Zertifikate neu erstellt werden.

5 EuroGard Service Router 2 VPN-Client

Der EuroGard Service Router kann auch als VPN-Client verwendet werden:

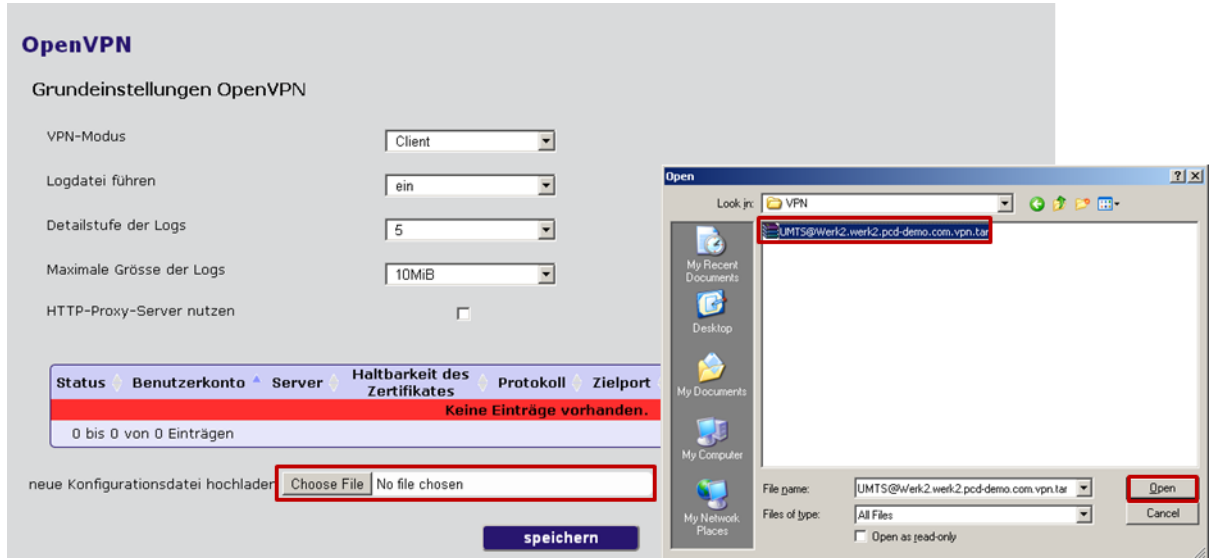


- 1) Als VPN-Server kommt ebenfalls ein EuroGard Router zum Einsatz. Konfigurieren des OpenVPN-Zugangs als Client:



- 2) Laden des vom Server erstellen Zertifikates beim Erstellen der Zugänge. Dieses Zertifikat enthält alle Schlüssel und Informationen zum Aufbau der Verbindung zum VPN Server

Server.



- 3) Der VPN-Server wird in der Tabelle eingetragen. Aktivieren des Zuganges in der Liste.

Status	Benutzerkonto	Server	Haltbarkeit des Zertifikates	Protokoll	Zielport	Paketgrößenlimit	Kryptoalgorithmus	Aktion
aktiviert	UMTS	werk2.pcd-demo.com	Jun 6 09:44:45 2038 GMT	udp	1194	1400	Kompatibilitätsmodus für v1-Router	<input type="checkbox"/> Zugang löschen <input checked="" type="checkbox"/> Zugang benutzen

- 4) Wenn der VPN Tunnel erfolgreich hergestellt wurde, ist der aktuelle Zustand unter Status-Logs → Netzwerke ersichtlich (CONNECTED)

Status-Logs → Netzwerke

- Info
- Routerkonfiguration
- Geräte
- Messaging
- «Status-Logs»
- Backup-Wartung

Netzwerk

IP-Adressen

WAN-IP:

- Netzwerk
- Logs
- Firewall
- dDNS
- Diagnose
- Routing

VPN-Status

Parameter

VPN-Modus: client

Port: 1194

Server: werk2.pcd-demo.com

Protokoll: udp

Paketgrößenlimit: 1400

Kryptoalgorithmus: Kompatibilitätsmodus für v1-Router

übertragene Daten:

durch VPN-Tunnel empfangen: 898 Byte

durch VPN-Tunnel gesendet: 660 Byte

Rohdaten empfangen: 7 KiByte

Rohdaten gesendet: 6 KiByte

Letzte 3 Statusmeldungen:

Thu Jun 13 07:50:09 2013 GET_CONFIG

Thu Jun 13 07:50:11 2013 ASSIGN_IP

Thu Jun 13 07:50:11 2013 CONNECTED

Verbunden mit: 92.104.90.64

Zugewiesene VPN-IP: 192.168.155.131

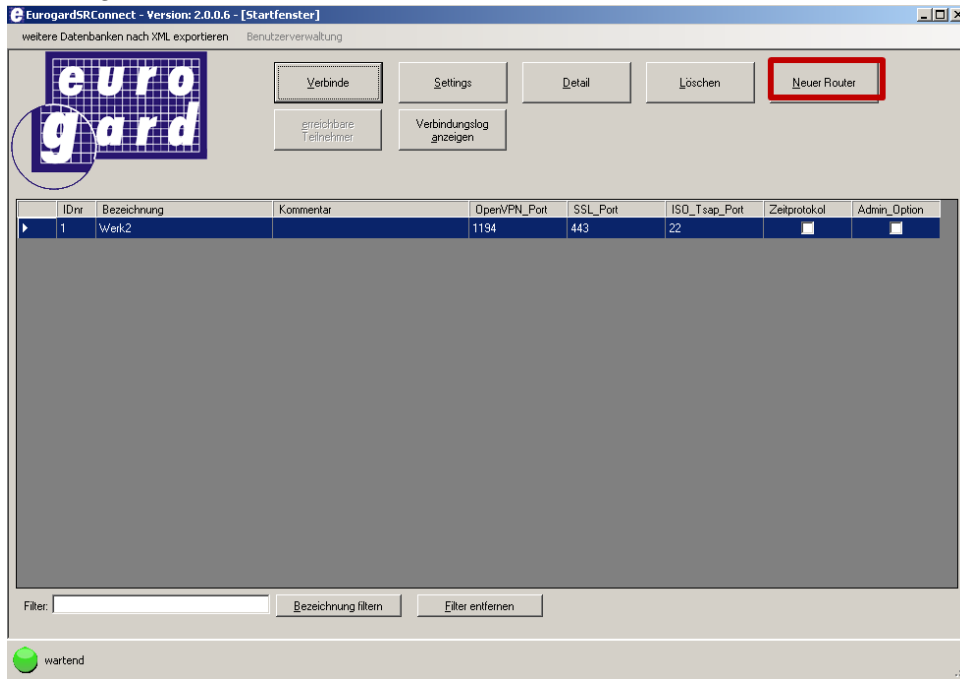
5.1 Client Software EurogardSRConnect

Die Client Software wird benötigt, um eine openVPN Verbindung mit dem Server des Eurogard Routers aufzubauen. Für die Installation des openVPN Client benötigen Sie Administrationsrechte.

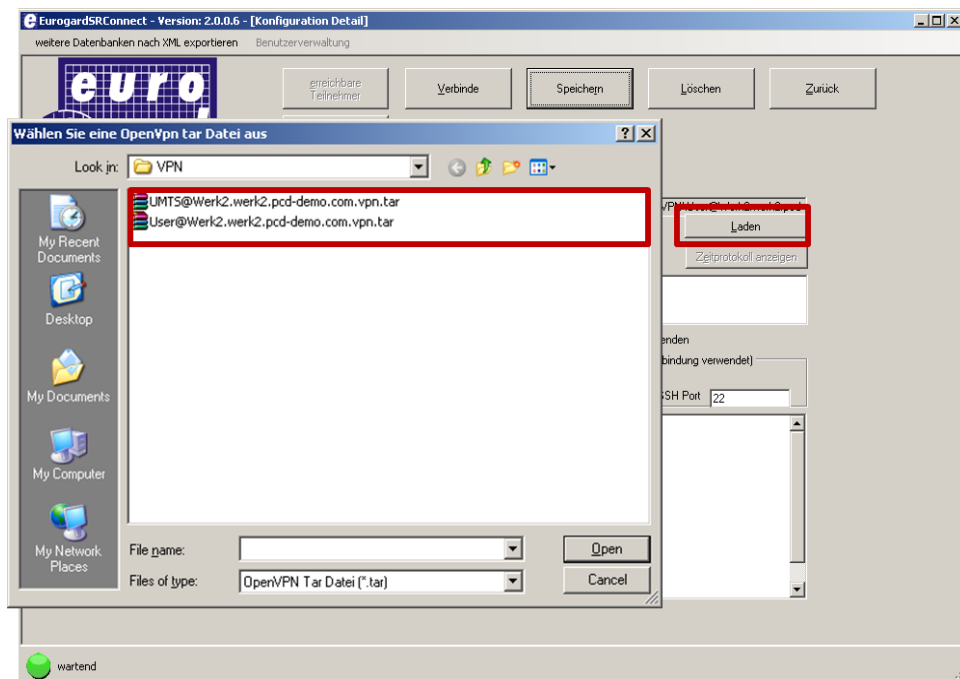
Die Software EuroGardSRConnect ist auf der Homepage von EuroGard erhältlich <http://www.eurogard.de>

Software Tool EuroGardSRConnect

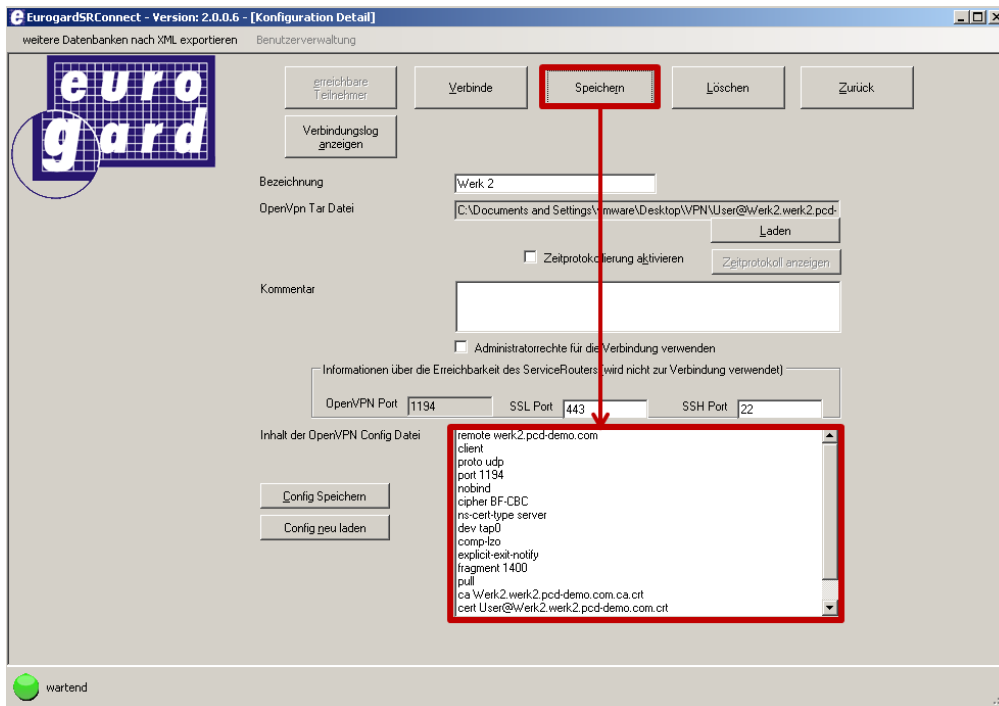
14) Hinzufügen eines neuen Routers:



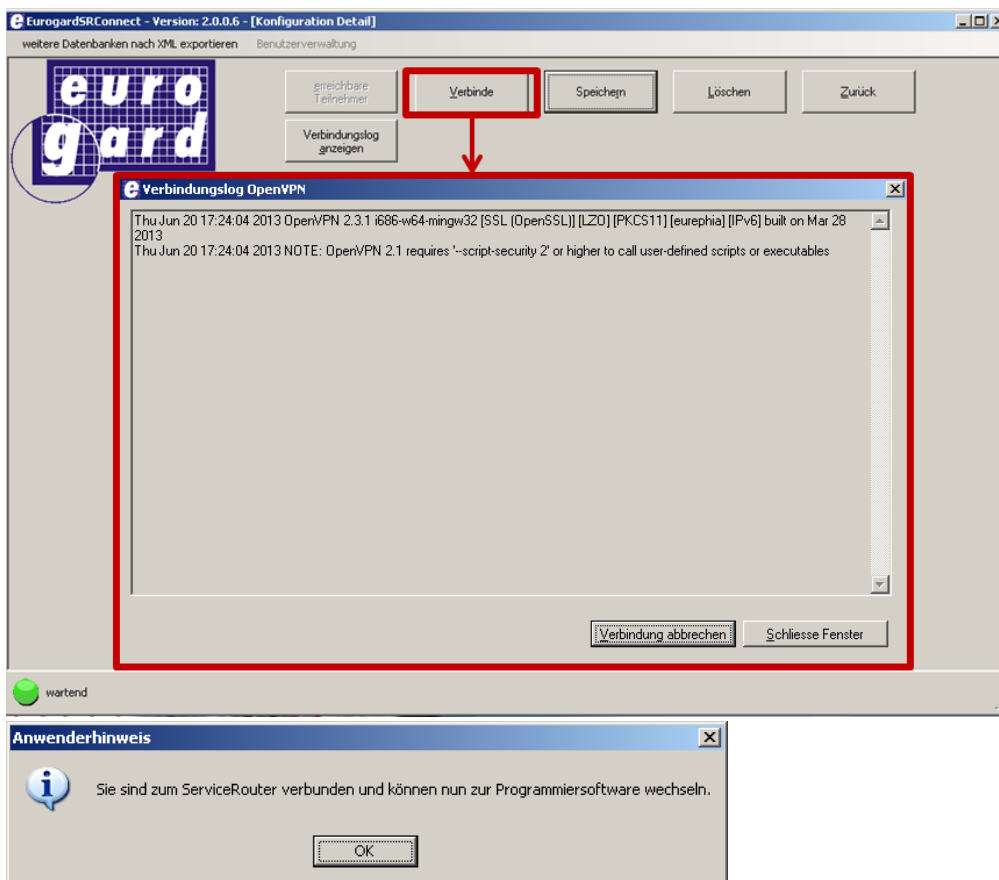
15) Laden Sie das vom Router generierte Benutzer-Zertifikat in die Applikation. Alle Schlüssel und Informationen sind in diesem Zertifikat enthalten.



16) Speichern Sie das geladene Benutzer-Zertifikat ab. Nach dem Speichern sehen Sie die Verbindungsparameter im unteren Fenster. Im Normalfall müssen diese Parameter nicht bearbeitet werden.



17) Verbinden Sie sich mit dem VPN-Server



18) Der PC ist nun ein Teilnehmer des gegenüberliegenden Netzwerkes. Der Zugriff auf die Geräte ist mit allen Applikationen die Ethernet unterstützen möglich.

- Browser
- PG 5

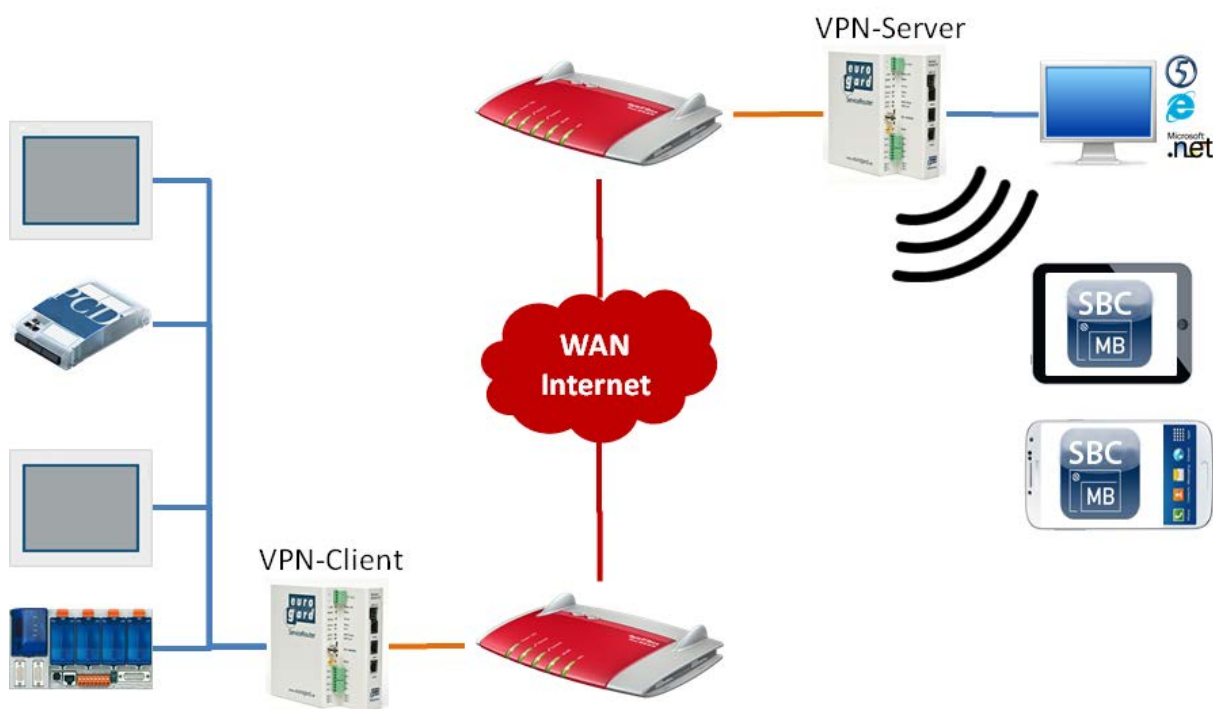


5.2 IOS und Android Systeme

Werden 2 Router im Client / Server Betrieb verwendet, so ist es möglich I-OS Systeme sowie Android Systeme kabellos am Netzwerk des EuroGard Service Router 2 anzumelden.

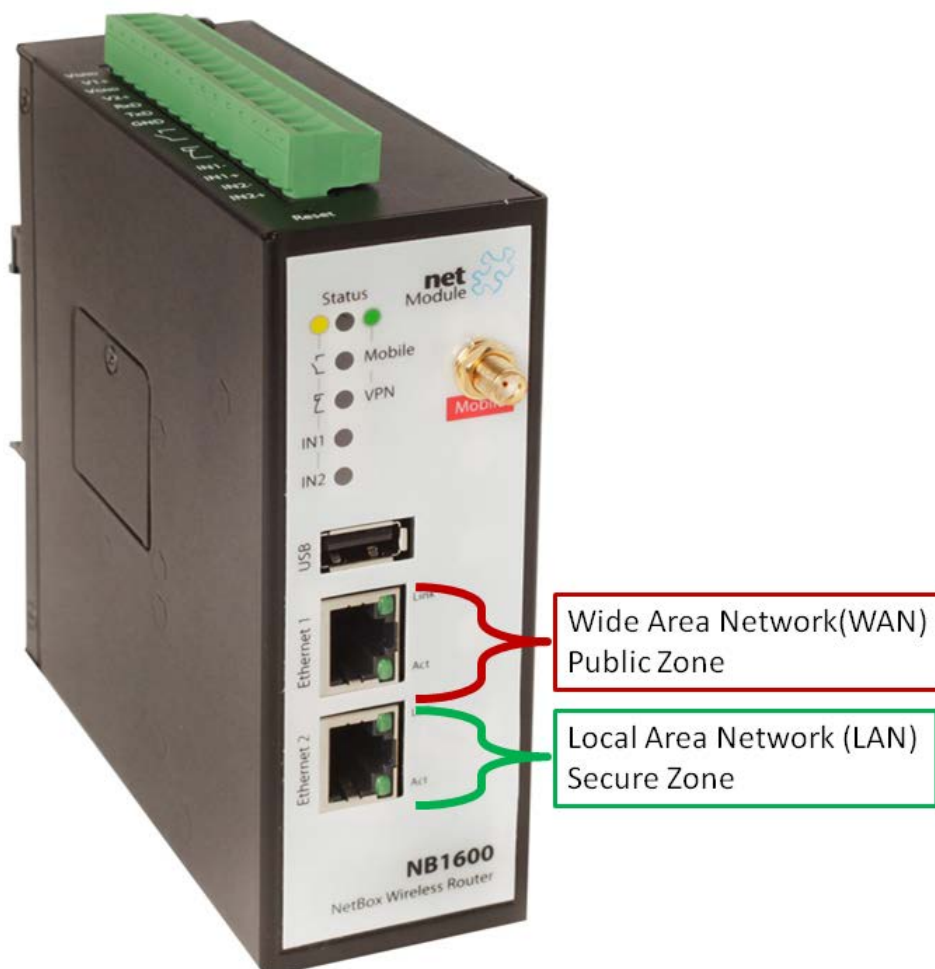
Dafür muss der Router, an welchem die Systeme verbunden werden sollen, mit einer W-LAN Option ausgestattet sein.

Der Euro Gard Client Router kann entweder über Kabel oder auch über UMTS mit dem Server verbunden werden.



6 Net Module VPN Router NB 1600 und 1600-U

Konfigurieren des NB 1600 oder NB 1600-U als openVPN-Server im Modus TUN.



Wide Area Network (WAN) → Verbindung zum Router mit öffentlichen IP-Adresse
Local Area Network (LAN) → Verbindung zum lokalen Netzwerk

6.1 Technische Daten

	Net Module NB 1600	Net Module NB 1600-U
Bestelldaten	NB 1600	NB 1600-U
Weitere Informationen	http://www.netmodule.de/products/industrial-routers/wireline-router.html	http://www.netmodule.de/products/industrial-routers/mobile-router.html
Einsatz/Bauform	Industriell	Industriell
Hutschienenmontage	Hutschienenmontage	Hutschienenmontage
Spannungsversorgung	24 V DC (-15% +20%)	24 V DC (-15% +20%)
VPN Eigenschaften		
Anzahl WAN Interfaces	1; LAN	2; LAN, UMTS
Integriertes ADSL/VDSL Modem	Nein	Nein
VPN PPTP	Ja	Ja
VPN L2TP/IPSec	Nein	Nein
openVPN	Ja	Ja
Anz. VPN Clients	10	10
Windows Client	Ja openVPN	Ja openVPN
IOS Client	Ja openVPN	Ja openVPN
Android Client	Ja openVPN	Ja openVPN
Erweiterungen		
3G / 4G Modem	Nein	3G (UMTS 7.2 Mbps)

6.2 Öffnen des Setup Menü

Zum Einrichten des Net Module Routers muss der PC mit einer LAN-Schnittstelle des Routers verbunden werden. Der Router wird mit einem aktivierten DHCP-Server ausgeliefert. Es sollte deshalb vermieden werden, den Net Module Router mit Werkskonfiguration in eine Ethernet-Infrastruktur mit bereits vorhandenem DHCP-Server zu konfigurieren.

Empfohlen:

Trennen Sie ihren PC von allen bestehenden Netzwerkverbindungen.

Verbinden Sie ihren PC direkt mit dem Router.

Die Standard IP-Adresse des Routers ist von Werk auf „192.168.1.1“ eingestellt. Der DHCP-Server des Routers wird dem angeschlossenen PC eine Adresse im Adressraum des DHCP-Servers zur Verfügung stellen.

Die Konfiguration des Routers wird mit Hilfe eines Browsers erstellt.

Damit die Konfigurationsoberfläche im Browser geladen wird, muss die IP-Adresse des Routers im Browser aufgerufen werden.

Der Router startet bei der ersten Verbindung einen Konfigurationsassistenten bei welchem die Passwörter und Benutzer Namen gesetzt werden.

net
Module

NB1600 WEB MANAGER

NB1600 Login

Please provide username and password to log in:

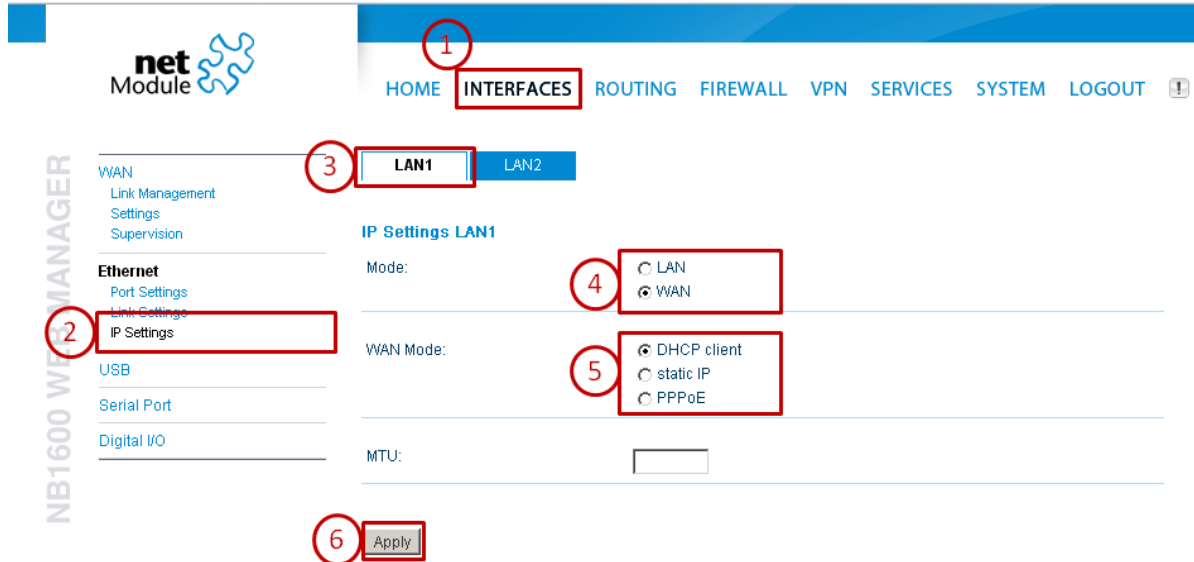
Username:

Password:

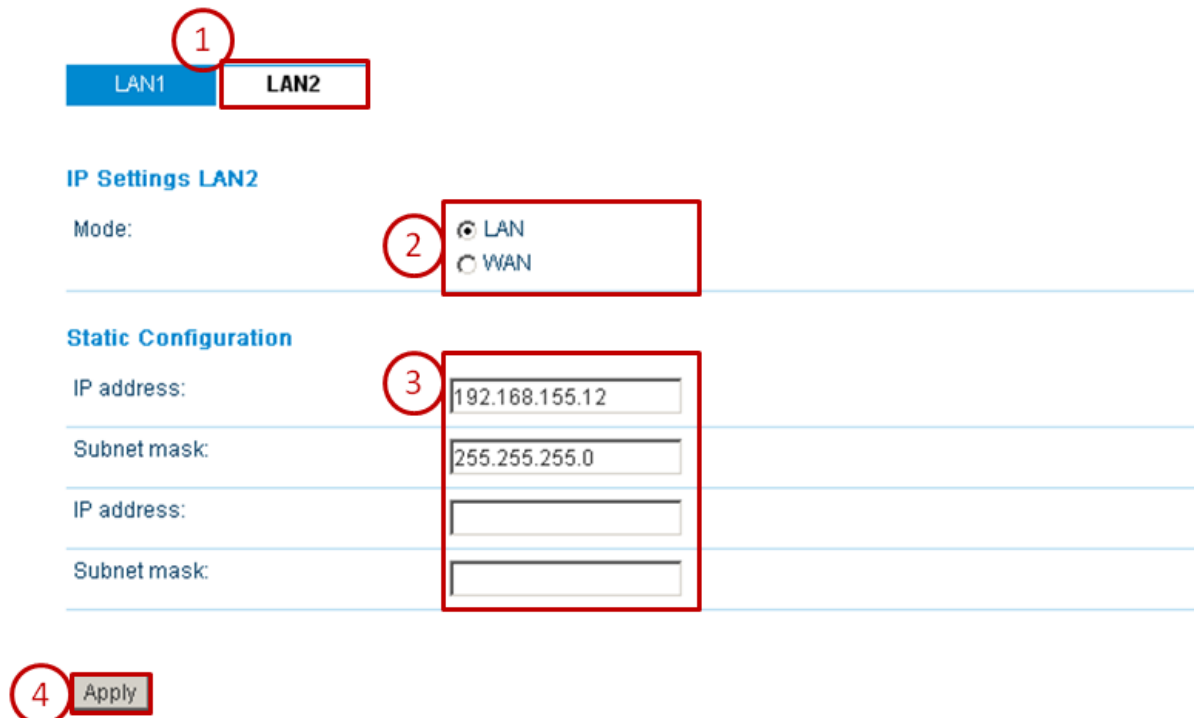
Login

6.3 Konfigurieren der WAN und LAN Ports (Wide Area Network)

Konfigurieren der LAN 1 Schnittstelle als WAN Interface. Die IP-Adresse des WAN Interfaces wird vom vorher positionierten Router bereitgestellt oder kann statisch vergeben werden im Bereich ausserhalb des vorhergehenden DHCP-Servers.



Die LAN 2 Schnittstelle wird für das Automationsnetzwerk verwendet und sollte eine IP-Adresse in dessen Bereich erhalten. Im folgenden Beispiel befindet sich das Automationsnetzwerk im IP-Adressen Bereich 192.168.155.0/24



Wenn DHCP-Client für die WAN Schnittstelle aktiviert wurde kann die vom DHCP-Server erhaltene IP-Adresse im Bereich HOME überprüft werden

Summary **LAN1**

Connection Details LAN1

Description	Value
Administrative state	enabled
Operational state	up
Link is up since	2013-09-30 07:09:30
IP address	192.168.0.19
Gateway	192.168.0.1
Transfer rate down / up	7.37 KByte/s / 1.79 KByte/s
Data downloaded / uploaded since 2013-04-12 04:53:33	878.13 MB / 6.17 MB <input type="button" value="Reset"/>

6.4 Zeitkonfiguration

Die Zeitkonfiguration des Routers muss vor dem Erstellen von Zertifikaten geprüft werden. Setzen Sie gegebenenfalls die Zeit manuell oder aktivieren Sie die Time Synchronisation.

→ Eine Internet Verbindung ist für die Time Synchronisation erforderlich.

The screenshot shows the Net Module web interface. The navigation menu at the top includes HOME, INTERFACES, ROUTING, FIREWALL, VPN, SERVICES, **SYSTEM**, and LOGOUT. The sidebar on the left lists various system settings, with **Time & Region** selected. The main content area is titled 'System Time' and contains the following configuration options:

- System Time:** Current system time: 2013-09-30 08:16:27 (with a 'Set time' button).
- Time Synchronisation:** NTP server: 0.pool.ntp.org; NTP server 2 (optional): 1.pool.ntp.org.
- Time zone:** Time zone: UTC+01:00 Amsterdam, Berlin, Bern, Rome, Stockholm (dropdown menu); Daylight saving changes: .

Buttons for 'Apply' and 'Sync' are located at the bottom of the configuration area.

6.5 Erstellen der Server Zertifikate

Die Server Zertifikate werden benötigt um einen openVPN Benutzer zu erstellen. Die im Router hinterlegten Informationen wie Hostname, e-Mail Adressen und mehr werden für das Zertifikat verwendet.

The screenshot shows the NetModule web manager interface. The top navigation bar includes 'HOME', 'INTERFACES', 'ROUTING', 'FIREWALL', 'VPN', 'SERVICES', 'SYSTEM', and 'LOGOUT'. The 'SYSTEM' menu item is circled with a red '1'. On the left sidebar, the 'Keys & Certificates' menu item is circled with a red '2'. The main content area shows the 'Root CA' configuration page. The 'Root CA certificate' and 'Root CA key' fields are both marked as 'missing' and circled with a red '2'. Below these fields is a 'Processing...' status message and a 'Processing...' button, which is circled with a red '3'. The 'Processing...' message states: 'The device is processing a key/certificate request, please stand by.' Below this, the steps are listed: 'Step 1: Initializing certificate database', 'Step 2: Generating random bits', and 'Step 3: Generating Diffie-Hellmann parameter file'. At the bottom of the configuration area, there are 'View' links for 'Root CA certificate' and 'Root CA key'.

Nach dem Erstellen des Server-Zertifikates muss ein Zertifikat für den openVPN-Tunnel erstellt werden.

The screenshot shows the NetModule web manager interface. The top navigation bar includes 'HOME', 'INTERFACES', 'ROUTING', 'FIREWALL', 'VPN', 'SERVICES', 'SYSTEM', and 'LOGOUT'. The 'SYSTEM' menu item is circled with a red '1'. On the left sidebar, the 'Keys & Certificates' menu item is circled with a red '2'. The main content area shows the 'OpenVPN1' configuration page. The 'OpenVPN1' menu item is circled with a red '3'. The 'Server certificate', 'Private key', and 'CA root certificate' fields are all marked as 'missing' and circled with a red '2'. Below these fields is a 'Processing...' status message and a 'Create' button, which is circled with a red '4'. The 'Processing...' message states: 'The device is processing a key/certificate request, please stand by.' Below this, the steps are listed: 'Step 1: Generating key for openvpn-tunnel0', 'Step 2: Creating certification request for /CN=NB1600/emailAddress=router@support.netmodule.com/O=NetModule/OU=NetModule/C=CHIST=Switzerland/0', 'Step 3: Signing certificate for openvpn-tunnel0 with config from /tmp/openvpn-tunnel0-ca.conf', 'Step 4: Copying CA root certificate/key', and 'Step 5: Verifying openvpn-tunnel0 certificate against root CA'. At the bottom of the configuration area, there are 'View' links for 'Server certificate', 'Private key', and 'CA root certificate'.

6.6 Aktivieren des openVPN Servers

Aktivieren des open VPN Servers

Damit sich ein Client anmelden kann muss der Tunnel Konfiguriert werden. Der Net Module Router ermöglicht das Konfigurieren von einem VPN-Server Tunnel oder 4 Client Tunnels.

Aktivieren Sie den Tunnel als Server.

Wenn mobile Geräte mit Android oder I-OS System sich am openVPN Server anmelden müssen, muss der TUN Modus mit Routing aktiviert werden.

6.7 Anlegen eines Client Zuganges

Aktivieren eines Clients in dem die Checkbox markiert wird es empfiehlt sich dem Client einen Namen zu vergeben.

net Module

HOME INTERFACES ROUTING FIREWALL **VPN** SERVICES SYSTEM LOGOUT

OpenVPN
Administration
Tunnel Configuration
Client Management

IPsec
Administration
Tunnel Configuration

PPTP
Administration
Tunnel Configuration

Client Management

Enabled	Client	Connection info
<input checked="" type="checkbox"/>	Daniel	
<input type="checkbox"/>	Client2	
<input type="checkbox"/>	Client3	
<input type="checkbox"/>	Client4	
<input type="checkbox"/>	Client5	
<input type="checkbox"/>	Client6	
<input type="checkbox"/>	Client7	
<input type="checkbox"/>	Client8	
<input type="checkbox"/>	Client9	
<input type="checkbox"/>	Client10	

Apply Refresh

Die Tunnel Adresse als auch die Client Netzwerk Adresse müssen bei der aktuellen Tunnelkonfiguration nicht verändert werden.

net Module

HOME INTERFACES ROUTING FIREWALL **VPN** SERVICES SYSTEM LOGOUT

OpenVPN
Administration
Tunnel Configuration
Client Management

IPsec
Administration
Tunnel Configuration

PPTP
Administration
Tunnel Configuration

Client Management

Client Networking

This menu can be used to configure a fixed tunnel endpoint address for each client. You may also specify a network, whose packets should get routed towards the client.

Select client: Daniel

Tunnel address: dynamic fixed

Client network: none specify

Apply

Damit die Netze hinter dem VPN-Tunnel bekannt gemacht werden müssen die Routen gesetzt werden. Hier muss die Netzadresse des Automationsnetzes eingetragen werden.

Die Konfigurationsfiles für den Client können vom Router geladen werden. Achten Sie darauf das die Serveradresse korrekt geschrieben und erreichbar ist

7 Windows openVPN Client für Net Module Router

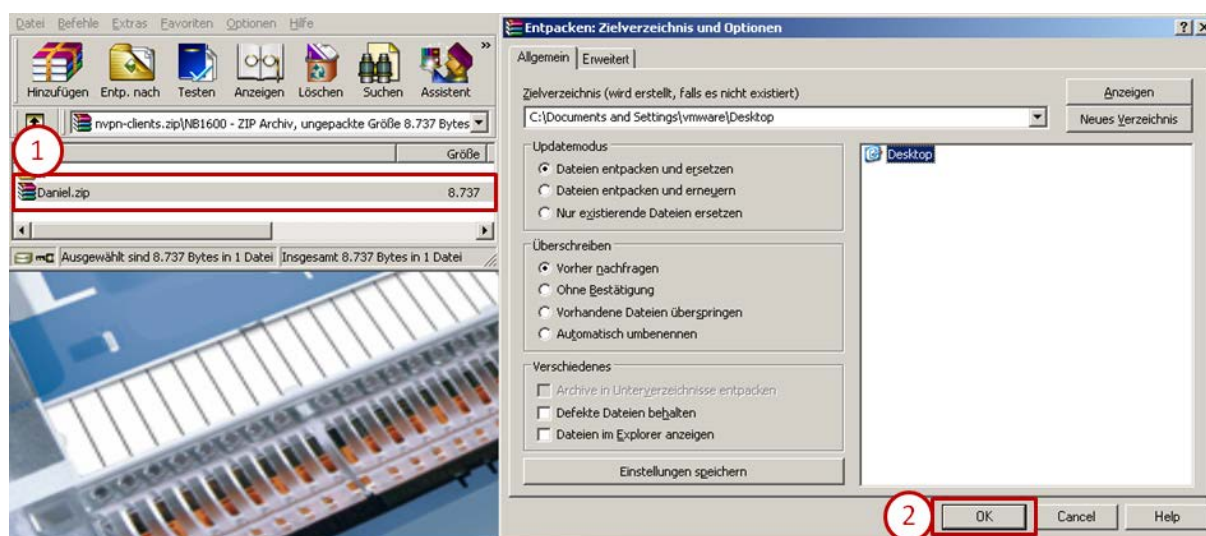
7.1 Installation

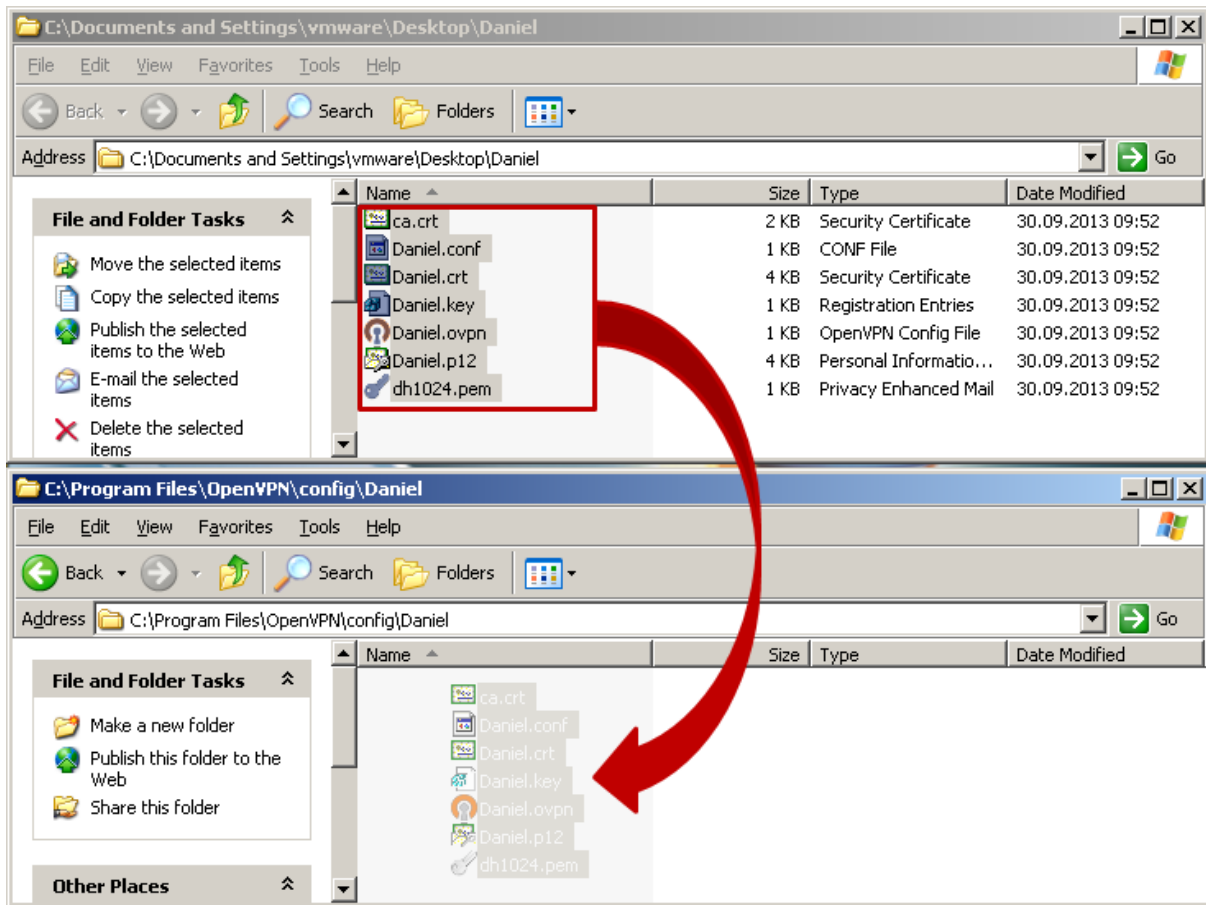
Installieren Sie die Applikation openVPN 2.2.2

(<http://www.netmodule.com/download/openvpn-client/windows>) Für die Installation benötigen Sie Administrationsrechte.

7.2 Entpacken des Konfigurationpakets

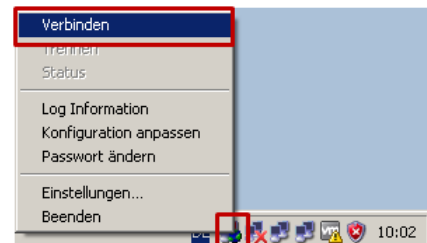
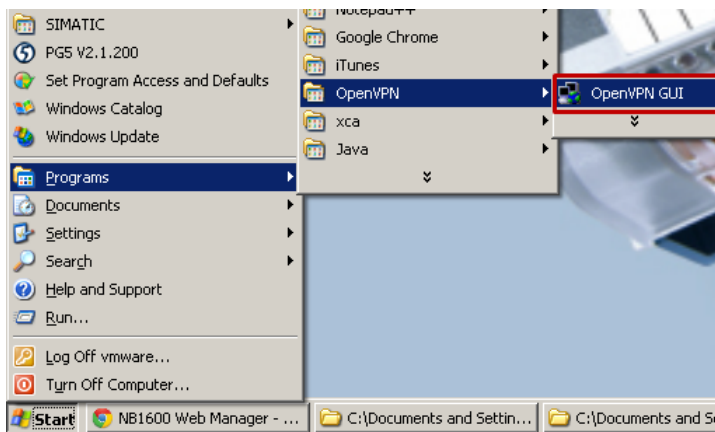
Entpacken Sie das vom Router geladene Konfigurationspaket. Kopieren Sie den Inhalt in den Ordner „config“ welchen Sie im Installationsverzeichnis des openVPN Clients finden „C:\Program Files\OpenVPN\config“.

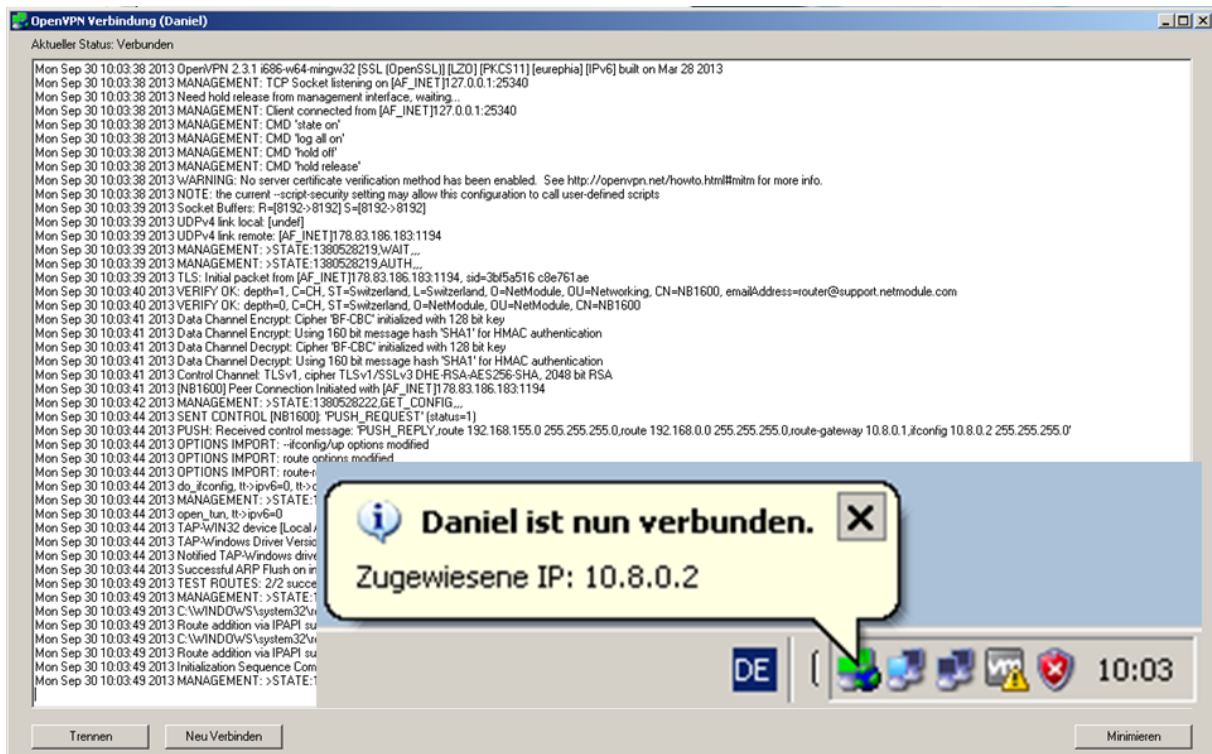




7.3 Herstellen einer Verbindung

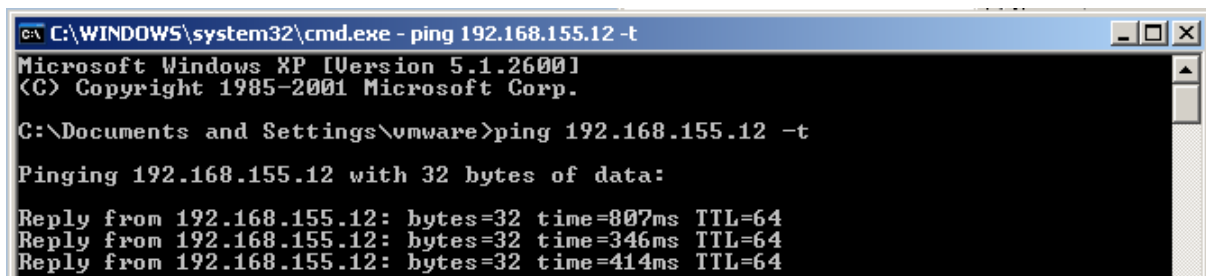
Starten des openVPN Client. Dieser wird mit einem kleinen Symbol in der Statusleiste des Betriebssystems angezeigt und bauen Sie einer Verbindung zum openVPN-Server auf.





Die im VPN-Server hinterlegten Routen werden aktiviert.

Achtung hierfür muss der eingeloggte Windows Benutzer rechte zum Erstellen von Routingtabellen besitzen.



8 Android openVPN Client für Net Module Router

Laden Sie die App OpenVPN Connect oder OpenVPN für Android über den Android Play Store herunter.

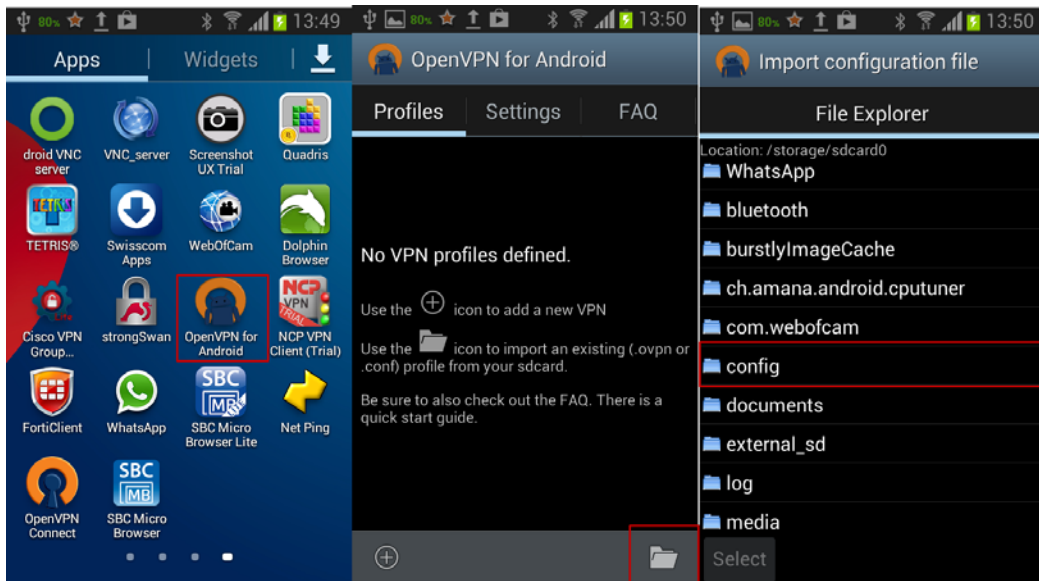
Verbinden Sie das Gerät mit ihrem PC, auf welchem sich die vom Router geladenen Konfigurationsdateien befinden.

Achtung: Der openVPN Server muss für Android Client Systeme im TUN Modus konfiguriert sein.

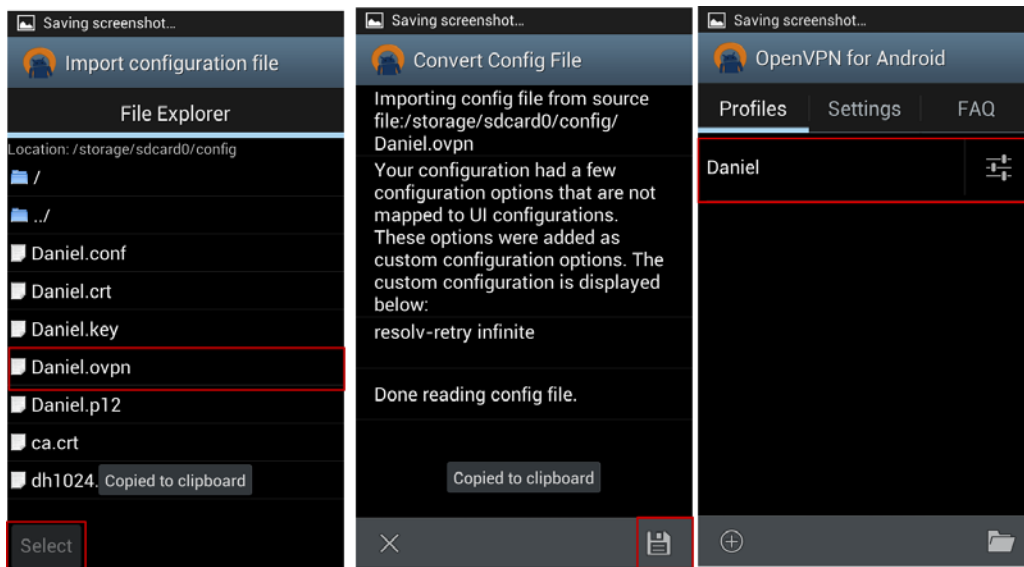
Kopieren Sie die Konfigurationsdateien auf das Gerät in das Verzeichnis „config“

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

Starten Sie die App OpenVPN für Android und öffnen Sie die vom PC geladene openVPN Konfigurationsdatei.



Das Profil ist nun in openVPN Client für Android importiert und verfügbar.

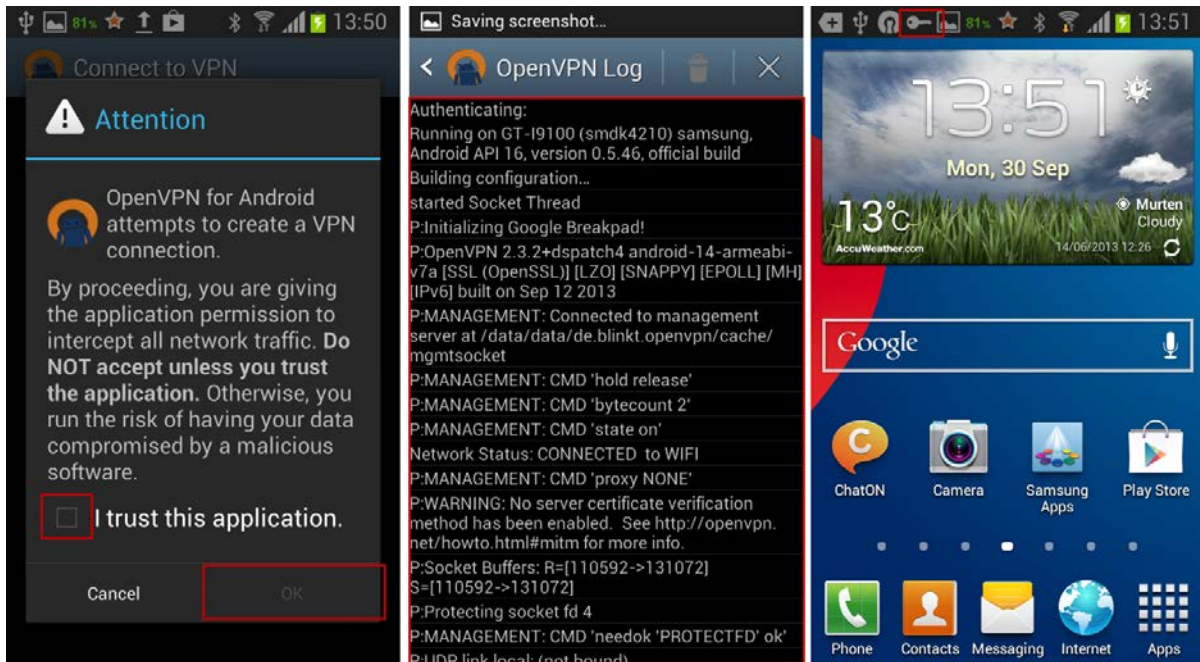


8.1 Herstellen einer Verbindung

Verbinden Sie sich mit dem openVPN Server.

Das Betriebssystem Android wird Sie bezüglich der Netzwerkkonfiguration fragen ob Sie dieser Applikation vertrauen. Damit eine Verbindung hergestellt werden kann, müssen Sie den Dialog bestätigen.

Wenn die Verbindung erfolgreich hergestellt wurde wird das Schlüssel Icon in der Statusleiste von Android angezeigt.



9 I-OS openVPN Client für Net Module Router

Installieren Sie die App openVPN aus dem Apple App Store

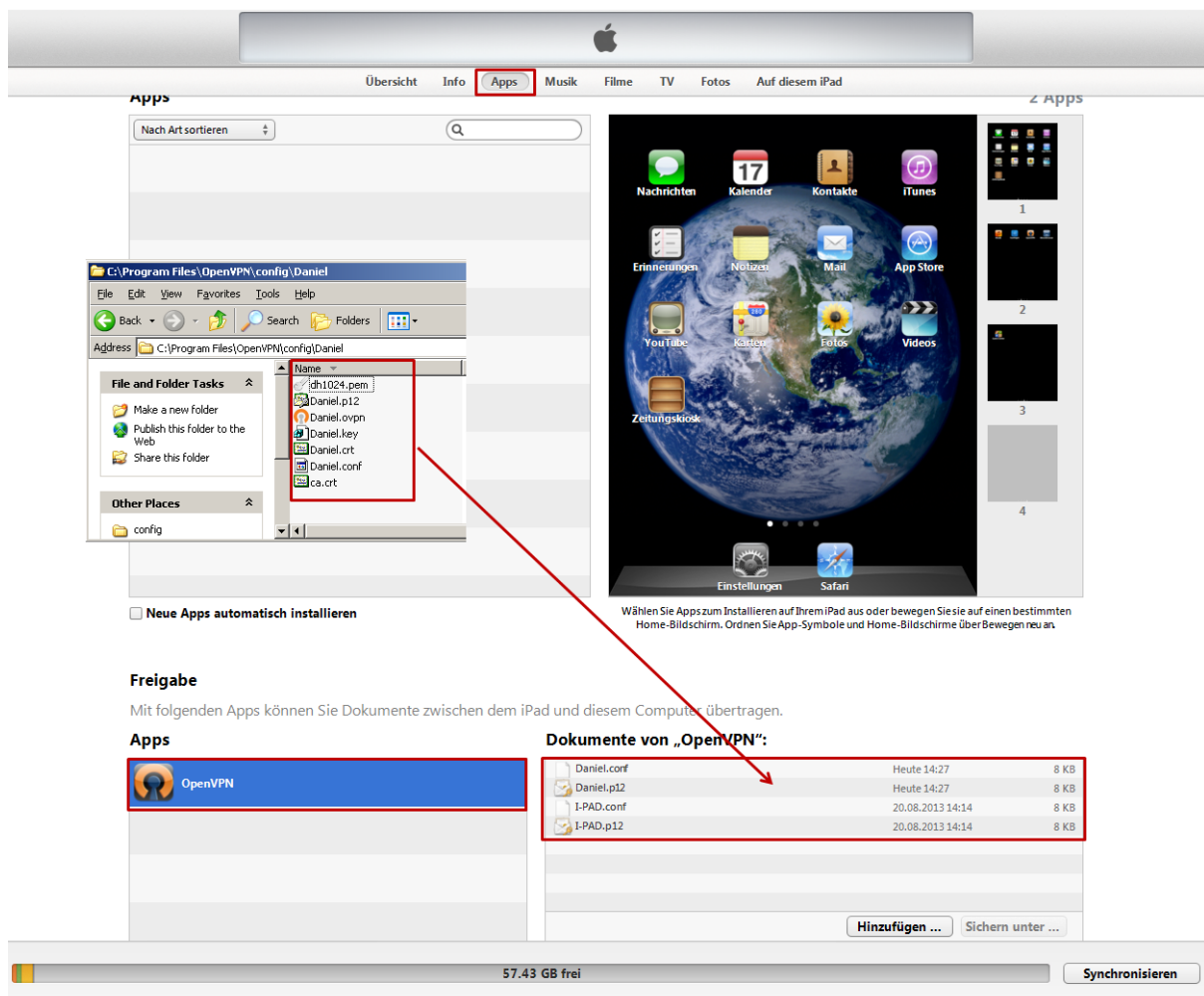
Installieren Sie die Applikation I-Tunes auf ihrem PC und Verbinden Sie das I-Pad mit ihrem PC.

Achtung: Der openVPN Server muss für I-OS Client Systeme im TUN Modus konfiguriert sein.

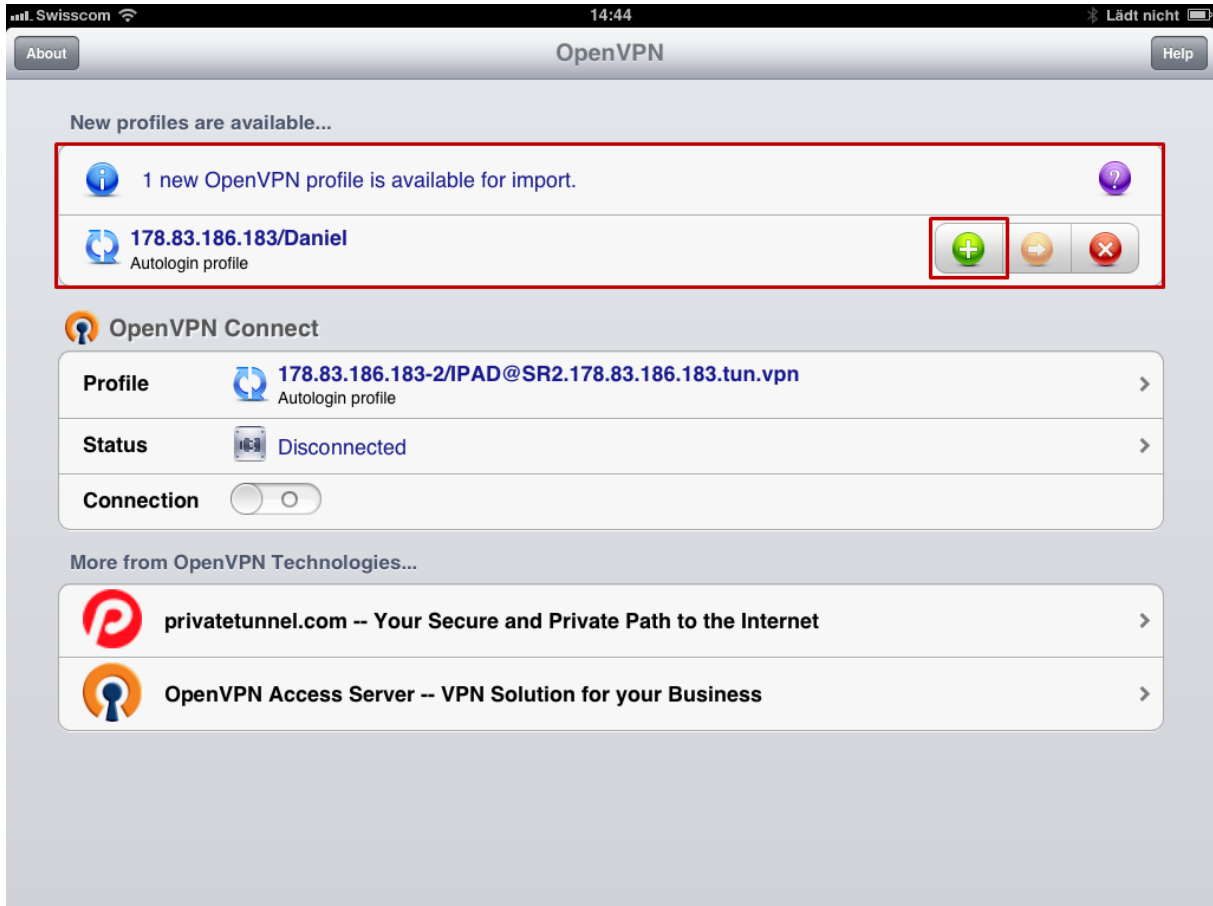
Öffnen Sie das iPad oder I-OS Gerät in I-Tunes



Laden Sie die vom Router entpackten Dateien für die openVPN Tunnel Konfiguration über den Reiter Apps → OpenVPN in die Applikation.



Öffnen Sie die App OpenVPN. Die geladene openVPN Server Konfiguration wird selbstständig erkannt und kann durch den Add Button bestätigt werden.



9.1 Herstellen einer Verbindung

Verbinden Sie sich mit dem openVPN Server indem Sie den Schieberegler bewegen



Wenn Sie den Status Connected erhalten wurde der VPN-Tunnel erfolgreich aufgebaut.

