

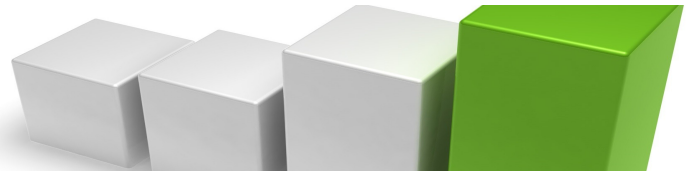
## IPSec-Verbindung CR230U-Vigor2910

### **1. Allgemeines**

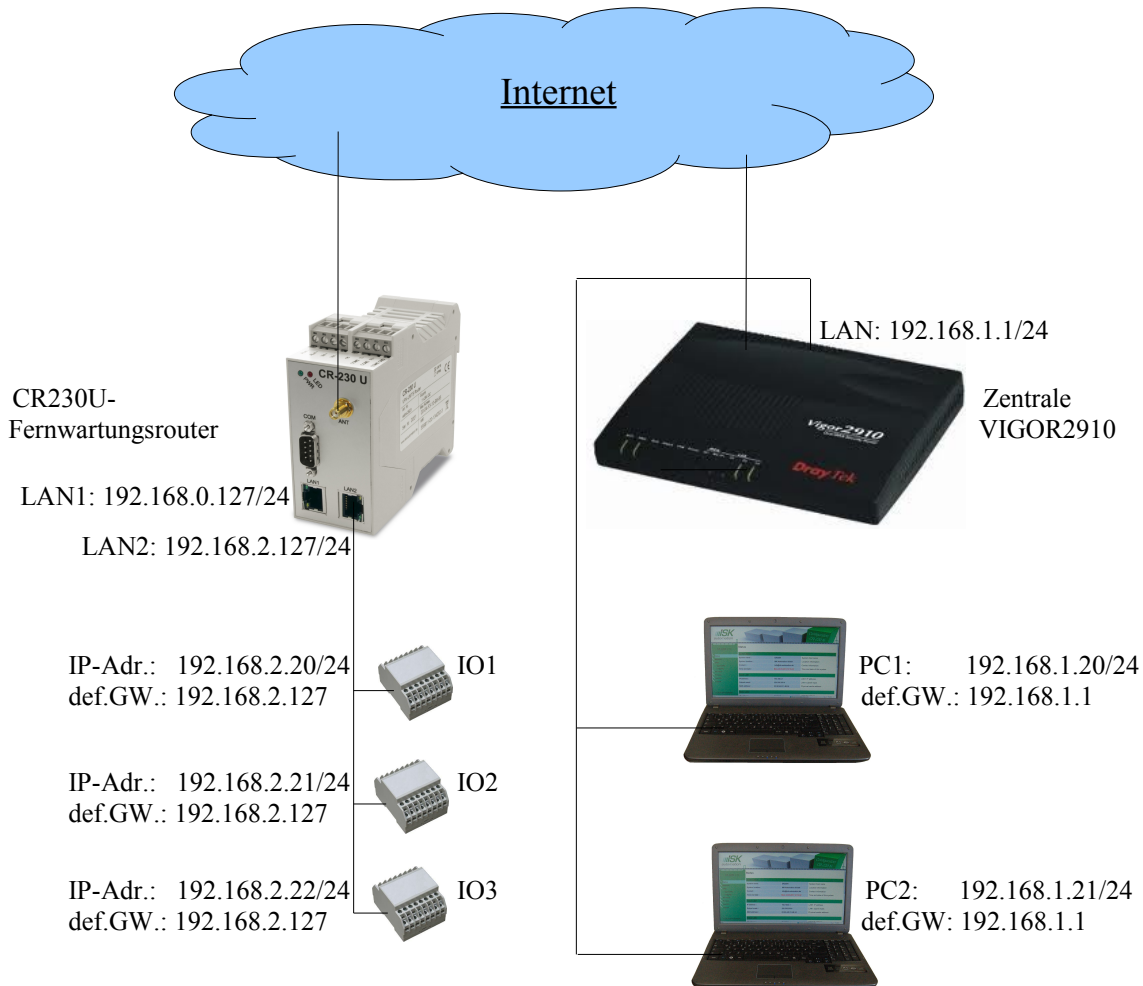
Der Vigor2910 wird oftmals als Router an zentralen Standorten eingesetzt, da er bis zu 32 IPSec-Tunnel bedient und durch sein Dual-WAN-Interface einen redundanten Internetzugang ermöglicht. Je nach Bedarf, kann man im Vigor2910 mehrere IPSec-Server konfigurieren und somit sichere Datenverbindungen zu IPSec-Clients herstellen, die sich an beliebigen Standorten befinden und über das Internet mit der Zentrale kommunizieren. Der CR230U ist als Client für eine solche Kommunikation geeignet. In diesem Anwendungsbeispiel wird die Konfiguration des CR230U und des Vigor2910 beschrieben.

### **2. Aufgabenstellung**

Der VPN-Router CR230U soll über sein eingebautes UMTS-Modem eine Verbindung zum Internet herstellen. Für diesen Internetzugang ist eine private IP ausreichend. Der Zentralrouter Vigor2910 baut über ein externes DSL-Modem ebenfalls eine Verbindung zum Internet auf. Für diesen Internetzugang wird eine feste public IP benötigt. Über einen IPSec-Tunnel sollen daraufhin die LAN-Subnetze beider Router miteinander verbunden werden, so dass alle Netzwerkteilnehmer am LAN2 des CR230U mit allen Netzwerkteilnehmern am Vigor2910-LAN miteinander kommunizieren können.



### 3. Netzwerkstruktur der IPSec-Verbindung mit Beispieladressen



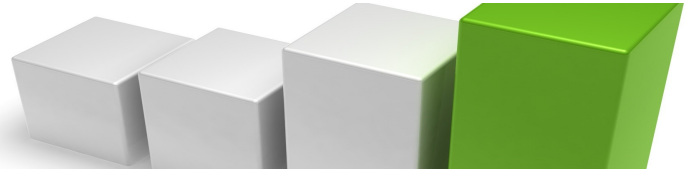
Testzugriffe:

PC1 → CR230U	ping 192.168.2.127
PC1 → IO1:	ping 192.168.2.20
PC1 → IO2:	ping 192.168.2.21
PC1 → IO3:	ping 192.168.2.22

Tipp1: PCs auf der Vigor2910-Seite (z.B. PC1) können die Konfigurationsseiten des CR230U durch den IPSec-Tunnel aufrufen. Die zugehörige URL lautet: <http://192.168.2.127:7777>

Tipp2: Das LAN1 des CR230U ist vom IPSec-Tunnel getrennt und kann für lokale Teilnehmer benutzt werden, die über IPSec nicht erreichbar sein sollen (z.B. PCs). LAN2-Teilnehmer können mit LAN1-Teilnehmern kommunizieren.

Tipp3: LAN1- und LAN2-Teilnehmer des CR230U können das Internet benutzen.



## 4. Checkliste zur Inbetriebnahme der IPSec-Verbindung CR230U-Vigor2910

### 1. Vorbereitungen

- Das "LAN" des Vigor2910 wird mit den lokalen Netzwerkteilnehmern verbunden, die später den IPSec-Tunnel benutzen sollen. z.B. PC1,PC2, usw.
- Das LAN2-Interface des CR230U wird mit den lokalen Netzwerkteilnehmern verbunden, die später den IPSec-Tunnel benutzen sollen, z.B. IO1,IO2,IO3, usw.
- Das LAN1-Interface des CR230U wird mit einem Konfigurations-PC verbunden. Konfigurationsseiten des "CR230U" auf dem Konfigurations-PC aufrufen:  
<http://192.168.0.127:7777>
- login: admin

### 2. CR230U-Werkseinstellung herstellen (siehe Bild1):

- System → System management:
- Schalter „DEFAULT“ betätigen.
  - 1 min warten.
  - login: admin

### 3. CR230U-WAN-Interface konfigurieren. (siehe Bild2)

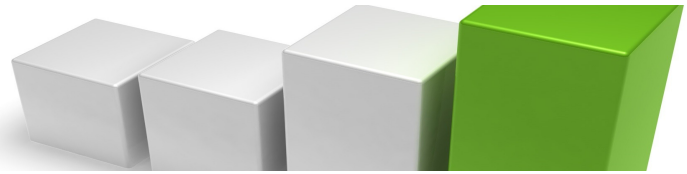
- Network → WAN → ISP settings:
- Provider: D2 (Beispiel)
  - SIM PIN: 0815 (Beispiel)
  - Confirm SIM PIN: 0815 (Beispiel)
- Network → WAN → Connection settings:
- Connect type: System start, always reconnect
  - Apply-Schalter betätigen.

### 4. CR230U-LAN2-Subnetzadresse konfigurieren: (siehe Bild3)

- Network → LAN → LAN2:
- IP address: 192.168.2.127
  - Subnet mask: 255.255.255.0
  - Apply-Schalter betätigen.

### 5. CR230U-IPSec-Client konfigurieren: (siehe Bild4 und Bild5)

- VPN → IPSec → IPSec status:
- Enable/Disable IPSec: aktivieren
- VPN → IPSec → eroute (Click auf den grünen Balken zum Öffnen)
- remote WAN-IP: 217.95.193.93 (Beispiel)
  - local subnet address: 192.168.2.0
  - local subnet mask: 255.255.255.0
  - remote subnet address: 192.168.1.0
  - remote subnet mask: 255.255.255.0
  - local ID: 192.168.2.127
  - remote ID: 217.95.193.93
- (Beispiel, hier die feste WAN-IP des Vigor2910 eintragen)



VPN → IPSec → Certificates (Click auf den grünen Balken zum Öffnen)

- Preshared Key:                   hallo (hier den Preshared Key eintragen)
- Confirm Preshared Key: hallo (Preshared Key Eintrag wiederholen)

VPN → IPSec → Key specifics and DPD (Click auf den grünen Balken zum Öffnen)

- PFS:                                 no
- alle anderen Voreinstellungen unverändert lassen.
- Apply-Schalter betätigen.

#### 6. Vigor2910-Firmwareversion testen: (Bild6)

Systemmanagement → Systemstatus:

- Firmwareversion kontrollieren.

Achtung: es muss mindestens Version 3.2.1 installiert sein. Andernfalls müssen Sie den Vigor2910 unbedingt updaten !!!

#### 7. Vigor2910-WAN-Internetzugang herstellen:

Da es für die Herstellung des WAN-Zugangs am Vigor2910 sehr viele Möglichkeiten gibt, wird der WAN-Zugang hier nicht beschrieben (siehe Vigor2910-Handbuch). Wichtig ist, dass der WAN-Zugang eine feste public IP erhält.

Achtung: Der Schalter „WAN-IP Alias“ darf nicht betätigt werden !!!

#### 8. Vigor2910-IPSec-Grundeinstellungen: (siehe Bild7)

VPN und externe Einwahl → IPSec Grundeinstellungen

- Preshared Key aus Punkt 5 eintragen, bestätigen.
- Alle Verschlüsselungsarten aktivieren.
- OK-Schalter betätigen.

#### 9. Vigor2910-Lan-zu-Lan: (siehe Bild8 bis Bild11)

Lan-zu-LAN → Index1 → 1.Allgemeine Einstellungen: (siehe Bild9)

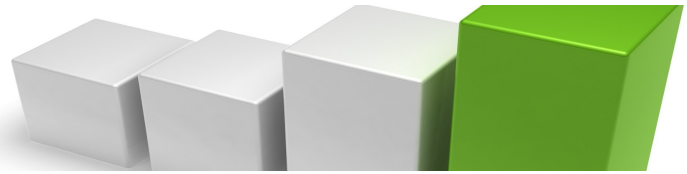
- Profilname:                         hallo (Beispiel)
- Checkbox aktiv:                   aktivieren
- VPN-Verbindung mit:             erst WAN1
- Anrufrichtung:                   „Rein“ aktivieren

Lan-zu-Lan → Index1 → 3.Einstellungen zum Einwählen: (siehe Bild10)

- IPSec:                               aktivieren
- Definieren Sie Remote Gateway-IP: aktivieren
- oder Peer-ID:                      192.168.2.127
- IKE Preshared Key:               aktivieren
- alle Schlüssel aktivieren

Lan-zu-Lan → Index1 → 4.TCP/IP Netzwerk-Einstellungen. (siehe Bild11)

- Remote Netzwerk-IP:             192.168.2.0
- Remote Netzwerk-Maske:         255.255.255.0
- Schalter „Mehr“ nicht betätigen.



## 5. Darstellung der zugehörigen Konfigurationsseiten zum Kapitel 4 dieser Doku

Bild 1 CR230U Werkseinstellung herstellen:

### System management

System management	
Reboot system :	<input type="button" value="REBOOT"/>
Reload factory defaults:	<input type="button" value="DEFAULTS"/>
System configuration	
Configuration download :	<input type="button" value="DOWNLOAD"/>
Configuration upload :	<input type="text"/> <input type="button" value="Durchsuchen..."/>

<input type="button" value="OK"/>	<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>
-----------------------------------	--------------------------------------	---------------------------------------

Bild 2 CR230U WAN-Interface konfigurieren:

### WAN configuration

ISP settings	
Provider :	<input type="text" value="D2"/>
SIM PIN :	<input type="text" value="...."/>
Confirm SIM PIN :	<input type="text" value="...."/>
DNS :	<input type="text" value="Automatic"/>
Gateway :	<input type="text" value="Automatic"/>
Connection settings	
Connect type :	<input type="text" value="System start, always reconnect"/>
Manuell test :	<input type="button" value="Connect"/> <input type="button" value="Disconnect"/> <input type="button" value="Check Modem"/>
Connection State :	Connected signal quality: -81 dBm / 3G-cell: HSDPA+HSUPA

<input type="button" value="OK"/>	<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>
-----------------------------------	--------------------------------------	---------------------------------------

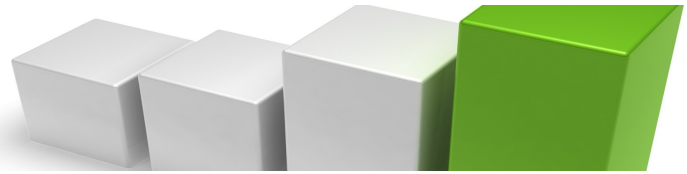


Bild 3 CR230U LAN2-Subnetzadresse konfigurieren

## LAN configuration

LAN1 configuration	
Enable/Disable interface LAN1 :	<input checked="" type="checkbox"/>
DHCP-client :	<input type="radio"/>
Use the following IP address :	<input checked="" type="radio"/>
IP address :	192 . 168 . 0 . 127
Subnet mask :	255 . 255 . 255 . 0
Enable/Disable alias IP address :	<input type="checkbox"/>

LAN2 configuration	
Enable/Disable interface LAN2 :	<input checked="" type="checkbox"/>
DHCP-client :	<input type="radio"/>
Use the following IP address :	<input checked="" type="radio"/>
IP address :	192 . 168 . 2 . 127
Subnet mask :	255 . 255 . 255 . 0

DNS configuration	
Use a DNS server address :	<input type="checkbox"/>

Default gateway configuration	
Use a gateway address :	<input type="checkbox"/>

OK	Apply	Cancel
----	-------	--------

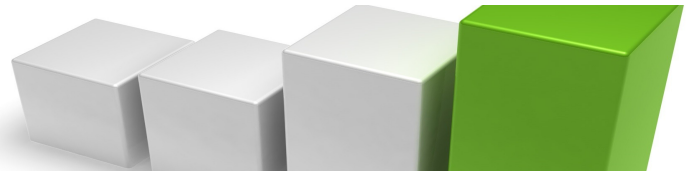


Bild4 und Bild 5 CR230U IPSec-Client konfigurieren

### IPsec configuration

IPsec status	
Enable/Disable IPsec:	<input checked="" type="checkbox"/>
Status:	IPSec SA established <span style="float: right;">Status</span>
(-) eroute	
Protocol:	NAT-T : NAT routers between endpoints
Server or client:	Client
remote WAN-IP:	217.95.193.93
local subnet address:	192 . 168 . 2 . 0
local subnet mask:	255 . 255 . 255 . 0
remote subnet address:	192 . 168 . 1 . 0
remote subnet mask:	255 . 255 . 255 . 0
local ID / remote ID:	192.168.2.127   217.95.193.93
(+ Certificates	
(+ Key specifics and DPD	

### IPsec configuration

IPsec status	
Enable/Disable IPsec:	<input checked="" type="checkbox"/>
Status:	IPSec SA established <span style="float: right;">Status</span>
(+ eroute	
(-) Certificates	
Authentication:	Pre-Shared Keys
Preshared Key:	•••••
Confirm Preshared Key:	•••••
(-) Key specifics and DPD	
Aggressive Mode:	Disable
PFS:	no
Algorithms for phase2:	secure set of defaults
IKE lifetime (s) / IPSEC lifetime (s):	86400   3600
Rekey Margin (s) / Rekey Fuzz (%):	540   100
DPD Delay (s) / DPD Timeout (s):	30   120

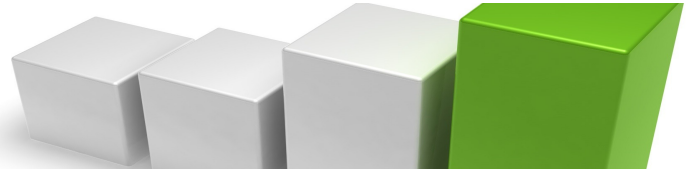


Bild6 Vigor2910 Firmwareversion testen

### Systemstatus

Modellname : Dray Tek Vigor2910  
Firmwareversion : 3.2.1  
Erstellungsdatum : Wed Aug 20 16:17:22.19 2008

Bild7 Vigor2910 IPSec-Grundeinstellungen

**Vigor2910 Series**  
Dual-WAN Security Router

DrayTek  
www.draytek.com

Schnellstart-Assistent  
Onlinestatus

WAN  
LAN  
NAT  
Firewall  
Objekte  
CSM  
Bandbreitenmanagement  
Anwendungen  
VPN und externe Einwahl  
▶ VPN-Client-Assistent  
▶ VPN-Server-Assistent  
▶ Einwahlmöglichkeiten  
▶ PPP-Einstellungen  
▶ IPSec Grundeinstellungen  
▶ IPSec-Identität  
▶ Externe Benutzer  
▶ LAN-zu-LAN  
▶ VPN Backup Management  
Status: Bereit

VPN und externe Einwahl >> IPSec Grundeinstellungen

IKE/IPSec Grundeinstellungen  
Einstellungen für die Einwahl in diesen Router von außen (LAN-zu-LAN).

IKE-Authentifizierungsmethode  
Pre-Shared Key  
Pre-Shared Key bestätigen

IPSec-Sicherheitsmethode  
 Mittel (AH)  
Daten werden authentifiziert, aber nicht verschlüsselt.

Hoch (ESP)  DES  3DES  AES  
Daten werden sowohl authentifiziert als auch verschlüsselt.

OK Abbrechen

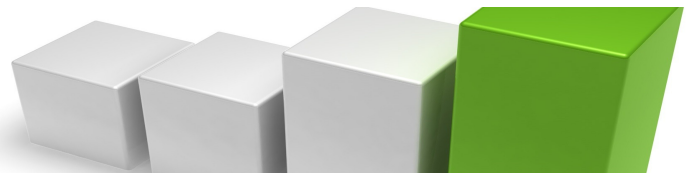
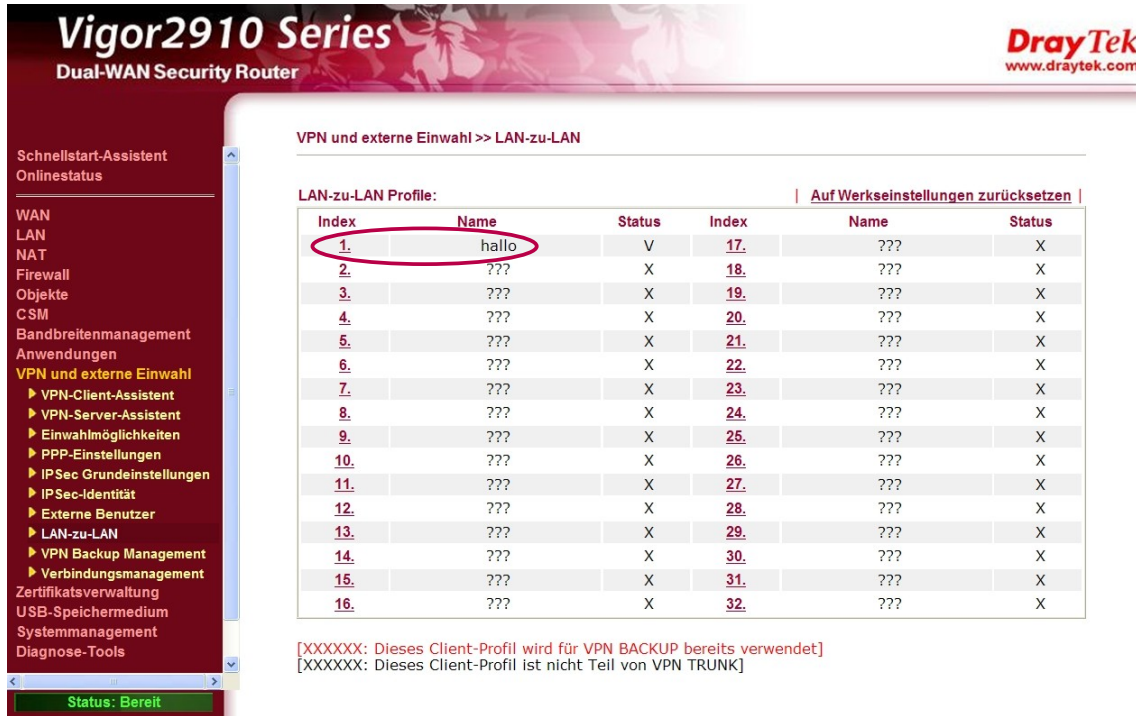


Bild 8 Vigor2910 Lan-zu-LAN Aufruf



**Vigor2910 Series**  
Dual-WAN Security Router

DrayTek  
www.draytek.com

VPN und externe Einwahl >> LAN-zu-LAN

LAN-zu-LAN Profile: [Auf Werkseinstellungen zurücksetzen](#)

Index	Name	Status	Index	Name	Status
1.	hallo	V	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

[XXXXXX: Dieses Client-Profil wird für VPN BACKUP bereits verwendet]  
[XXXXXX: Dieses Client-Profil ist nicht Teil von VPN TRUNK]

Status: Bereit

Bild9 Vigor2910 Lan-zu-Lan Allgemeine Einstellungen

VPN und externe Einwahl >> LAN-zu-LAN

Profil Index : 1

1. Allgemeine Einstellungen

Profilname: <input type="text" value="hallo"/>	Anrufrichtung: <input type="radio"/> Beide <input type="radio"/> Raus <input checked="" type="radio"/> Rein
<input checked="" type="checkbox"/> aktiv	<input type="checkbox"/> immer in Betrieb
VPN-Verbindung mit: <input type="text" value="erst WAN1"/>	Max. Leerlaufzeit: <input type="text" value="0"/> Sekunden
NetBIOS-Name durchlassen: <input checked="" type="radio"/> ja <input type="radio"/> nein	<input type="checkbox"/> Dauer-Ping aktiv
Multicast via VPN: <input type="radio"/> ja <input checked="" type="radio"/> nein (z.B. für IGMP, IP-Kameras, DHCP-Relay, usw.)	Ping an die IP: <input type="text"/>

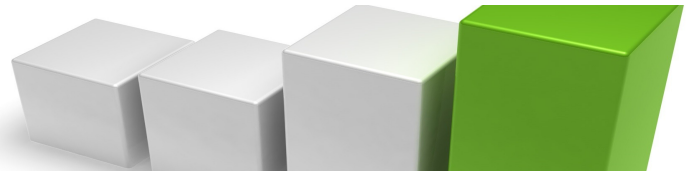


Bild10 Vigor2910 Einstellungen zum Einwählen

**3. Einstellungen zum Einwählen**

<p><b>Einwahl zulassen über</b></p> <p><input checked="" type="checkbox"/> ISDN</p> <p><input type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec</p> <p><input type="checkbox"/> L2TP mit IPsec <span>nein</span></p> <hr/> <p><input checked="" type="checkbox"/> Definieren Sie Remote Gateway-IP Peer VPN-Server-IP</p> <p><input type="text"/></p> <p>oder Peer-ID <input type="text" value="192.168.2.127"/></p>	<p>Benutzername <input data-bbox="1070 488 1273 517" type="text" value="???"/></p> <p>Passwort <input type="password"/></p> <p>VJ-Komprimierung <input checked="" type="radio"/> An <input type="radio"/> Aus</p> <hr/> <p><b>IKE-Authentifizierungsmethode</b></p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p><input type="button" value="IKE Pre-Shared Key"/> <input type="password" value="....."/></p> <p><input type="checkbox"/> Digitale Signatur (X.509)</p> <p><input type="text" value="nein"/></p> <hr/> <p><b>IPSec-Sicherheitsmethode</b></p> <p><input checked="" type="checkbox"/> Mittel (AH)</p> <p>Hoch (ESP)</p> <p><input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <hr/> <p><b>Rückrufeinstellungen (CBCP)</b></p> <p><input type="checkbox"/> Rückruffunktion aktiv</p> <p><input type="checkbox"/> Rückrufnummer festlegen</p> <p>Rückrufnummer <input type="text"/></p> <p>max. Rückrufdauer <input type="text" value="0"/> Minuten</p>
--	--

Bild11 Vigor2910 TCP/IP Netzwerk-Einstellungen

**4. TCP/IP Netzwerk-Einstellungen**

<p>Meine WAN-IP <input type="text" value="0.0.0.0"/></p> <p>Remote Gateway-IP <input type="text" value="0.0.0.0"/></p> <p>Remote Netzwerk-IP <input type="text" value="192.168.2.0"/></p> <p>Remote Netzwerk-Maske <input type="text" value="255.255.255.0"/></p> <p><input type="button" value="Mehr"/></p>	<p>RIP-Richtung <input type="text" value="inaktiv"/></p> <p>Vom ersten bis zum entfernten Subnetz soll der VPN-Tunnel</p> <p><input type="text" value="Routen"/></p> <hr/> <p><input type="checkbox"/> Alle Anfragen ins Internet über diesen Tunnel leiten (nicht bei aktivem Dual-WAN möglich)</p>
--	--