

# VPN Verbindungen mit Draytek Router 2600 / 2900 / 2910 [Stand: 2007-05]

## Modellübersicht:

Die 2600er Serie besitzt ein integriertes DSL Modem (bis zu 3Mbit downstream), jedoch keinen WAN Anschluss und arbeitet daher nicht mit externen DSL Modems zusammen. Die 2900er Serie besitzt kein integriertes DSL Modem. Diese Router unterstützen PPPoE/PPTP für den Verbindungsaufbau und sind somit weitaus flexibler (Annex-A Modem, Annex-B Modem, Kabelmodem etc.) Der WAN Port beim 2900er leistet z. B. bis zu 30Mbit Die 2910er Serie hat ebenfalls kein integriertes DSL Modem, bietet zusätzlich einen zweiten WAN Port, Load Balancing, Internet Content Filter sowie ein Bandbreitenmanagement. Jedes der verfügbaren Modelle hat einen integrierten 4 Port Switch, DynDNS Support und einen VPN Server mit 16 simultanen Verbindungen. Des weiteren sind noch verschiedene Modellausprägungen auf dem Markt verfügbar. Diese erkennt man an den Buchstaben hinter der Modellbezeichnung. Nachfolgend die am weitest verbreiteten Modelle:

- 2910            Standardmodell
- 2910V        zusätzlich mit Voice Over IP
- 2910Gi       zusätzlich mit 54Mbit WLAN und ISDN
- 2910VGi     zusätzlich mit VoIP, WLAN und ISDN



Die Screenshots der Anleitung beziehen sich auf das aktuelle 2910 Modell. Die Konfigurationsmasken der früheren Modelle sind zu den neuen grösstenteils identisch, nur bieten die neuen eben teilweise mehr Funktionen. Zudem befinden sich die Masken beim 2910 nicht mehr alle im direkt im Hauptmenü, sondern in einer Navigationsleiste. Bei beiden Modellen findet man sich jedoch schnell zurecht.

## Vigor2910 Series

Dual-WAN Security Router

www.draytek.com

Schnellstart Assistent  
Onlinestatus

---

WAN  
LAN  
NAT  
Firewall  
Objekte und Gruppen  
Bandbreite Management  
Anwendungen  
VPN und externe Einwahl  
Zertifikatsverwaltung  
VoIP  
ISDN  
Wireless LAN  
VLAN  
Systemmanagement  
Diagnose Tools

Alle Rechte vorbehalten.

**Systemstatus**

Modell Name : DrayTek Vigor2910  
Firmware Version : v3.0.2  
Erstellungsdatum : Tue Aug 22 16:41:58.53 2006

LAN	WAN 1
MAC-Adresse : 00-50-7F-33-F4-B6	Link Status : <span style="color: red;">Disconnected</span>
1te IP-Adresse : 192.168.2.155	MAC-Adresse : 00-50-7F-33-F4-B7
1te Subnetz Maske : 255.255.255.0	Verbindung : -----
DHCP Server : J	
DNS : 19	

**VoIP**

Port : 1  
SIP Registrar :  
Konto ID : cha  
Verzeichnis :  
Codec :  
eingehende Anrufe : 0  
ausgehende Anrufe : 0

**DrayTek** Firmware Version : v2.5.9.1\_J213  
Erstelldatum: Fri Oct 13 18:14:57 2006  
LAN MAC-Adresse : 00-50-7F-28-3E-1B

**Grundeinstellungen**

- [Schnellstart Assistent](#)
- [Administrator Passwort](#)
- [LAN und DHCP](#)
- [ISDN](#)
- [Wireless LAN](#)

**Erweiterte Einstellungen**

- [Dynamisches DNS](#)
- [Verbindungseinstellungen PPP/MP](#)
- [Verbindungstimer](#)
- [NAT](#)
- [RADIUS](#)
- [Feste Adressumleitung](#)
- [IP Filter und Firewall](#)
- [VPN und externe Einwahl](#)
- [UPnP](#)
- [VoIP \(Internettelefonie\)](#)
- [VLAN](#)

**Schnellstart (2.Schritt)**

- [Einwahl ins Internet](#)
- [Virtueller TA](#)

**Systemmanagement**

- [Onlinestatus](#)
- [VPN Verbindungsmanagement](#)
- [Erstellen / Laden eines Backups](#)
- [SysLog und Mail-Alarm](#)
- [Zeit und Datum](#)
- [Verwaltung](#)
- [Diagnose Tools](#)
- [Neustart](#)
- [Firmware aktualisieren](#)

Vergleich Menüstruktur Draytek 2910 / 2900

### IP Adresse des Routers ändern:

Die Router besitzen im Auslieferungszustand die IP 192.168.1.1 und lassen sich webbasiert konfigurieren. Um die IP zu ändern, muss sich der PC, an dem die Konfiguration vorgenommen wird, im selben IP Bereich befinden. Browser starten, <http://192.168.1.1> eintragen und als Benutzer „admin“ eingeben. Die IP lässt sich unter „LAN“. konfigurieren. Optional kann hier ein DHCP Server sowie eine zweite IP definiert werden.

#### Ethernet TCP / IP und DHCP

<b>LAN Konfiguration</b> NAT: 1te IP-Adresse <input type="text" value="192.168.1.254"/> 1te Subnetz Maske <input type="text" value="255.255.255.0"/> IP Routing <input type="radio"/> aktiv <input checked="" type="radio"/> inaktiv 2te IP-Adresse <input type="text" value="192.168.2.1"/> 2te Subnetz Maske <input type="text" value="255.255.255.0"/> <input type="button" value="2ter Subnetz DHCP-Server"/> RIP <input type="text" value="inaktiv"/>	<b>DHCP Server</b> <input checked="" type="radio"/> aktiv <input type="radio"/> inaktiv Relay Agent: <input type="radio"/> 1tes Subnetz <input checked="" type="radio"/> 2tes Subnetz Start IP-Adresse <input type="text" value="192.168.1.80"/> IP Pool (max. Anzahl) <input type="text" value="50"/> Gateway IP-Adresse <input type="text" value="192.168.1.254"/> DHCP Server IP-Adresse für Relay Agent <input type="text"/> <b>DNS Server</b> <input type="checkbox"/> Folgende DNS Einstellungen verwenden Primäre IP-Adresse <input type="text"/> Sekundäre IP-Adresse <input type="text"/>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### Routerpasswort definieren:

Das Passwort für den Router lässt sich unter Systemmanagement\ Administrator Passwort setzen.

### Firmware Update:

Oftmals sind in neueren Firmwareversionen Fehler vom Hersteller ausgebessert worden. Daher macht es Sinn, auf die aktuellste Version zu Updaten. Die 2900 Serie war z. B. erst bei Version 2.5.9.1-(2)(3) dauerhaft stabil. Um die Firmware updaten zu können muss sich der Router im sogenannten TFTP Server Modus befinden. Dies erreicht man zum einen über das Webinterface in Systemmanagement\ Firmware aktualisieren oder in dem man während des Einschaltens den Resetknopf für 5 Sekunden lang gedrückt hält. Ist der Router im TFTP Modus blinken die beiden linken LEDs „ACT“ und „ISDN“. Er bleibt für 40 Sekunden aktiv. Um die Firmware zu aktualisieren, benötigt man das Firmware Upgrade Utility (auf [www.vigorkom.de](http://www.vigorkom.de) zu finden). Es ist die IP und der Pfad zur Datei anzugeben, sowie ggf. das Passwort. Man erhält von Draytek immer 2 Dateien (des selben Softwarestands), eine \*.all, sowie eine \*.rst Datei. Die \*.all Datei behält die aktuellen Einstellungen des Routers bei, die \*.rst setzt ihn auf Werkseinstellungen.

Timeout (s)	Vigor IP
<input type="text" value="5"/>	<input type="text" value="192.168.1.254"/>
Port	Pfad zur Firmware
<input type="text" value="69"/>	<input type="text" value="G:\Vigor2910 Serie - Firmware -"/>
Passwort	
<input type="text"/>	<input type="button" value="Abbrechen"/> <input type="button" value="Senden"/>

## Internetzugangsdaten eintragen / Zwangstrennungzeitpunkt definieren

Um die Zugangsdaten eintragen zu können muss man zuerst im Menü WAN\ Einwahl ins Internet\ den WAN Port wählen, sowie die Verbindungsart.

### Einwahl ins Internet

Index	Anzeigename	Modus	Verbindungsart	
WAN1		Ethernet	PPPoE	Details
WAN2		Ethernet	keine	Details

Über Details kommt man ins Menü für die Zugangsdaten.

### WAN >> Einwahl ins Internet

#### WAN 1

<p><b>PPPoE Modus</b></p> <p><input checked="" type="radio"/> aktiv <input type="radio"/> inaktiv</p> <hr/> <p><b>ISP Einstellungen</b></p> <p>Benutzername: <input type="text" value="7209#0001@t-online.de"/></p> <p>Passwort: <input type="password" value="....."/></p> <p>Index (1-15) aus der <b>Verbindungstimer</b> Konfiguration: =&gt; <input type="text" value="1"/>, <input type="text" value="2"/>, <input type="text" value=""/>, <input type="text" value=""/></p> <p><b>Alternative Einwahlmöglichkeit mit ISDN</b></p> <p>ISDN-Backup: <input type="text" value="nein"/></p>	<p><b>PPP/MP Einstellungen</b></p> <p>PPP Authentifizierung: <input type="text" value="PAP oder CHAP"/></p> <p>Max. Leerlaufzeit: <input type="text" value="-1"/> Sekunden</p> <p><b>IP Adresszuweisung (IPCP)</b> <input type="button" value="WAN IP Alias"/></p> <p>Feste IP: <input type="radio"/> Ja <input checked="" type="radio"/> Nein (dynamische IP)</p> <p>Feste IP-Adresse: <input type="text"/></p> <hr/> <p><input checked="" type="radio"/> Voreingestellte MAC-Adresse verwenden  <input type="radio"/> MAC-Adresse selbst definieren</p> <p>MAC-Adresse:  <input type="text" value="00"/> <input type="text" value=".50"/> <input type="text" value=".7F"/> <input type="text" value=":33"/> <input type="text" value=".F4"/> <input type="text" value=".B7"/></p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Nach dem Eintragen der Zugangsdaten kann man über die Option Verbindungstimer einen Zeitpunkt definieren, zu dem der Router die Internetverbindung deaktiviert. Wird eine Verbindung ins Internet hergestellt, so trennt der Provider in der Regel nach 24 Stunden automatisch. Über den Timer kann man den Zeitpunkt Zwangstrennung steuern, damit die Trennung nicht während der Geschäftszeit erfolgt. Dies wäre z. B. bei Standortkopplungen oder Remoteeinwahlen inakzeptabel, da laufende Datenströme für einige Sekunden unterbrochen werden würden. Im Router müssen hierfür Zeitpunkte definiert werden, in denen die Verbindung aktiv sein bzw. getrennt werden soll. Im Verbindungstimermenü klickt man auf 1., definiert den Zeitpunkt für die aktive Verbindung (Startzeit täglich 00:01, Dauer 23:49), danach auf OK und auf Abbrechen um wieder zum Timermenü zurückzukehren. Danach definiert man den Zeitpunkt für den Verbindungsabbau (Startzeit täglich 23:51, Dauer 5 Min.) Damit die Timer für die Verbindung aktiv werden, muss im Menü der

#### Verbindungstimer:

Index	Status
1.	v
2.	v
3.	x

#### Index Nr. 1

<input checked="" type="checkbox"/> aktiv	
Anfangsdatum (yyyy-mm-dd)	<input type="text" value="2000"/> <input type="text" value="1"/> <input type="text" value="1"/>
Startzeit (hh:mm)	<input type="text" value="0"/> <input type="text" value="1"/>
Dauer (hh:mm)	<input type="text" value="23"/> <input type="text" value="49"/>
Aktion	<input type="text" value="Verbindung aufbauen"/>
Max. Leerlaufzeit	<input type="text" value="0"/> Minute(n) - max. 255, 0
<b>Wiederholungen</b>	
<input type="radio"/> einmalig	
<input checked="" type="radio"/> wochentags	
	<input checked="" type="checkbox"/> So <input checked="" type="checkbox"/> Mo <input checked="" type="checkbox"/> Di <input checked="" type="checkbox"/> Mi <input checked="" type="checkbox"/> Do <input checked="" type="checkbox"/> Fr <input checked="" type="checkbox"/> Sa

Internetzugangsdaten „1“ und „2“ bei Verbindungstimerkonfiguration eingefügt werden, siehe oben.

#### Index Nr. 2

<input checked="" type="checkbox"/> aktiv	
Anfangsdatum (yyyy-mm-dd)	2000 . 1 . 1
Startzeit (hh:mm)	23 : 54
Dauer (hh:mm)	0 : 2
Aktion	Verbindung beenden
Max. Leerlaufzeit	0 Minute(n) - max. 255, 0 ist voreingestellt
Wiederholungen	
<input type="radio"/> einmalig	
<input checked="" type="radio"/> wochentags	
<input checked="" type="checkbox"/> So	<input checked="" type="checkbox"/> Mo
<input checked="" type="checkbox"/> Di	<input checked="" type="checkbox"/> Mi
<input checked="" type="checkbox"/> Do	<input checked="" type="checkbox"/> Fr
<input checked="" type="checkbox"/> Sa	

Da der Router die Uhrzeit nach einem Abschaltvorgang verliert ist es erforderlich, dass sich der Router die Zeit aus dem Internet holt. Einstellen kann man dies unter Systemmanagement\ Zeit und Datum. Hier die Zeitzone korrekt einstellen und den Haken bei Sommer/Winterzeit setzen.

Alternative Zeitserver: ptb1.ptb.de, time.nist.gov, time.windows.com

#### Zeitinformation

Aktuelle Systemzeit	2007 Feb 22 Thu 14 : 37 : 5	Zeit abrufen
---------------------	-----------------------------	--------------

#### Zeit und Datum

<input type="radio"/> Rechner/Browser-Zeit	
<input checked="" type="radio"/> Internet-Zeit	
Zeitprotokoll	NTP (RFC-1305)
Server IP-Adresse	pool.ntp.org
Zeitzone	(GMT+01:00) Amsterdam, Berlin, Bern
autom. auf Sommer-/Winterzeit umstellen	<input checked="" type="checkbox"/>
Aktualisierungsintervall	30 Min.

OK Abbrechen

#### Anmerkung für 2900 Serie:

Der Router beginnt nach einer Stromunterbrechung wieder bei 0:00 Uhr. Wird der Timer für den Verbindungsaufbau z. B. auf 1:00 Uhr gesetzt, würde der Router erst nach 1 Stunde die Verbindung wieder automatisch aufbauen und die Zeit synchronisieren. Dieser Router orientiert sich am Startpunkt und nicht an der Verbindungsdauer. D. h. der Verbindungsaufbau muss zwingend auf 0:00 gestellt werden.

#### Anmerkung für 2910 Serie:

Dieser Router orientiert sich beim Verbindungsaufbau an der Verbindungsdauer. D. h. es kann ein beliebiger Zeitraum definiert werden, sofern keine Konflikte zwischen Verbindungsabbau und -aufbau bestehen. Momentan (Firmware v3.02) darf der Verbindungsaufbau jedoch nicht gleich 0:00 sein, da der Router sonst abstürzen würde und

via Firmware zurückgesetzt werden müsste. Dies wird in einer zukünftigen Firmware behoben werden.

## VPN Verbindungen / externe Einwahl (PPTP / IP Sec)

### Dynamisches DNS

Sofern man keinen Internetzugang mit Fester IP besitzt, erhält man vom Provider bei jedem Internetverbindungsaufbau eine neue IP Adresse. Um einen externen Zugriff über das Internet zu ermöglichen, müsste dem Remoteuser die jeweils aktuelle IP bekannt sein. Es gibt Internetdienste, die diese dynamisch zugewiesene IP registrieren und einem benutzerdefinierten Domainnamen „hinterlegen“ können. Wird die Internetverbindung neu aufgebaut, teilt der Router dem DynDNSanbieter die neue IP Adresse mit. Daher muss der Router diese Funktion beherrschen. Draytek unterstützt aktuell folgende Anbieter: dyndns.org, no-ip.com, dtdns.com, changeip.com, dns4biz.com, ddns.com.cn und oray.net. Bei einem dieser Anbieter muss also ein Benutzeraccount und ein Domainname angelegt werden. Danach müssen diese Zugänge im Router eingetragen werden: Unter Anwendungen\ Dynamisches DNS den Haken bei aktiv setzen und eine der 3 Verbindungsmöglichkeiten anklicken. Hier erneut aktivieren, den Anbieter auswählen und den Domainnamen eintragen sowie den dazugehörigen Benutzernamen und das Passwort.

#### Anwendungen >> DynDNS >> Konto Einstellungen

##### Index : 1

<input checked="" type="checkbox"/> aktiv			
WAN Schnittstelle	erstWAN1		
Anbieter	dyndns.org (www.dyndns.org)		
Servicetyp	dynamisch		
Domain Name	drmuster	.dyndns.org	dyndns.org
Login Name	muster	(max. 23 Zeichen)	
Passwort	●●●●●●	(max. 23 Zeichen)	
<input type="checkbox"/> Wildcards			
<input type="checkbox"/> Backup MX			
Mailerweiterung			

OK

Löschen

Abbrechen

Um die Funktion zu kontrollieren, gibt es im DynDNS Menü den Punkt “Log anschauen“. Nachfolgend ein Beispiel Log nach erfolgreicher IP Aktualisierung

#### DDNS Log

```
00:01:58.0 >>>> DDNS is updating. <<<<<
00:01:58.0 A= sn-gmbh4, H= mueller, U= 1
00:02:02.4 Connecting to the DDNS server (0x3fd0c45e)...
00:02:02.5 Return Code= good 84.154.87.178
00:02:02.5 Updated successfully.
```

## Einwahl über PPTP (Point-to-Point Tunneling Protocol)

Das PPTP Protokoll ist in Windows 2000/XP bzw. Vista bereits integriert und bietet eine einfache Möglichkeit eines Verbindungsaufbaus ohne zusätzliche Software zu installieren. PPTP gilt jedoch als entschlüsselbar, sofern eine aufgebaute Verbindung über Tage hinweg mitgeschnitten wird. Es ist daher nur für gelegentliche Fernwartungen empfehlenswert. Technisch möglich wäre auch eine Verbindung über den Draytek SmartVPN Client. Dieser beherrscht auch IPSec, muss aber separat installiert werden.

Das Hostnetzwerk muss in einem anderen TCP/IP Bereich als das Remotenetzwerk liegen um einen Netzwerkressourcenzugriff zu ermöglichen. Würden die Netze identisch sein, kommen Suchanfragen (z. B. nach einem PC) nicht über das lokale Netzwerk hinaus. Es gibt 2 Möglichkeiten ein Einwahlkonto anzulegen: Entweder über das Feld „Externe Benutzer“ oder über das „LAN-zu-LAN“ Profil. Im LAN-zu-LAN Profil sind erweiterte Konfigurationsmöglichkeiten vorhanden wie z. B. eine feste Zuweisung der Einwahl IP. Dies benötigt man beispielsweise, wenn sich mehrere Computer einwählen und auf diese übers Netzwerk zugegriffen werden soll (Remotedrucken).

Einstellungen am Router:

Bei VPN und externe Einwahl\ Einwahlmöglichkeiten kontrollieren, ob Haken bei PPTP gesetzt.

- *Einwahl über Externe Benutzer:*

- VPN und externe Einwahl\ Externe Benutzer ein Benutzerprofil wählen
- Auf aktiv schalten, Benutzername, Kennwort vergeben und Leerlaufzeit auf „0“ stellen.

### VPN und externe Einwahl >> Externe Benutzer

#### Index Nr. 1

<b>Benutzerkonto und Authentifizierung</b>	
<input checked="" type="checkbox"/> aktiv	Benutzername <input type="text" value="user1"/>
Max. Leerlaufzeit <input type="text" value="0"/> Sekunden	Passwort <input type="password" value="••••••"/>

- *Einwahl über LAN-zu-LAN Profil:*

- VPN und externe Einwahl\ LAN-zu-LAN ein Benutzerprofil wählen
- Name für das Profil vergeben und Haken bei „Aktiv“ setzen
- Anrufrichtung auf „rein“ stellen und Leerlaufzeit auf „0“ stellen
- Den Punkt „2. Einstellungen zum Rauswählen“ kann man in diesem Fall übergehen
- Unter „3. Einstellungen zum Einwählen“ Benutzername und Kennwort vergeben
- In „4. TCP/IP Netzwerk-Einstellungen“ kann optional die IP festgelegt werden, die der PC bei der Einwahl erhält. Diese muss bei „Remote Gateway IP“ eingetragen werden.

**Profil Index : 1**

**1. Allgemeine Einstellungen**

Profil Name <input type="text" value="PC1"/> <input checked="" type="checkbox"/> aktiv	Anrufrichtung: <input type="radio"/> Beide <input type="radio"/> Raus <input checked="" type="radio"/> Rein <input type="checkbox"/> Immer in Betrieb Max. Leerlaufzeit <input type="text" value="0"/> Sekunden <input type="checkbox"/> Dauer-Ping aktiv Ping an die IP-Adresse <input type="text"/>
VPN Verbindung durch: <input type="text" value="erstWAN1"/>	

**3. Einstellungen zum Einwählen**

ISDN Number oder VPN Server IP-Adresse <b>Einwahl zulassen über</b> <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP mit IPsec <input type="text" value="nein"/>	Benutzername <input type="text" value="User1"/> Passwort <input type="password" value="....."/> VJ Komprimierung <input checked="" type="radio"/> An <input type="radio"/> Aus <b>IKE Authentifizierungsmethode</b>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

Meine WAN-IP <input type="text" value="0.0.0.0"/> Remote Gateway-IP <input type="text" value="192.168.1.81"/> Remote Netzwerk-IP <input type="text" value="0.0.0.0"/> Remote Netzwerk-Maske <input type="text" value="255.255.255.0"/> <input type="button" value="Mehr"/>	RIP Richtung <input type="text" value="inaktiv"/> RIP Version <input type="text" value="Ver. 2"/> Im NAT-Betrieb, betrachte entfernte Subnetze als <input type="text" value="private IP"/> <input type="checkbox"/> Alle Anfragen ins Internet über diesen Tunnel leiten (Default Route)
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

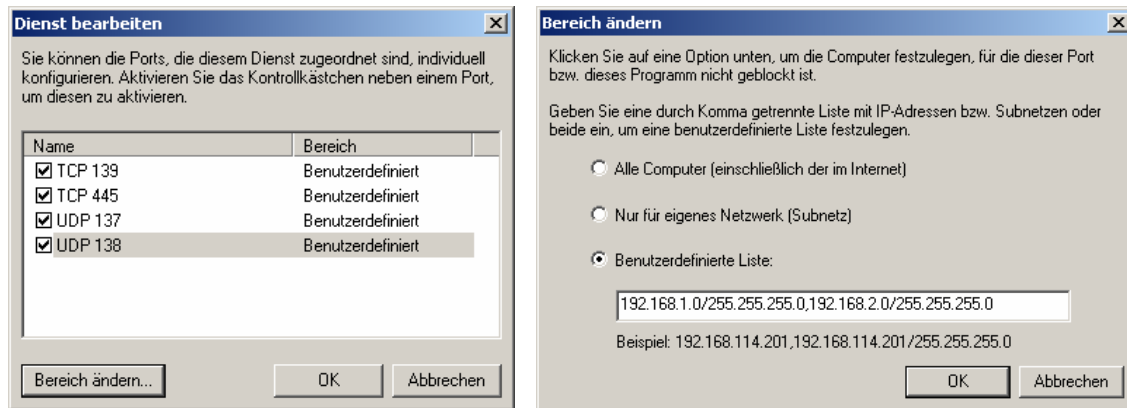
**Clientkonfiguration (für Win XP)**

In den Eigenschaften der Netzwerkkumgebung den „Assistent für Netzwerkverbindung ausführen“. Danach „Verbindung mit dem Netzwerk am Arbeitsplatz herstellen“ anklicken und VPN wählen. Verbindungsname definieren, keine Anfangsverbindung wählen und den DynDNS Namen oder die Feste IP eintragen. Benutzername und Kennwort eintragen. Nach dem Verbindungsaufbau über VPN lassen sich alle Ressourcen des Remote-Netzwerkes via IP ansprechen. Die Geschwindigkeit ist abhängig vom Upload des Host-Netzwerkes.

Ist auf dem Client PC die Windows XP Firewall aktiviert, so ist es standardmäßig nicht möglich, aus dem Remote-Netz auf eine Freigabe dieses PCs zuzugreifen (z. B. für Remotedrucken). Diese würde alle Anfragen, die sich nicht im Subnetz des einwählenden PCs befinden, blockieren. Daher muss erst eine Ausnahme in der Firewall definiert werden. Im nachfolgenden Beispiel liegt der Client PC im IP-Bereich 192.168.2.x und das Remote-Netzwerk in 192.168.1.x.

In den Firewall-Einstellungen unter Ausnahmen die Eigenschaften der „Datei- und Druckerfreigabe bearbeiten“ hier für alle Ports eine Benutzerdefinierte Liste mit dem eigenen bzw. dem Remote-Netzwerk definieren wie z. B.:

192.168.1.0/255.255.255.0, 192.168.2.0/255.255.255.0



## Router zu Router Kopplungen über IPSec

### Grundlagen zu IP Sec:

Es erfolgt zuerst die Authentifizierung beider Kommunikationspartner per vordefinierten Schlüssel (PSK - Pre Shared Key) oder via Zertifikat (X.509). Danach erfolgt die Verschlüsselungsvereinbarung über das IKE (Internet Key Exchange) Protokoll in zwei Phasen.

In Phase 1 wird eine „Security Association“ (Sicherheitsvereinbarung) ausgehandelt. Hierfür kommt der sogenannte „Main Mode“ oder „Aggressive Mode“ zum Einsatz. Dem „Main Mode“ liegt zugrunde, dass die IP Adresse des Absenders und des Adressaten bekannt ist. Bei dynamischen IP Adressen ist daher nur der etwas unsichere Aggressive Mode zu wählen. Die Sicherheit steigt mit der Länge des PSKs. Im Aggressive Mode dienen statt IP Adressen die „Local ID“ und „Peer ID“ als Identifizierungsmerkmal.

In Phase 2 wird die „Security Association“ mittels „Quick Mode“ erzeugt. Im Quick Mode wird ein Schlüssel vorgeschlagen und mit einem Hashwert (SHA1 oder MD5) übertragen.

Nach erfolgter Einigung wird die Verbindung aufgebaut und die Übertragung erfolgt verschlüsselt über das AH- (Authentication Header ) oder ESP-Protokoll (Encapsulating Security Payload). ESH ist die sicherere Verbindung. Als Verschlüsselungsform ist Triple DES (3DES) oder AES möglich. Zur Zeit gängig ist 3DES. Beide gelten derzeit als noch nicht geknackt.

### Einrichtung:

Will man zwei Standorte per IPSec über das Internet miteinander vernetzen, so ist dies ebenfalls mit einem LAN-zu-LAN Profil möglich. Auch die Subnetze müssen sich wieder unterscheiden, um Routing zu ermöglichen. Empfehlenswert sind 2 baugleiche Routermodelle, um Kompatibilitätsprobleme zu vermeiden. Um eine schnelle Lösung bei einem Routerausfall gewährleisten zu können, ist auch ein dritter Router sinnvoll, der vom Kunden aufbewahrt wird. Je nach Einsatzbereich müssen auf den Clients Gateways oder statische Routen eingetragen werden, dazu später mehr. Ein Router wird für die Verbindungsannahme konfiguriert, der andere baut die Verbindung zu ihm auf.

#### • *Verbindungsannahmeprofil konfigurieren.*

- VPN und externe Einwahl\LAN-zu-LAN ein Benutzerprofil wählen
- Name für das Profil vergeben z. B. „VPN\_in“ und Haken bei „Aktiv“ setzen
- Anrufrichtung auf „rein“ stellen und Leerlaufzeit auf „0“ stellen
- Den Punkt „2. Einstellungen zum Rauswählen“ kann man in diesem Fall übergehen

Profil Index : 1

1. Allgemeine Einstellungen

Profil Name <input type="text" value="VPN_in"/> <input checked="" type="checkbox"/> aktiv	Anrufrichtung: <input type="radio"/> Beide <input type="radio"/> Raus <input checked="" type="radio"/> Rein <input type="checkbox"/> Immer in Betrieb Max. Leerlaufzeit <input type="text" value="0"/> Sekunden <input type="checkbox"/> Dauer-Ping aktiv Ping an die IP-Adresse <input type="text"/>
VPN Verbindung durch: <input type="text" value="erstWAN1"/>	

- Einwahl zulassen über „IPsec Tunnel“ (alles andere abwählen)
- Haken bei „Definieren Sie ISDN CLID oder Remote Gateway-IP“ setzen:
  - Bei fester IP muss die Internet IP Adresse des entfernten Routers eingetragen werden
  - Bei dyn. IP muss die Peer ID eingetragen werden (die Peer ID bezeichnet das Kennwort für den Schlüsselaustausch)
- Danach einen Pre-Shared Key eintragen (wird zur Authentifizierung verwendet)
- IPSec Sicherheitsmethode auf „3DES“ einstellen (wird als Verschlüsselung während der Verbindung eingesetzt)

3. Einstellungen zum Einwählen

ISDN Number oder VPN Server IP-Adresse <b>Einwahl zulassen über</b> <input type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP mit IPsec <input type="text" value="nein"/>	Benutzername <input type="text"/> Passwort <input type="password"/> VJ Komprimierung <input checked="" type="radio"/> An <input checked="" type="radio"/> Aus
<input checked="" type="checkbox"/> Definieren Sie ISDN CLID oder Remote Gateway-IP IP-Adresse <input type="text" value="172.0.123.3"/> oder Peer ID <input type="text"/>	<b>IKE Authentifizierungsmethode</b> <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="password" value="....."/> <input type="checkbox"/> Digitale Signatur(X.509) <input type="text" value="nein"/>
	<b>IPSec Sicherheitsmethode</b> <input type="checkbox"/> Mittel (AH) Hoch (ESP) <input type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input type="checkbox"/> AES
	<b>Rückrufeinstellungen (CBCP)</b> <input type="checkbox"/> Rückruffunktion aktiv <input type="checkbox"/> Rückrufnummer festlegen Rückrufnummer <input type="text"/>

- Unter „4. TCP/IP Netzwerkeinstellungen“ die Netzwerkadresse des entfernten Netzwerks eintragen. WAN-IP und Remote Gateway IP können leer bleiben, sie werden beim Verbindungsaufbau vom Router automatisch ergänzt.

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

Meine WAN-IP	<input type="text" value="0.0.0.0"/>	RIP Richtung	<input type="text" value="inaktiv"/>
Remote Gateway-IP	<input type="text" value="0.0.0.0"/>	RIP Version	<input type="text" value="Ver. 2"/>
Remote Netzwerk-IP	<input type="text" value="192.168.1.0"/>	Im NAT-Betrieb, betrachte entfernte Subnetze als	<input type="text" value="private IP"/>
Remote Netzwerk-Maske	<input type="text" value="255.255.255.0"/>		
<input type="button" value="Mehr"/>		<input type="checkbox"/> Alle Anfragen ins Internet über diesen Tunnel	

#### • Verbindungsaufbauprofil konfigurieren

- VPN und externe Einwahl\LAN-zu-LAN ein Benutzerprofil wählen
- Name für das Profil vergeben z. B. „VPN\_out“ und Haken bei „Aktiv“ setzen
- Anrufrichtung auf „raus“ stellen und Leerlaufzeit auf „-1“ oder „immer in Betrieb“ stellen

#### Profil Index : 2

##### 1. Allgemeine Einstellungen

Profil Name	<input type="text" value="VPN_out"/>	Anrufrichtung:	<input type="radio"/> Beide <input checked="" type="radio"/> Raus <input type="radio"/> Rein
<input checked="" type="checkbox"/> aktiv		<input checked="" type="checkbox"/> Immer in Betrieb	
VPN Verbindung durch:	<input type="text" value="erst WAN1"/>	Max. Leerlaufzeit	<input type="text" value="-1"/> Sekunden
		<input type="checkbox"/> Dauer-Ping aktiv	
		Ping an die IP-Adresse	<input type="text"/>

- „IPSec Tunnel“ anwählen
- IP Adresse der Gegenstelle eintragen (bei dynamischen DNS die DynDNS Adresse)
- den PreShared Key identisch zur Gegenstelle eintragen
- „IPSec Sicherheitsmethode“ auf „Hoch“ stellen und „3DES mit Authentifizierung“ eintragen

##### 2. Einstellungen zum Rauswählen

<b>Verbindung zum VPN-Server über</b>	
<input type="radio"/> ISDN	Verbindung
<input type="radio"/> PPTP	Benutzername
<input checked="" type="radio"/> IPSec Tunnel	Passwort
<input type="radio"/> L2TP mit IPSec <input type="text" value="nein"/>	PPP Authentifizierung
ISDN-Nummer oder Server-IP/Host-Name für VPN. (z.B. 5551234, draytek.com or 123.45.67.89)	VJ Komprimierung
<input type="text" value="213.23.123.2"/>	<input checked="" type="radio"/> An <input type="radio"/> Aus
	<b>IKE Authentifizierungsmethode</b>
	<input checked="" type="radio"/> Pre-Shared Key
	IKE Pre-Shared Key <input type="text" value="....."/>
	<input type="radio"/> Digitale Signatur(X.509)
	<input type="text" value="nein"/>
	<b>IPSec Sicherheitsmethode</b>
	<input type="radio"/> Mittel(AH)
	<input checked="" type="radio"/> Hoch(ESP) <input type="text" value="3DES mit Authentifizierung"/>
	<input type="button" value="Erweitert"/>

- Danach auf „erweitert“ klicken. (bei IPSec Sicherheitsmethode)
- wird eine feste IP benutzt muss man den „Main Mode“ verwenden und bei IKE Phase 1 Proposal (Art des Hash Wertes für den Schlüsselaustausch) auf „DES\_MD5\_G1/DES\_SHA1\_G1/3DES\_MD5\_G1/3DES\_MD5\_G2“ stellen. Das Gerät verwendet dann die zur Gegenstelle kompatible Hashwert Methode.

#### IKE Erweiterte Einstellungen

IKE Phase 1 Modus	<input checked="" type="radio"/> Main mode	<input type="radio"/> Aggressive mode
IKE Phase 1 Proposal	DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2	
IKE Phase 2 Proposal	3DES_SHA1/DES_MD5	
IKE Phase 1 Key Lifetime	28800	(900 ~ 86400)
IKE Phase 2 Key Lifetime	3600	(600 ~ 86400)
Perfect Forward Secret (PFS)	<input checked="" type="radio"/> inaktiv	<input type="radio"/> aktiv
lokale ID		

- wird eine dynamische IP verwendet, muss in den „Aggressive Mode“ gewechselt werden, „Perfect Forward Secret“ auf aktiv setzen und ein Passwort bei „lokale ID“ für den Schlüsselaustausch adäquat zur „Peer ID“ eingetragen werden

#### IKE Erweiterte Einstellungen

IKE Phase 1 Modus	<input type="radio"/> Main mode	<input checked="" type="radio"/> Aggressive mode
IKE Phase 1 Proposal	DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_SHA1_G1	
IKE Phase 2 Proposal	3DES_SHA1/DES_MD5	
IKE Phase 1 Key Lifetime	28800	(900 ~ 86400)
IKE Phase 2 Key Lifetime	3600	(600 ~ 86400)
Perfect Forward Secret (PFS)	<input type="radio"/> inaktiv	<input checked="" type="radio"/> aktiv
lokale ID	passwort	

- Den Punkt „3. Einstellungen zum Einwählen“ kann man in diesem Fall übergehen
- Unter „4. TCP/IP Netzwerkeinstellungen“ die Netzwerkadresse des entfernten Netzwerk einzutragen. WAN-IP und Remote Gateway IP können leer bleiben, sie werden beim Verbindungsaufbau vom Router automatisch ergänzt.

#### 4. TCP/IP Netzwerkeinstellungen

Meine WAN-IP	0.0.0.0	RIP Richtung	inaktiv
Remote Gateway-IP	0.0.0.0	RIP Version	Ver. 2
Remote Netzwerk-IP	192.168.2.0	Im NAT-Betrieb, betrachte entfernte Subnetze als	private IP
Remote Netzwerk-Maske	255.255.255.0		
	Mehr		
		<input type="checkbox"/> Alle Anfragen ins Internet über diesen Tunnel leiten (Default Route)	

## Diagnosetools:

- Den generellen Status über die Einwahlmöglichkeiten (ISDN, DSL) findet man im Menü „Onlinestatus“

Systemstatus			Router aktiv seit: 97:2:33				
<b>LAN Status</b>		Primär DNS: 195.50.140.252		Sekundär DNS: 195.50.140.114			
IP-Adresse	TX Pakete	RX Pakete					
192.168.2.199	119528	210570					
<b>WAN 1 Status</b>							
Aktiv	Anschluss	Name	Modus	Verbindung aktiv seit			
Ja	Ethernet		---	00:00:00			
IP	GW IP	TX Pakete	TX Rate	RX Pakete	RX Rate		
---	---	0	0	0	0		
<b>WAN 2 Status</b>							
Aktiv	Anschluss	Name	Modus	Verbindung aktiv seit			
Nein	Ethernet		---	00:00:00			
IP	GW IP	TX Pakete	TX Rate	RX Pakete	RX Rate		
---	---	0	0	0	0		
<b>ISDN Status</b> >> <a href="#">Dial ISDN</a> >> <a href="#">B1 trennen</a> >> <a href="#">B2 trennen</a>							
Kanal	Aktive Verbindung	TX Pakete	TX Rate	RX Pakete	RX Rate	Verbindung aktiv seit	AOC
B1	Arcor [212.144.206.42]	174	4	166	4	0:8:53	0
B2	Idle [---]	0	0	0	0	0:0:0	0
D	UP						

- Den Status über VPN Verbindungen findet man über „VPN und externe Einwahl Verbindungsmanagement“

### VPN und externe Einwahl >> Verbindungsmanagement

Verbindung mit entferntem Netz herstellen Aktualisierungsintervall:  Aktualisieren

### VPN Verbindungs-Status

Aktuelle Seite: 1

Seite

VPN	Typ	Remote IP	virtuelles Netzwerk	Tx Pakete	Tx Rate	Rx Pakete	Rx Rate	Verbindung aktiv seit	
1 (sn)	PPTP/MPPE	84.56.90.97	192.168.1.42/32	1740	72	1201	16	0:15:43	<input type="button" value="Trennen"/>
2 (VPN_Out)	IPSec Tunnel 3DES-SHA1 Auth	212.144.206.42	192.168.2.0/24	0	0	1	3	0:0:12	<input type="button" value="Trennen"/>

xxxxxxx : Daten sind verschlüsselt.

xxxxxxx : Daten sind nicht verschlüsselt.

## Routing der Netzwerke konfigurieren

Damit die Netzwerkwerkkomponenten (PCs, Printserver, Access Points) zwischen beiden Netzen kommunizieren können muss jedem PC ein „Weg“ in das andere Netz definiert werden. Dies ist entweder über einen Gateway Eintrag möglich oder über das setzen von statischen Routen. Statische Routen haben Vorrang gegenüber den Gateway Einstellungen, daher erfolgt das Routing schneller.

Ist als Anforderung gegeben, dass einige PCs auf das Internet Zugriff haben sollen, empfiehlt sich der Einsatz eines separaten Routers um die Bandbreite für die VPN Verbindung nicht einzuschränken. Nachfolgend ein Beispielnetz skizziert:

