Vigor3100 Serie
Benutzerhandbuch

Version: 2.0

Datum: 2007/11/27

Dieses Produkt wurde entworfen und ist zertifiziert für die EG und Schweiz.

Inhaltsverzeichnis

1 Einleitung

Die Vigor3100 Serie stellt mit dem integrierten SDSL Modem eine außergewöhnliche Bandbreite für den Internetzugang zur Verfügung. So ist ein Down- und Uploadstream von je bis zu 2.3 Mbit/s (S-DSL) möglich, was jede Internetverbindung aufwertet – egal ob diese privat oder im Büro genutzt wird.

Die Sicherheit Ihres Netzwerks gewährt die Vigor3100-Serie durch eine integrierte Firewall mit erweiterten Funktionen, wie Stateful Packet Inspection (SPI) zum Erkennen und Verwerfen von bösartigen Datenpaketen, NAT mit Multi-VPN Pass-Through, konfigurierbarem Web-Filter zur elterlichen Kontrolle und zum Schutz vor dem Internet-Missbrauch, sowie viele weitere Funktionen.

Ihr Vigor 3100 ist mit 32 VPN Tunnel ausgestattet, auf die Sie auch alle Firewall Regeln einsetzen können. Die Hardeware basierte DES/3DES Engine, ermöglicht den verschlüsselten Aufbau von VPN Tunnel über das Internet, ohne Leistungsverluste, im Vergleich zur einer reinen Software Verschlüsselung.

1. Anschlüsse und Kontrolllampen (LED)

1.1.1 Vorderansicht des Vigor3100

LED		Status	Beschreibung
VPN		An	Eine VPN-Verbindung ist aktiv
QoS		An	Die QoS Funktion ist aktiv
		Aus	Die QoS Funktion ist deaktiviert
Printer		An	Die USB Schnittstelle ist aktiv
DSL		An	SDSL Leitung aktiv und verbunden
ACT (Activity)		An	Der Vigor ist angeschaltet
		Blinkend	Der Vigor ist angeschaltet und arbeitet normal
LAN (1, 2, 3, 4)	LNK	Nicht an	Eine 10Mbit/s ist an diesem Port installiert
		An	Eine 100Mbit/s ist an diesem Port installiert
		Blinkend	Ethernet Datenpakete werden transferiert
	FDX	Nicht an	Halb duplex Verbindung
		An	Full duplex Verbindung
		Blinkend	Paket Fehler / Kollision

Schnittstelle	Beschreibung
PWR	Anschluss für Kaltkabel 220V Anschluss (Rückseite)
ON/OFF	Schalter für die Stromversorgung (Rückseite)
RST Factory Reset	Auf Werkseinstellungen zurücksetzen. Anwendung: Vigor anschalten (ACT LED blinkt). Die versenkte Taste länger als fünf Sekunden drücken. Wenn die ACT LED beginnt schneller als normal zu blinken, kann die Taste losgelassen werden. Jetzt wird der Vigor mit den Werkseinstellungen neu gestartet.
DSL	Schnittstelle zum Internetzugang über die SDSL Leitung
LAN 4 – 1	Schnittstelle für lokale Netzwerkgeräte

1.2 Hardware Installation

Bevor Sie die Konfiguration des Vigors beginnen, überprüfen Sie bitte, ob alle Anschlüsse korrekt verbunden sind.

1.Verbinden Sie Ihren Router mit dem SDSL Anschluss Ihres Providers mit dem Netzkabel (RJ11 auf RJ-45 oder RJ 45 auf RJ 45). Für Deutschland benutzen Sie bitte das TAE auf RJ-45 Kabel. Schließen Sie den RJ-45 an den DSL-Port Ihres Routers.

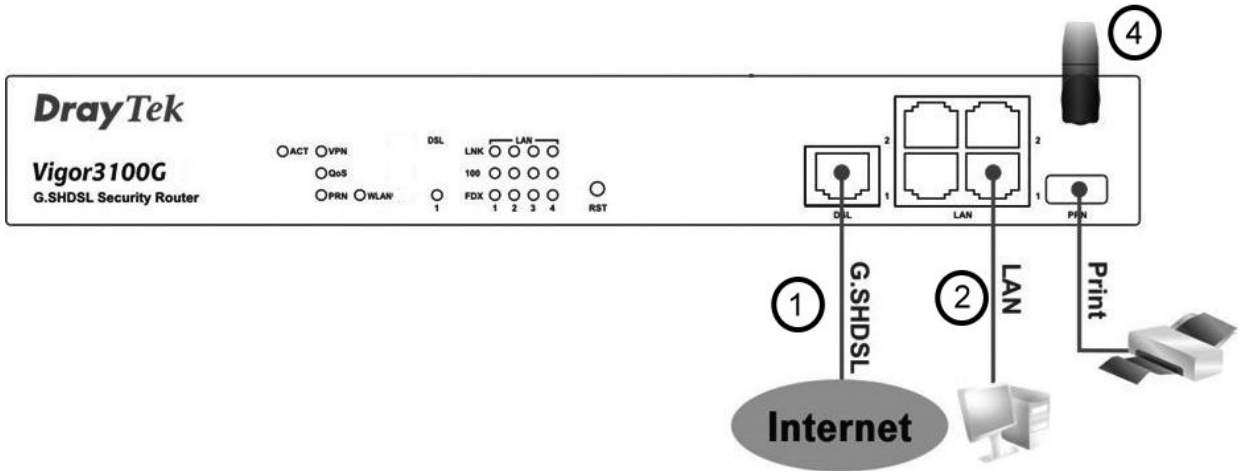
2.Verbinden Sie einen beliebigen LAN-Port (P1, P2, P3, P4) mit der Netzwerkkarte Ihres Computers. Verwenden Sie hierfür das blaue RJ45-Kabel. Sie können bis zu vier PCs direkt anschließen.

3.Versorgen Sie den Vigor mit Strom. Benutzen Sie den beiliegenden Stromanschluss Kabel..

4.Schalten Sie den Vigor an.

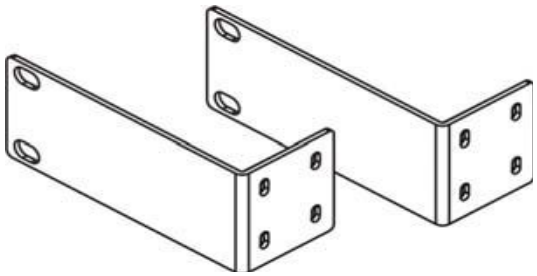
5.Prüfen Sie die **ACT** sowie die **LAN** LEDs, um sicher zu gehen, dass alle Netzwerkverbindungen korrekt angeschlossen sind.

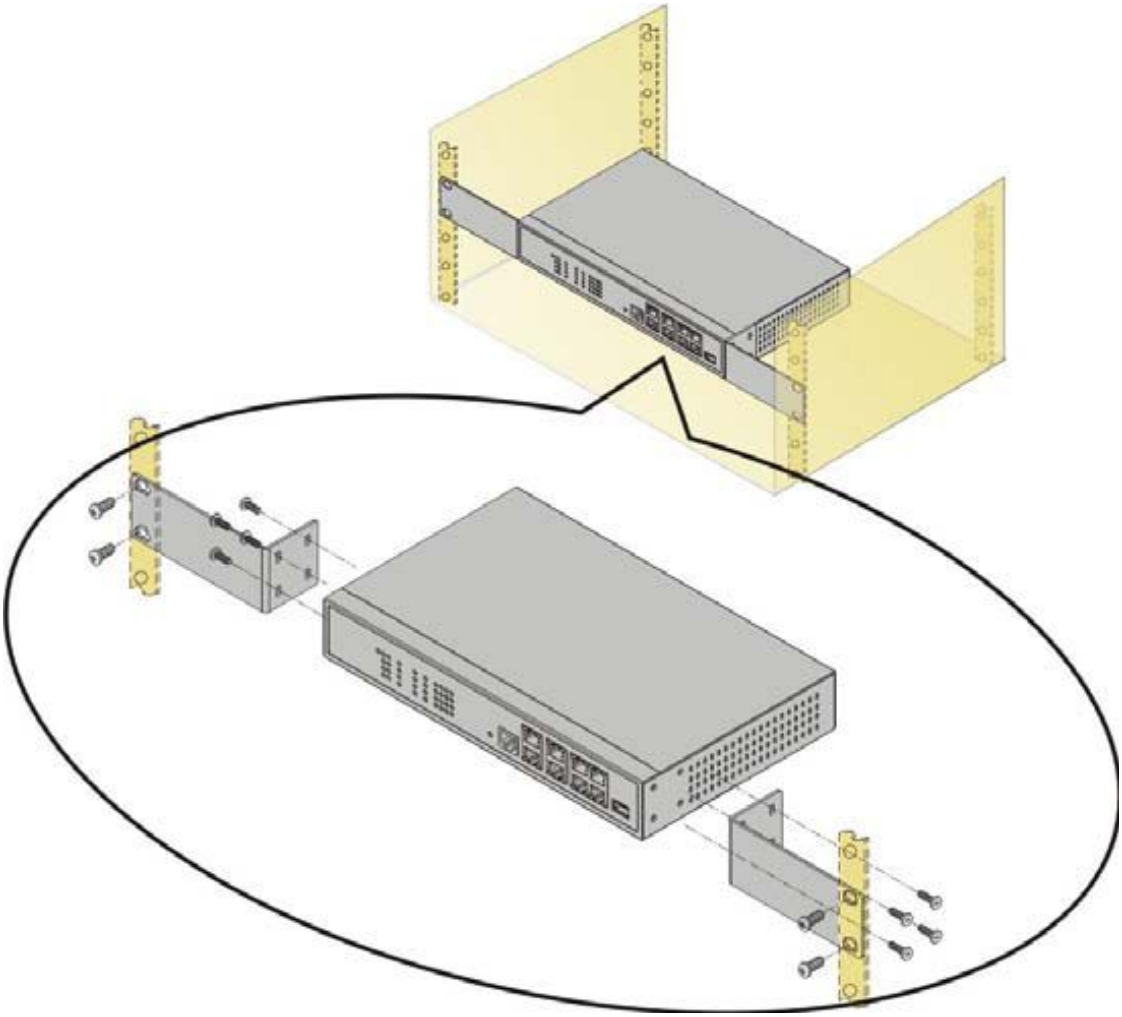
(Detaillierte Informationen zum LED Status finden Sie im Abschnitt 1.1.)



1.2.1 19“ Anschluss Mouting Kit

Ihr Vigor 3100 Router können Sie Problemlos in 19” Schränke montieren. Hierfür benutzen Sie bitte das mitgelieferte Zubehör.





2 Systemkonfiguration

Damit es einzig Ihnen obliegt, Konfigurationen an dem Vigor vorzunehmen, sollten Sie als erstes ein Zugangspasswort vergeben.

Diese Kapitel erklärt, wie das Administrator Passwort gesetzt wird und beschreibt die ersten Schritte zu einer erfolgreichen Einwahl ins Internet.

2.1 Ändern des Passworts

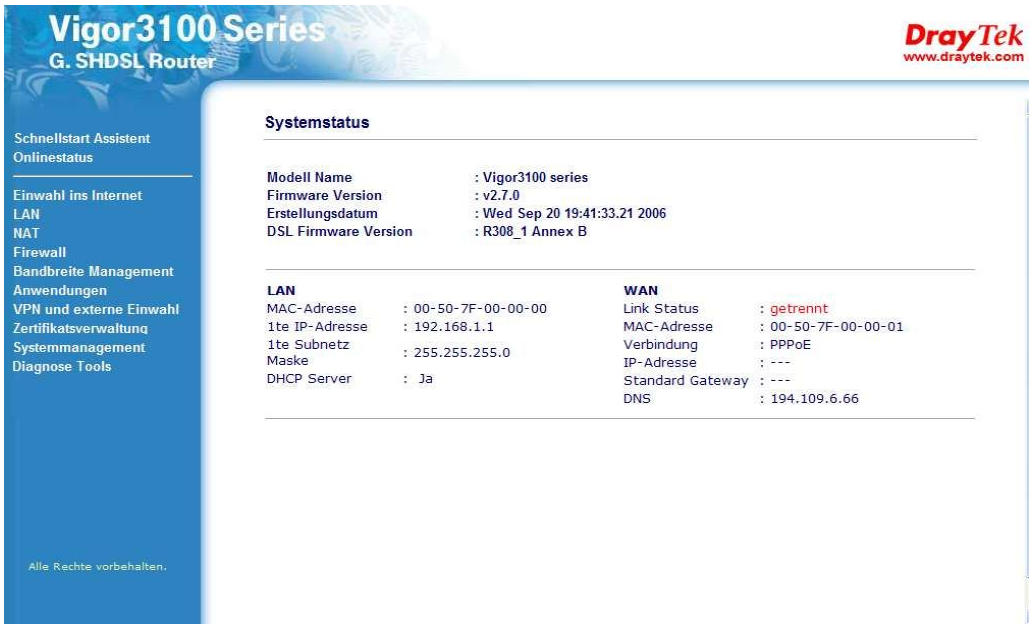
Um das Passwort Ihres Vigors zu ändern, müssen Sie zunächst auf die grafische Benutzeroberfläche.

1.Vergewissern Sie sich, dass Ihr Computer korrekt mit dem Vigor verbunden ist (siehe Abschnitt 1.2).

Hinweis: Ihr Computer sollte entweder die IP-Adresse automatisch beziehen (DHCP) oder Sie vergeben eine IP aus dem gleichen Adressbereich des Vigors. Die S**tandard-IP-Adresse des Vigors ist 192.168.1.1, ein Standard-Passwort exisistiert nicht**. Weitere Informationen finden Sie in dem Kapitel Problemlösungen.

2.Öffnen Sie einen Web-Browser auf Ihrem Computer (z.B. Internet Explorer oder Safari) und geben Sie in die Adresszeile **http://192.168.1.1** ein. Es erscheint ein Pop-Up Fenster und fordert die Eingabe eines Benutzernamen und Kennworts. Da ab Werk weder ein Benutzername noch ein Passwort vergebene wurde, bestätigen Sie die Abfrage mit **OK**.

3.Als nächstes Fenster wird das Hauptmenü der grafischen Benutzeroberfläche des Vigors erscheinen.



4.Navigieren Sie zum **Systemmanagement** und wählen Sie **Administrator Passwort**.

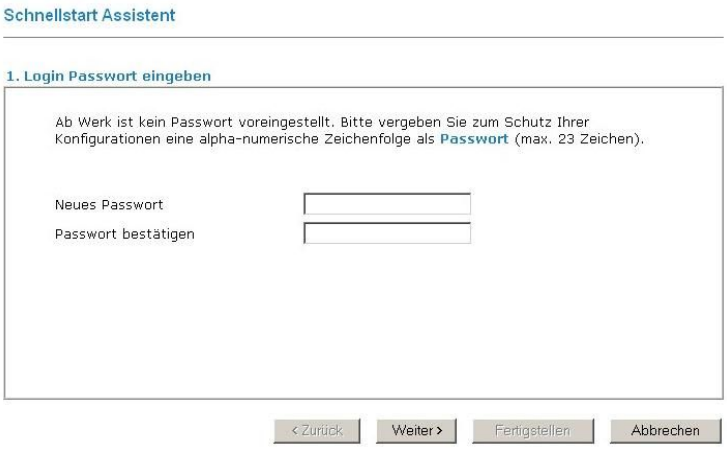
5.Geben Sie zunächst das aktuelle Passwort (ab Werk ist kein Passwort vorgegeben) in das Feld **Altes Passwort** ein. Vergeben Sie nun unter **Neues Passwort** sowie **Neues Passwort wiederholen** das Administrator Passwort. Bestätigen Sie mit **OK**.

6.Nun wurde das Passwort geändert. Somit sind nur noch Zugriffe mit diesem Passwort erlaubt. Daher müssen Sie sich erneut am Vigor anmelden – dieses Mal mit dem neuen Passwort.

2.2 Schnellstart Assistent

Der **Schnellstart Assistent** unterstützt Sie bei der Basiskonfiguration der relevanten Parameter für den Zugang ins Internet. Da ab Werk kein Zugangspasswort vergeben wurde, beginnt der Assistent mit der Aufforderung ein Passwort zu setzen. Das Passwort darf eine Folge von Zahlen und Buchstaben mit bis zu 23 Zeichen sein. Nachdem Sie ein Zugangspasswort eingegeben haben, klicken Sie bitte auf **Weiter**.

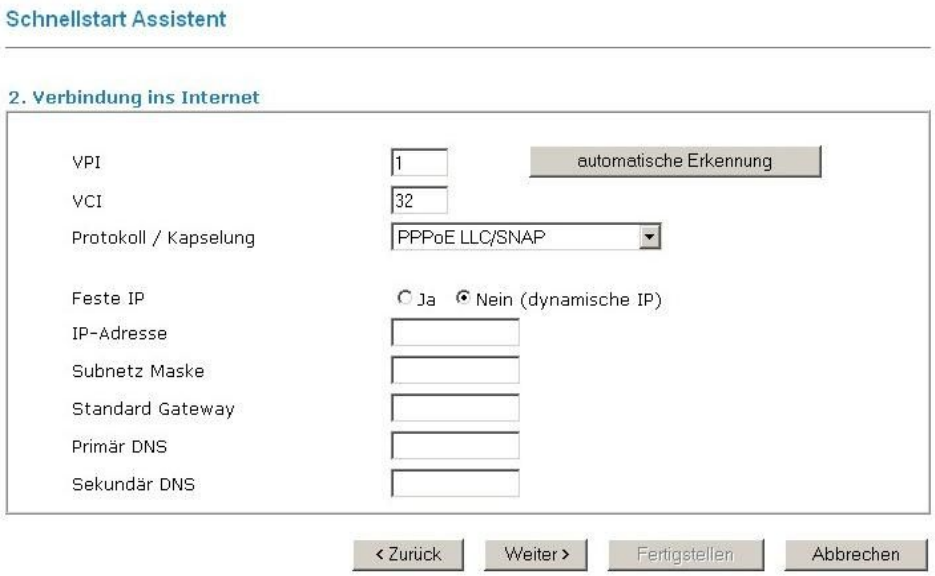
Haben Sie bereits wie in Abschnitt 2.1 erklärt ein Administrator Passwort gesetzt, so wird dieser Punkt beim Aufruf des **Schnellstart Assistent**en übersprungen.



2.2.1 Einstellen der Internetanbindung

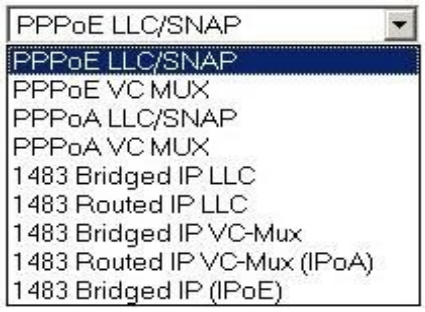
Für die Einwahl ins Internet können Sie zwischen verschiedenen Protokollen und Modi wählen: **PPPoE**, **PPPoA, Bridged IP oder Routed IP**.

In Deutschland wird die Einwahl zu einem ISP durch PPPoE geregelt. Die Internetanbindung in großen Teilen Österreichs und der Schweiz geschieht mittels PPPoA. Dies sind die "normalen" Betriebsarten. Business-Lösungen, wie die Verwendung einer festen IP-Adresse, benutzen Bridged IP bzw. Routed IP.



Zunächst müssen Sie Ihre entsprechende Art der Interneteinwahl wählen. Hier helfen die Daten, die Ihnen Ihr Internetanbieter (Internet Service Provider, ISP) zugesendet hat.

VPI	Der **Virtual Path Identifier** ist ein 8 bit großer Header einer ATM Zelle. Er gibt an, wie die Zelle geroutet werden soll. ATM ist eine weit verbreitete Methode zum Datentransfer. Die verwendeten Zellen sind immer gleich groß.
VCI	Der **Virtual Channel Identifier** ist ein 16 bit großes Feld einer ATM Zelle. Hier wird das nächste Ziel der Zelle angegeben. Ein virtueller Kanal (virtual Channel) ist eine logische Verbindung zwischen zwei Punkten eines Netzwerks. Ein virtueller Kanal bündelt mehrere virtuelle Pfade (virtual Path).
VPI und **VCI**	sind verantwortlich für die Wegewahl in Weitverkehrsnetzen.
Protokoll / Kapselung	Wählen Sie den IP Modus für die DSL Schnittstelle. Zur Auswahl stehen die Modi **PPPoE**, **PPPoA, Bridged IP** und **Routed IP**.



Vorteilhaft ist, dass sich die meisten deutschen ISPs, wie T-Online und Freenet, auf die Werte VPI=1, VCI=32 und Protokoll/Kapselung=PPPoE LLC/SNAP geeinigt haben. In Österreich hingegen dominieren für AnnexB Gebiete die Einstellungen VPI=8, VCI=48 und Protokoll/Kapselung=PPPoA VC MUX. Schweizer Vigor-Besitzer geben im Allgemeinen die Werte VPI=8, VCI=35 und Protokoll/Kapselung=PPPoE LLC/SNAP ein.[1]

Feste IP	Haben Sie von Ihrem ISP eine feste IP-Adresse erhalten, so klicken Sie auf **Ja** und definieren Sie folgend die relevanten Parameter. Anderenfalls klicken Sie auf **Nein (dynamische IP)**, um so eine IP dynamisch von Ihrem ISP zugewiesen zu bekommen. In diesem Fall entfällt auch die Eingabe der folgenden Parameter auf dieser Seite.
IP-Adresse	Geben Sie hier die feste IP an.
Subnetz Mask	Weisen Sie für **Routed IP** und **Bridged IP** eine Maske zu.
Standard Gateway	Weisen Sie für **Routed IP** und **Bridged IP** ein Gateway zu.
Primär DNS	Weisen Sie eine IP-Adresse für den primären DNS zu.
Sekundär DNS	Weisen Sie eine IP-Adresse für den sekundären DNS zu.

[1]Detaillierte Informationen zu den Einstellungen erhalten Sie von Ihrem Internetabieter (ISP). Angaben ohne Gewähr.

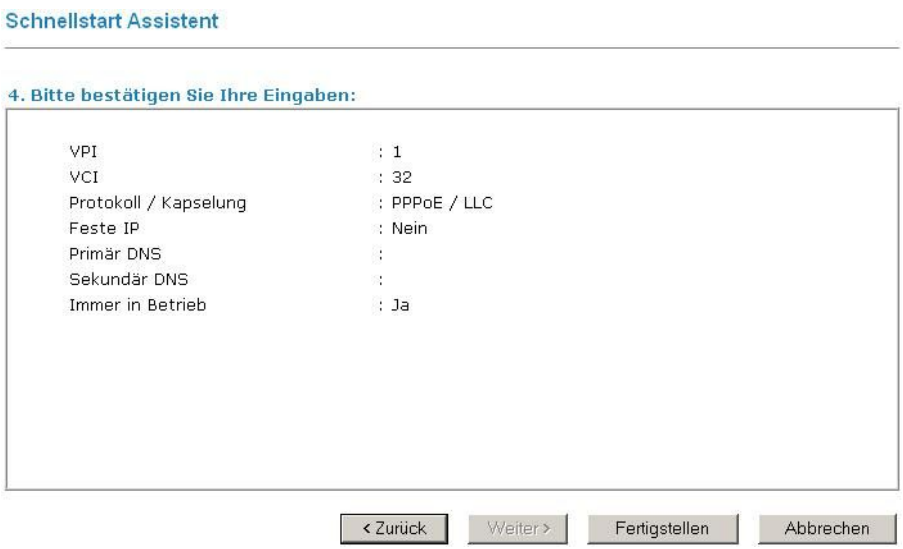
2.2.2 PPPoE/PPPoA

PPPoE (**Point-to-Point Protocol over Ethernet**) verbindet die User durch ein Ethernet mit dem Internet und verwendet hierfür eine Breitbandleitung, welche im Allgemeinen durch eine xDSL Leitung, ein Kabelmodem oder eine wireless Lösung bereitgestellt wird. Der Unterschied zu PPPoA (**Point-to-Point Protocol over ATM**) besteht darin, dass die Transportart nicht auf Ethernet sondern auf ATM basiert.

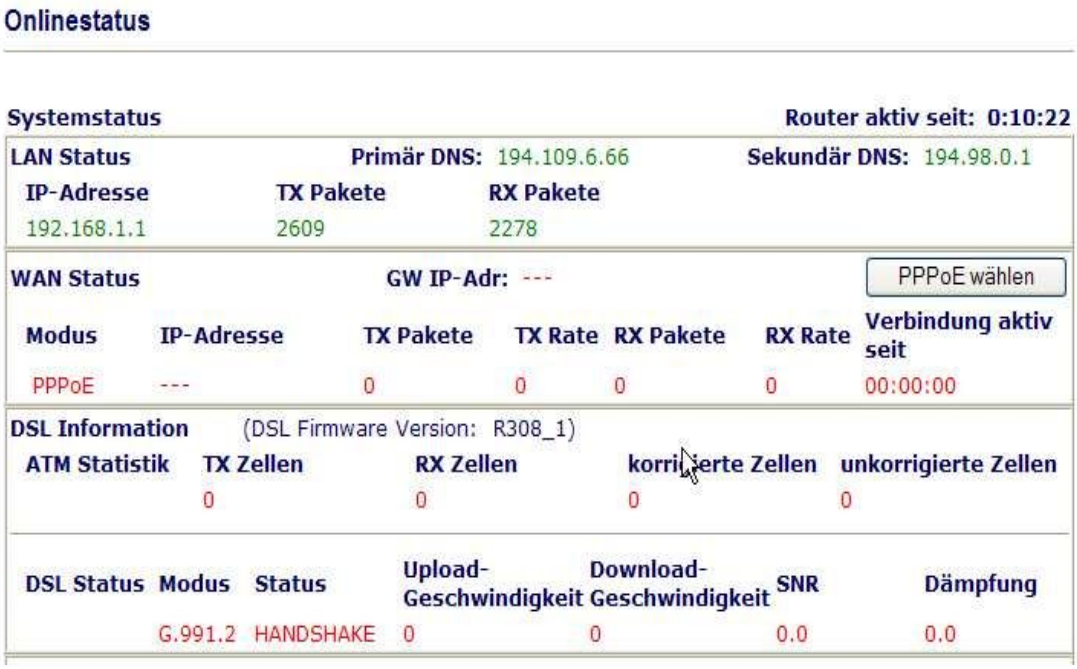
Die Einwahl über PPPoE/PPPoA mit einem vom Internet Anbieter bereitgestellten Benutzernamen und Passwort ist am weitesten verbreitet.

Name des Anbieters	Manche ISPs verlangen die Eingabe eines bestimmten Namens. Ansonsten kann er frei gewählt werden.
Benutzername	Geben Sie den Benutzernamen ein, welchen Sie von Ihrem ISP erhalten haben.
Passwort	Geben Sie das Passwort ein, welches Sie von Ihrem ISP erhalten haben.
Passwort bestätigen	Geben Sie das Passwort zur Bestätigung ein zweites Mal ein.
Immer in Betrieb	Aktivieren Sie diese Option, damit die Internetverbindung immer aktiv ist (dies empfiehlt sich besonders bei einer Flatrate).
Max. Leerlaufzeit	Definieren Sie die Dauer, wie lange die Internetverbindung noch gehalten werden soll, nachdem keine Anfragen aus dem Netzwerk mehr gestellt werden.

Klicken Sie **Weiter**, um zur Übersicht zu gelangen.

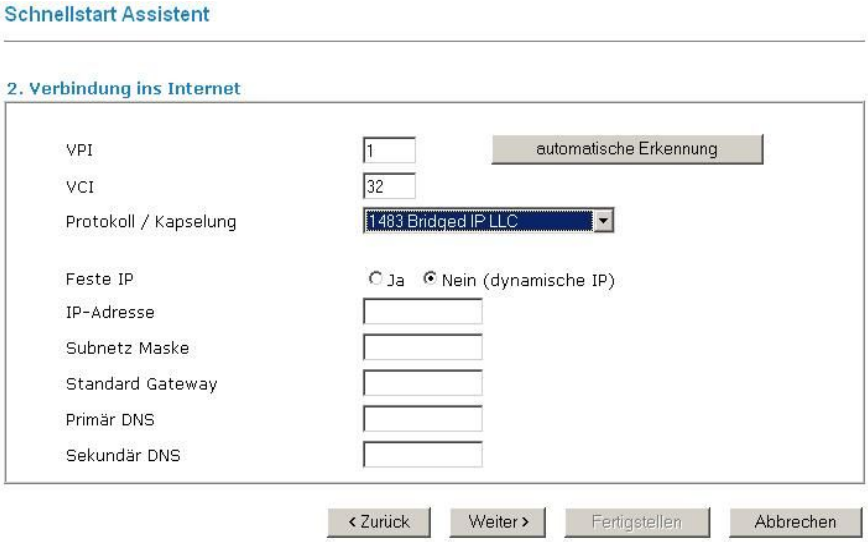


Klicken Sie auf **Fertigstellen.** Der Onlinestatus für PPPoE/PPPoA wird wie folgt angegeben:



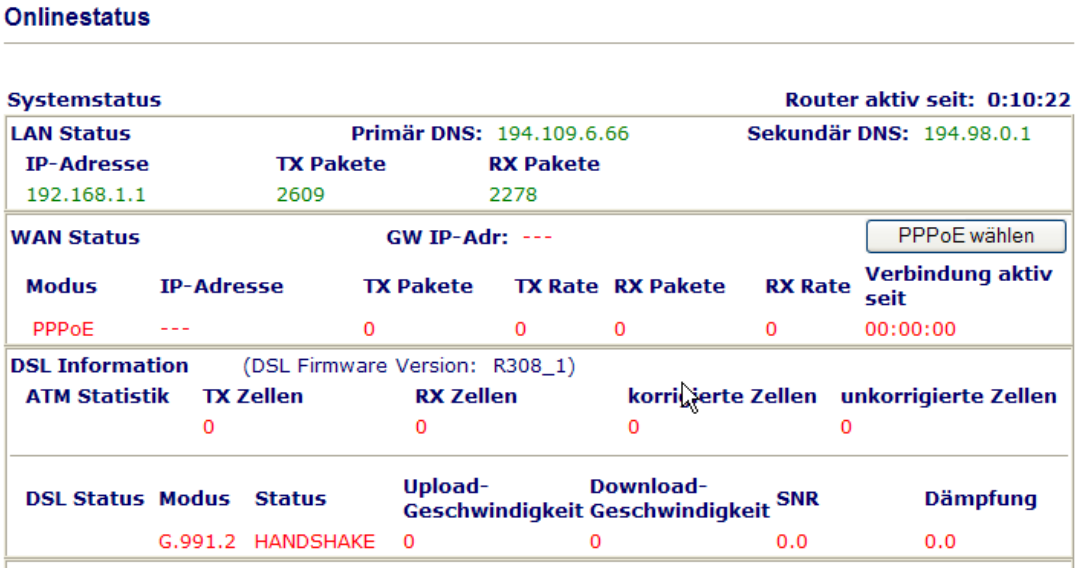
2.2.3 Bridged IP

Wählen Sie **1483 Bridged IP** als Protokoll, müssen Sie alle Parameter eingeben, die Ihnen Ihr ISP übermittelt hat.



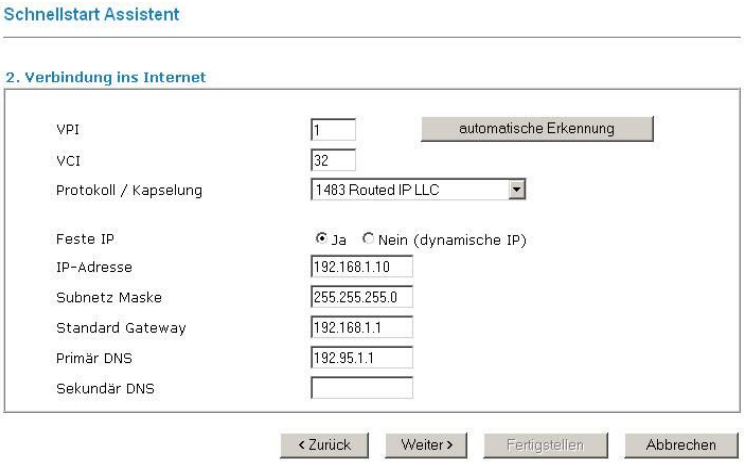
Nachdem Sie diese Seite konfiguriert haben, klicken Sie bitte **Weiter** und Sie erreichen die folgende Seite.

Klicken Sie auf **Fertigstellen.** Der Onlinestatus wird wie folgt angegeben:



2.2.4 Routed IP

Wählen Sie **1483 Routed IP** als Protokoll, müssen Sie alle Parameter eingeben, die Ihnen Ihr ISP übermittelt hat.



Nachdem Sie diese Seite konfiguriert haben, klicken Sie bitte **Weiter**.

Klicken Sie auf **Fertigstellen.** Der Onlinestatus wird wie folgt angegeben:

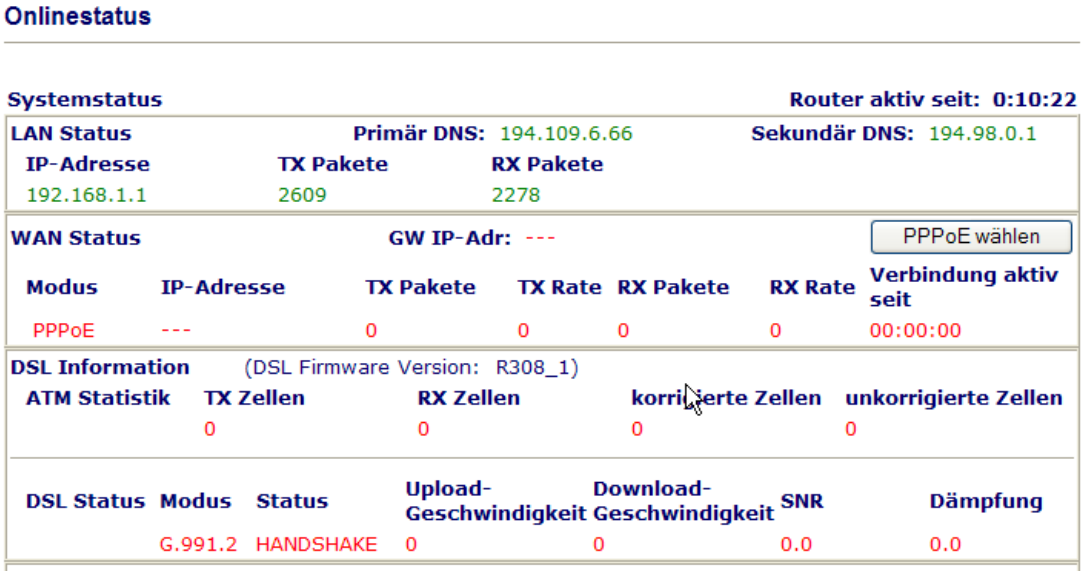
2.3 DSL Einstellungen

Nach Durchführung des Schnellstart Assistenten navigieren Sie zum Menü **Einwahl ins Internet** und wählen Sie **DSL Einstellungen** um die DSL Einstellungen gemäß Ihres Anschlusses zu konfigurieren. Bitte Wählen Sie unter Annex Typ (A oder B) den richtigen Modulationstyp aus. In Deutschland ist generell Typ B auszuwählen. Bei einer falschen Einstellung ist eine Verbindung zu Ihrem Provider nicht möglich.

2.4 Onlinestatus

Der Onlinestatus spiegelt Ihnen einen kompletten Status des Systems und zeigt im Speziellen die Zustände der vorhandenen Schnittstellen LAN, WAN und DSL auf einer Seite. Neben dem gänzlichen Überblick, können Sie auch – sofern PPPoE/PPPoA gewählt wurde – die Einwahl ins Internet manuell forcieren.

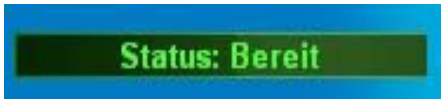
Onlinestatus von PPPoA/PPPoE



Primär DNS	Zeigt die zugewiesene IP-Adresse des primären DNS-Servers.
Sekundär DNS	Zeigt die zugewiesene IP-Adresse des sekundären DNS-Servers.
IP-Adresse (in LAN)	Zeigt die IP-Adresse der WAN Schnittstelle.
TX Pakete	Zeigt die Geschwindigkeit von versendeten Paketen am LAN.
RX Pakete	Zeigt die Geschwindigkeit von ankommenden Paketen am LAN.
GW IP-Adr:	Zeigt die zugewiesene IP-Adresse des Standard Gateways.
IP-Adresse (in WAN)	Zeigt die IP-Adresse der WAN Schnittstelle.
TX Rate	Zeigt die Geschwindigkeit von versendeten Paketen am WAN.
RX Rate	Zeigt die Geschwindigkeit von ankommenden Paketen am WAN.
Verbindung aktiv seit	Zeigt an, wie lange die Schnittstelle bereits aktiv ist.
TX Zellen	Zeigt die Anzahl aller versendeten ATM Zellen.
RX Zellen	Zeigt die Anzahl aller angekommenen ATM Zellen.
korrigierte Zellen	Zeigt die Anzahl aller angekommenen fehlerhaften ATM Zellen, welche korrigiert werden konnten.
unkorrigierte Zellen	Zeigt die Anzahl aller angekommenen fehlerhaften ATM Zellen, welche nicht korrigiert werden konnten.
Modus	Zeigt den verwendeten Modulations Modus.
Status	Zeigt den DSL Status an. Es wird zwischen den Status *Idle*, *Handshake*, *Training*, *Initialization* und *Showtime* unterschieden.
Upload-Geschw.	Zeigt die Upload-Geschwindigkeit (bits / Sekunde).
Download-Geschw.	Zeigt die Download-Geschwindigkeit (bits / Sekunde).
SNR	Zeigt den Wert des Signal-Rausch-Abstands (dB). Der Wert sollte über 7 liegen – je höher, desto besser ist die Signalqualität.
Dämpfung	Zeigt die Leitungsdämpfung – je niedriger der Wert, desto besser ist die Signalqualität.

2.5 Status Leiste

Jedes Mal, wenn Sie auf der grafischen Benutzerobefläche des Vigors zur Bestätigung von Konfigurationsänderungen **OK** drücken, benachrichtigt der Vigor Sie interaktiv.



Bereit gibt an, dass der Vigor bereit für weitere Eingaben ist.

Einstellungen gespeichert bedeutet, dass Ihre Einstellungen gespeichert wurden.

3 Erweiterte Einstellungen

Nachdem die Basiskonfiguration des Vigors abgeschlossen ist, haben Sie Zugang zum Internet. All diejenigen Benutzer, welche den Vigor auf die eigenen Bedürfnisse konfigurieren möchten, finden in diesem Kapitel eine Übersicht der Funktionalitäten.

3.1 Einwahl ins Internet

3.1.1 Grundlagen

Jedes Gerät in einem auf IP (Internet Protocol) basierenden Netzwerks wie Router, Print Server und Host PCs benötigen eine IP-Adresse, um in einem Netzwerk adressiert werden zu können. IP Konflikte, d.h. zwei IP-Geräte mit der selben Adresse, werden vermieden, da jede IP-Adresse durch die Netzwerkkarte im lokalen Netzwerk veröffentlicht wird. Die Einzigartigkeit einer IP-Adresse ist wichtig, weil nur so gewährleistet werden kann, dass Datenpakete an den richtigen Empfänger geleitet werden. Da die Adressen begrenzt sind, existieren für lokale, private Netzwerke (LAN) eigene IP-Adressen. Die so genannten privaten IP-Adressen werden niemals in öffentlichen Netzwerken wie das Internet verwendet und sind in folgenden Bereichen definiert:

von	**10.0.0.0**	**bis**	**10.255.255.255**
von	**172.16.0.0**	**bis**	**172.31.255.255**
von	**192.168.0.0**	**bis**	**192.168.255.255**

Was sind öffentliche und private IP-Adressen?

Neben der Verwaltung und dem Schutz des LANs verbindet der Vigor auch eine Gruppe von Hosts PCs. Im Allgemeinen, hat jeder von diesen eine eigene private IP-Adresse von dem integrierten DHCP Server zugewiesen bekommen. Der Router selbst hat auch eine private IP-Adresse in dem gleichen IP-Adressbereich, damit er mit den Host PCs kommunizieren kann. Ab Werk ist die private IP des Vigors 192.168.1.1.

Indessen kommuniziert der Vigor auch WANseitig durch seine öffentliche IP-Adresse mit anderem Netzwerkgeräten z.B. im Internet. Wenn der Datenfluss von WAN nach LAN –oder umgekehrt– durch den Vigor geht, übersetzt NAT (Network Address Translation) die öffentliche Adresse in eine private und leitet das Datenpaket an den entsprechenden Host weiter. Aus diesem Grund können alle Hosts sich eine einzelne Verbindung ins Internet teilen.

Eine öffentliche IP-Adresse bekommen

Damit Ihr Vigor eine öffentliche IP-Adresse von Ihrem ISP (Internet Service Provider) erlangt, gibt es drei Protokolle: PPPoE, PPPoA und MPoA. Multi-PVC unterstützt komplexere Konfigurationen als oben beschrieben.

SDSL benötigt PPP zum Authentifizieren und Autorisieren des CPEs (customer premises equipment) – z.B. der Vigor oder ein benutzereigenes Modem. PPPoE/PPPoA verbindet also Ihr privates Netzwerk über ein Modem mit dem Server Ihres ISPs. Dabei werden auch die Zugriffskontrolle, Fakturierung und der Diensttyp geregelt.

Wenn Ihr Vigor eine Verbindung zu de ISP aufbauen möchte, werden eine Reihe von Prozessen gestartet. Ihr Benutzername und Passwort werden mittels PAP oder CHAP an einem RADIUS authentifiziert. Anschließend erhalten Sie Ihre öffentliche IP-Adresse, DNS Server sowie andere relevanten Informationen und Parameter.

3.2 LAN

LAN (Local Area Network) ist eine Gruppe von Subnetzen, welche durch den Vigor geregelt werden.

3.2.1 Grundlagen

Der Vigor kommuniziert mit den Servern im Internet indem er seine öffentliche IP-Adresse (WAN IP) verwendet. Die Kommunikation mit den Computer im LAN, den sogenannten lokalen Hosts, geschieht über die private IP-Adresse (LAN IP) des Vigors. Die fundamentalste Funktion dabei ist NAT, was für Sie ein privates Netzwerk erschafft. NAT bildet hierfür die Datenpakete aus dem Internet an der WAN IP auf die LAN IP ab und leitet diese an die lokalen Hosts weiter – und umgekehrt. Des Weiteren verfügt der Vigor über einen integrierten DHCP Server, welcher lokalen Hosts automatisch IP-Adressen zuweist.

RIP (Routing Information Protocol)

Der Vigor tauscht mit Hilfe des RIPs Informationen zur Wegewahl (Routing) mit benachbarten Routern aus. Dies erlaubt Benutzern Parameter des Vigors wie die LAN IP-Adresse zu ändern. Der Vigor wird dann automatisch die Nachbarrouter informieren.

Feste Adressumleitung

Haben Sie mehrere Subnetze in Ihrem LAN, so ist gelegentlich die Verbindung derer untereinander zweckmäßiger und schneller durch die Verwendung einer Adressumleitung gewährleistet als durch andere Methoden. Hierzu muss einfach eine entsprechende Regel definiert werden, welche Daten von einem spezifische Subnetz in ein anderes weiterleitet. Es wird kein RIP benötigt.

Virtuelle LANs

Lokale Hosts können in bis zu vier portbasierende virtuelle LANs (VLAN) gruppiert werden. Konfigurieren Sie die physikalischen Ports und die Bandbreite nach Ihrem Ermessen.


Internet
VLAN1
VLAN0
192.168.1.13
192.168.1.12
192.168.1.11
192.168.1.10

3.3 NAT

Üblicherweise arbeitet der Vigor als ein NAT (Network Address Translation) Router. NAT ist ein Mechanismus, um private IP-Adressen auf eine öffentliche abzubilden. Die öffentliche IP-Adresse erhalten Sie von Ihrem ISP und müssen im Allgemeinen dafür bezahlen. Private IP-Adressen sind kostenlos, eine Kommunikation ins Internet ist aber nicht möglich. Die Vorteile von NAT sind:

●**Kosten sparen**
NAT erlaubt mehreren Hosts im LAN mit verschiedenen privaten IP-Adressen, die eine öffentliche IP zu verwenden, welche in Vertretung für die privaten Anfragen ins Internet leitet.

●**Hohe Sicherheit** Die NAT Funktion schützt das interne Netzwerk vor Angriffen, welche gegen IP-Adressen gerichtet sind. Der Angreifer kennt die IP-Adresse des Hosts im LAN nicht, da diese durch NAT verschleiert wird.

3.3.1 Portumleitung

Die Portumleitungstabelle wird gewöhnlich benutzt, um Zugriff auf LANseitige Dienste wie E-Mail-, Web- und FTP-Server aus dem Internet zu erlangen.

Service Name	Vergeben Sie dem Eintrag eine Bezeichnung.
Protokoll	Wählen Sie ein Protokoll (TCP oder UDP) aus der Transport Schicht.
öffentlicher Port	Definieren Sie, welcher Port an die folgend eingetragene interne IP und Port umgeleitet werden soll.
private IP	Definieren Sie die IP-Adresse des internen Hosts, welcher den Dienst auf dem öffentlichen Port annehmen soll.
privater Port	Definieren Sie den Port, an welchem der Dienst von dem internen Hosts angenommen werden soll.
Aktiv	Aktivieren Sie den Eintrag.

3.3.2 DMZ Host

Im Gegensatz zur Portumleitung, bei welcher nur ein Port des eingehenden Datenverkehrs zu einem Host im LAN umadressiert wurde, wird bei der DMZ Host Funktion der komplette eingehende Datenverkehr an eine IP-Adresse unangetastet an diese weitergegeben. Damit ist es auch Protokollen, welche auf keinem festen Port arbeiten (z.B. ESP und AH), möglich, von außen mit diesem Port auf den gewählten Host im LAN zuzugreifen. Hierdurch wird der gewählte Host ungeschützt ins Internet gestellt, was meist bei der Verwendung von Anwendungen wie Netmeeting oder Online Spielen hilfreich ist. Hierdurch werden die Aktivitäten der anderen Hosts im LAN nicht beeinträchtigt.

aktiv	Aktivieren Sie die DMZ Funktion.
private IP	Definieren Sie die IP-Adresse eines Hosts im LAN, welcher in die DMZ gestellt werden soll. Alternativ wählen Sie ***PC wählen***.
PC wählen	Klicken Sie diesen Button und wählen Sie eine IP-Adresse in dem neu erscheinenden Fenster. Im Fenster finden Sie eine Liste aller IPs des lokalen Netzwerks. Die gewählte IP-Adresse wird als DMZ-Host

in die Funktion eingefügt.

3.3.3 Offene Ports

Einstellungen offener Ports erlaubt Ihnen ganze Portbereiche für Anwendungen wie P2P Applikationen, Internet Kamera usw. zu öffnen. Informieren Sie sich bezüglich der Anwendung und den zu öffnenden Ports, um nicht Opfer eines Angriffs zu werden. Der Vigor bietet Ihnen die Möglichkeit zehn Profile für verschiedene lokale IP-Adressen mit jeweils zehn Portbereichen zu öffnen. Sie können also insgesamt 100 Portbereiche öffnen.

Klicken Sie in der Übersichtstabelle auf einen Index, um ein Profil zu editieren.

aktiv	Aktivieren Sie dieses Profil.
Bezeichnung	Vergeben Sie einen Profil-Namen.
lokaler Computer	Definieren Sie die IP-Adresse eines Hosts im LAN oder klicken Sie auf den ***PC wählen***-Button.
PC wählen	Klicken Sie diesen Button und wählen Sie eine IP-Adresse in dem neu erscheinenden Fenster. Im Fenster finden Sie eine Liste aller IPs des lokalen Netzwerks.
Protokoll	Wählen Sie das Transportprotokoll zwischen ***TCP***, ***UDP*** und **-**(kein).
Start-Port	Definieren Sie den ersten Port des Dienstes, welcher direkt an den lokalen Host geleitet wird.
End-Port	Definieren Sie den letzten Port des Dienstes, welcher direkt an den lokalen Host geleitet wird.

3.3.4 Liste gebräuchlicher Ports

Diese Seite zeigt Ihnen eine Übersicht über die Standard-Ports und deren Transportprotokoll.

3.4 Firewall

3.4.1 Grundlagen

Während die Benutzer im LAN immer mehr Bandbreite für multimediale interaktive Anwendungen fordert, sollte dennoch auf die Sicherheit ein großer Wert gelegten. Die Firewall hilft, Ihr Netzwerk vor Angriffe von unautorisierten Außenstehenden zu verhindern. Sie kann weiterhin den Zugang zum Internet für manche Benutzer oder Anwendungen einschränken oder unterbinden. Selbstverständlich könne Sie auch verhindern, dass Programme ungewollt auf das Internet zugreift.

Neben den Firewall Regeln ist die größte Grundsicherheit die Vergabe eines Passworts. Denn sobald ein Angreifer auf Ihren Vigor Zugriff hat, kann er alle Konfigurationen ändern! Vergeben Sie daher immer ein Administrator Passwort.

3.4.2 Basiskonfiguration

Anruf-Filter	Aktivieren Sie die Anruf-Filter Funktion und weisen Sie einen Start Filter zu, mit dessen Regeln der Verbindungsaufbau ins WAN bzw. Internet eingeschränkt werden.
Daten-Filter	Aktivieren Sie die Daten-Filter Funktion und weisen Sie einen Start Filter zu, mit dessen Regeln das LAN vor Angriffen von außen geschützt wird.
Log Flag	Zur Fehleranalyse ist eine Übersicht der Filterfunktion hilfreich. **Aus** – Die Log Funktion ist inaktiv. **Alle durchgelassenen Pakete** – Alle Pakete, die aufgrund einer Filterregel durchgelassen wurde, werden geloggt. **Alle blockierten Pakete** – Alle Pakete, die durch eine Filterregel verworfen wurde, werden geloggt. **Alle Pakete ohne Übereinstimmung** – Alle Pakete, auf die keine Filterregel angewendet wurde, werden geloggt. Beachte Sie, dass das Log nur über Telnet mit dem Befehl ***log –f*** eingesehen werden kann.
Stateful Packet Inspection (SPI) aktiv	SPI ist eine zustandsgesteuerte Filterung, welche sich den Zustand einer Verbindung merkt und dadurch neue Datenpakete logisch einer Verbindung zuordnen kann. Ein einfacher Paketfilter dagegen muss jedes neue Datenpaket komplett analysieren. Aktivieren Sie diese Funktion, um SPI zu nutzen.
Filter auf alle eingehenden VPN ...	Aktivieren Sie diese Funktion, um die definierten Filterregeln auch auf VPN Verbindungen anzuwenden.
Trenne Verbindungen auf TCP-Port 80 ...	Aktivieren Sie diese Funktion, um den TCP-Port 80 für http zu reservieren und somit keinen andere Diensten den Zugriff hierauf zu gewähren.
Fragmentierte UDP-Pakete akzeptieren	Einige Online Spiele (z.B. Half Life) bzw. Sprach- oder Videotransmissionen verwenden für die Datenüberragung große Mengen von unfragmentierten UDP Paketen. Da dies auch eine bekannte Angriffsmethode ist, betrachtet der Vigor diese Pakete generell als Sicherheitsrisiko und verwirft sie. Aktivieren Sie diese Funktion, um angesprochenen Anwendungen benutzen zu können.

3.4.3 Filtereinstellungen

Die IP Filter bestehen aus 12 Filter-Sätzen mit jeweils 7 Filterregeln, welche chronologisch abgearbeitet werden. Um eine Filteregel zu ändern oder zu generieren, klicken Sie zunächst auf einen Filter-Satz.

Filteregel	Klicke Sie auf eine Filterregel (1-7), um diese i einem neuen Fenster zu editieren.
Aktiv	Aktivieren Sie die Filterregel.
Beschreibung	Vergeben Sie einen bis zu 23 Zeichen langen Namen für den Satz.
Nächster Filter Satz	Verlinken Sie diesen Filter-Satz zu einem weiteren. Nachdem alle Regeln dieses Filter-Satzes abgearbeitet wurden, werden die Filterregeln des nächsten bearbeitet. Beachten Sie keine Schleifen zu bilden!

Um nun eine Filteregel zu ändern oder zu generieren, klicken Sie auf einen Filterregel-Button.

Bezeichnung	Vergeben Sie einen bis zu 14 Zeichen langen Namen für die Regel.
Filterregel aktiv	Aktivieren Sie die Filterregel.
Durchlassen oder Blockieren	Definieren Sie die einzutreffende Aktion, wenn die Regel greift. **sofort durchlassen** – Pakete, auf die diese Regel zutreffen, werden durchgelassen. **sofort blockieren** – Pakete, auf die diese Regel zutreffen, werden verworfen. **durchlassen, falls keine weitere Übereinstimmung** – Pakete, auf die diese Regel und keine weiteren Regeln zutreffen, werden durchgelassen. **blockieren, falls keine weitere Übereinstimmung** – Pakete, auf die diese Regel und keine weiteren Regeln zutreffen, werden verworfen.
Weiterleiten an Filter-Satz	Pakete, auf die diese Regel zutreffen, werden an einen anderen Filter-Satz weitergeleitet. Wählen Sie den nächsten Filter-Satz aus der Liste.
Log	Aktivieren Sie die Funktion, um diese Regel zu loggen. Beachte Sie, dass das Log nur über Telnet mit dem Befehl ***log –f*** eingesehen werden kann.
Richtung	Definieren Sie die Richtung des Paketflusses und wähle Sie zwischen eingehendem und ausgehendem Datenverkehr. Diese Funktion kann nur auf Daten-Filter angewendet werden, da bei Anruf-Filtern der Datenverkehr immer Raus, also ins WAN bzw. Internet, geht.
Protokoll	Definieren Sie das Protokoll bzw. die Protokolle, auf welche diese Filterregel angewendet werden soll.
IP-Adresse	Definieren Sie die IP-Adressen von Quelle und Ziel, auf welche diese Filterregel angewendet werden soll. Beachten Sie hierbei die definierte Richtung. Stellen Sie das ***!***-Zeichen vor die IP-Adresse, so wird diese Regel nicht auf die IP-Adresse angewendet. Lassen Sie das Feld frei oder geben Sie ***any*** ein, so wird die Regel auf alle IP-Adressen angewendet.

Subnetz Maske	Wählen Sie die zu der IP-Adresse zugehörige Maske.
Operator, Start-Port und End-Port	Die Operator Spalte bezieht sich auf die Port Einstellungen. Ist der Start-Port leer, wird auch der End-Port ignoriert. Es werden alle angegebenen Ports gefiltert. ***(=)*** Ist der End-Port leer, wird die Regel nur auf den Start-Port angewendet. Wurden Start- und End-Port definiert, so wird die Regel auf den angegebenen Bereich inklusive Start- und End-Port angewendet. ***(!=)*** Ist der End-Port leer, wird die Regel auf alle Ports mit Ausnahme des Start-Ports angewendet. Wurden Start- und End-Port definiert, so wird die Regel auf alle Ports mit Ausnahme des angegebenen Bereichs inklusive Start- und End-Port angewendet. ***(>)*** Die Regel wird auf alle Ports größer gleich des Start-Ports angewendet. ***(<)*** Die Regel wird auf alle Ports kleiner gleich des Start-Ports angewendet.
Zustand bewahren	Diese Funktion nutzt die Parameter aus Richtung, Protokoll, IP-Adresse, Subnetz Maske und den Port Einstellungen und kann nur auf Daten-Filter angewendet werden. Diese Funktion ist SPI. Sie verfolgt Datenströme und akzeptiert nur Pakete, deren Zustand eindeutig als gültig definiert wurde. Die Gültigkeit kann aufgrund eines Vergleichs der oben genannten Parametern mit denen im Paket selbst hinterlegten Werten bestimmt werden. Nicht angeforderte Pakete werden verworfen.
Regel bezieht sich auf	Diese Funktion wird nur auf Daten-Filter angewendet. Wählen Sie zwischen ***alle Datenpakete***, ***alle nicht fragmentierten Datenpakete***, ***alle fragmentierten Datenpakete*** und ***alle Fragmente ohne Header*** auf welche Pakete die Regel angewendet werde soll.

3. IM Filter

Wählen Sie aus einer Liste welche Instant Messenger blockiert werden sollen. Verwenden Sie den Verbindungstimer, um eine zeitgesteuerte Restriktion der Funktion zu generieren. Abschließend aktivieren Sie die Funktion und klicken Sie **OK**.

3.4.5 P2P Filter

Wählen Sie aus einer Liste welche Peer-zu-Peer Verbindungen verweigert bzw. zugelassen werden sollen. Verwenden Sie den Verbindungstimer, um eine zeitgesteuerte Restriktion der Funktion zu generieren. Abschließend aktivieren Sie die Funktion und klicken Sie **OK**.

3.4.6 DoS Abwehr

Wählen Sie aus 15 vorgefertigten Filterregeln, welche den gängigsten Angriffsarten begegnen. Ab Werk ist die DoS Abwehr inaktiv. Aktivieren Sie DoS und wählen Sie die gewünschten Abwehrmechanismen. Klicken Sie abschließend auf **OK**.

3.4.7 Inhaltsbezogener URL-Filter

aktiv	Aktivieren Sie die Einstellungen auf dieser Seite.
Schwarze Liste	Wählen Sie diese Option, um den Zugriff auf die entsprechende Webseite mit einem der gelisteten Schlüsselworte zu verbieten.
Weiße Liste	Wählen Sie diese Option, um den Zugriff nur auf die Webseiten mit einem der gelisteten Schlüsselworte in der URL zu erlauben.
Schlüsselwort	Basierend auf den eingetragenen Begriffen untersucht der Vigor den die URL jeder ausgehenden *http* Anfrage. Unabhängig ob das Wort nur einen Teil der URL ausmacht, wird entsprechend der **Schwarzen** bzw. **Weißen Liste** gehandelt. Der Vigor bietet acht Felder für die Eingabe mehrerer Schlüssel-worte, welche durch Leerzeichen, Komma oder Semikolon getrennt sein müssen. In jedes Feld können bis zu 32 Zeichen eingegeben werden. Das Schlüsselwort darf ein Wort, ein Wortteil oder eine komplette URL sein. Beachten Sie, dass durch eine komplexe Liste die Performanz leiden kann.
Seitenaufrufe durch Eingabe der IP ...	Aktivieren Sie diese Funktion, damit der URL-Filter nicht durch die Eingabe der Ziel IP-Adresse umgangen werden kann. Löschen Sie aus diesem Grund auch den Cache Ihres Browsers.
Eingeschränkte Web-Features aktiv	Aktivieren Sie diese Funktion und wählen Sie anschließend die zu blockenden Merkmale. ***Java*** – Der Vigor schaltet die Internet Java Objekte aus. ***ActiveX*** – Alle ActiveX Objekte aus dem Internet werden geblockt. ***ZIP Dateien*** – Der Vigor blockiert alle komprimierte Dateien mit den Erweiterung **zip**, **rar**, **.arj**, **.ace**, **.cab** und **.sit**. ***EXE Dateien*** – Der Vigor blockiert die Erweiterungen **.exe**, **.com**, **.scr**, **.pif**, **.bas**, **.bat**, **.inf** und **.reg**. ***Cookie*** – Filtert Cookies ins WAN und schützt Ihre Privatsphäre. ***Proxy*** – Verwirft jegliche Proxy Übetragung. ***Multimedia Dateien*** – Blockiert den Download der Erweiterungen **.mov**, **.mp3**, **.rm**, **.ra**, **.au**, **.wmv**, **.wav**, **.asf**, **.mpg**, **.mpeg**, **.avi** und **.ram**, um limitierte Bandbreite zu schützen.
Ausnahmebestimmungen für folgende ...	Four entries are available for users to specify some specific IP addresses or subnets so that they can be free from the *URL Access Control*. To enable an entry, click on the empty checkbox, named as **ACT**, in front of the appropriate entry.
Verbindungstimer	Setzen Sie Timer, um die Einstellungen zeitlich zu beschränken.

3.4.8 Inhaltsbezogener Web-Filter

Diese Funktion bietet DrayTek in Kooperation mit SurfControl an. SurfControl ist ein Unternehmen, welches Webseiten im Internet kategorisiert. Detaillierte Informationen erhalten Sie auf der Hompage von SurfControl.

Testen Sie die Funktion für 30 Tage kostenlos oder werden Sie Kunde bei SurfControl.

Wählen Sie danach aus der Liste welche Themenbereiche blockiert werden sollen. Verwenden Sie den Verbindungstimer, um eine zeitgesteuerte Restriktion der Funktion zu generieren. Abschließend aktivieren Sie die Funktion und klicken Sie **OK**.

3.5 Anwendungen

3.5.1 Dynamisches DNS

Aktivieren Sie zunächst die DynDNS Einstellungen und klicken Sie anschließend auf einen Index, um das registrierte Konto eines DDNS Providers auf den Vigor anzuwenden.

aktiv	Aktivieren Sie dieses DDNS Profil.
Anbieter	Wählen Sie den Provider des registrierten DDNS Kontos.
Servicetyp	Wählen Sie zwischen dynamisch, benutzerdefiniert und statisch
Domain Name	Geben Sie die zugewiesene Domain an.
Login Name	Geben Sie den zugewiesenen Login Namen an.
Passwort	Geben Sie das zugewiesene Passwort an**.**

Wildcard und **Backup MX** werden nicht von jedem DDNS Provider angeboten. Detaillierte Informationen hierzu finden Sie auf deren Webseiten.

Klicken Sie abschließend auf **OK**, um die Konfiguration zu übernehmen.

3.5.2 Verbindungstimer

Der Vigor verfügt über eine Systemzeit, welche es erlaubt zeitkritische Funktionen auszuführen. Die Systemzeit kann manuell oder automatisch mittels NTP (Network Time Protocol) aktualisiert unter ***Systemmanagement >> Zeit und Datum*** werden.

Sie können insgesamt 15 Timer definieren und diese dann in den verschiedenen Funktionen wie Interneteinwahl und VPN Verbindungen verwenden. Klicken Sie auf einen Index, um den Timer zu konfigurieren.

aktiv	Aktivieren Sie diesen Timer.
Anfangsdatum	Definieren Sie das Datum, ab wann der Timer aktiv ist.
Startzeit (hh:mm)	Definieren Sie Startzeit, ab wann dieser Timer gültig ist.
Dauer (hh:mm)	Definieren Sie, wie lange der Timer gültig sein soll.
Aktion	Definieren Sie, was während der gültigen Zeit geschehen soll: **Verbindung aufbauen** – Die Verbindung ist immer aktiv . **Verbindung beenden** – Die Verbindung ist immer getrennt. **Einwahl zulassen** – Eine Verbindung darf aufgebaut werden. Definieren Sie zusätzlich die ***max. Leerlaufzeit***. **Einwahl unterbinden** – Die Verbindung bleibt nach der Trennung inaktiv.
max. Leerlaufzeit	Ist die Verbindung für die angegebene Zeitspanne unproduktiv, so wird diese getrennt.
Wiederholungen	Definieren Sie wie oft der Timer angewendet werden soll: **einmalig** – Der Timer ist nur einmal gültig. **wochentags** – Wählen Sie an welchen Tagen der Timer gültig ist.

3.5.3 RADIUS

RADIUS (Remote Authentication Dial-In User Service) ist ein Client/Server Sicherheits-protokoll. Der integrierte RADIUS Client ermöglicht dem Vigor externe Benutzer, WLAN Clients und dem RADIUS Server mit einer gegenseitigen Authentifizierung zu unterstützen.

aktiv	Aktivieren Sie das RADIUS Client Feature.
Server IP-Adresse	Geben Sie die IP-Adresse des RADIUS Servers an.
Ziel-Port	Geben Sie den UDP Port des RADIUS Servers an. Nach RFC 2138 ist der Standardwert 1812.
Shared Secret	RADIUS Server und Client teilen sich ein geheimes Passwort, welches zum Authentifizieren der gesendeten Nachrichten verwendet wird. Beide Seiten müssen das Passwort selbe Passwort nutzen.
Shared Secret wiederholen	Wiederholen Sie die Eingabe.

3.5.4 UPnP

Das UPnP (Universal Plug and Play) Protokoll bringt den über ein Netzwerk verbundenen Geräten die gleichen Annehmlichkeiten, wie es bei lokal angeschlossenen Windows 'Plug and Play'-Peripheriegeräten bereits bekannt ist. Für NAT Router ist das Hauptmerkmal von UPnP die Unterstützung von **NAT Traversal**. Dies ermöglicht Anwendungen Ports zu öffnen, damit diese den Router passieren können. Es bringt die Vorteile, dass der Router nicht selbst erarbeiten muss, welche Anwendung welchen Port benötigt und auch der Benutzer dies nicht manuell konfigurieren muss. UPnP ab **Windows XP** verfügbar.

3.5.5 QoS

Mit QoS (Quality of Service) können Sie Bandbreite für Anwendungen garantieren.

aktiv	Aktivieren Sie die QoS Funktion.
Richtung	Definieren Sie auf welchen Datenverkehr die Regeln angewendet werden sollen. **Rein –** nur auf eingehenden Verkehr. **Raus** – nur auf ausgehenden Verkehr. **Beide** – ein- und ausgehender Verkehr.
Index	Es existieren vier Gruppen.
Gruppenname	Definieren Sie einen Namen für die Gruppe.
Reservierte Bandbreite	Geben Sie das Verhältnis an. Es beinhaltet die reservierte Bandbreite für Up- und Downstream Geschwindigkeit.
Einstellungen	Es gibt zwei Level der Einstellung: **Einfach** – Weisen Sie der reservierten Bandbreite Servicetypen zu. Hierfür steht Ihnen eine Liste der gebräuchlichen Service-typen zur Verfügung. **Erweitert –** Weisen Sie der reservierten Bandbreite benutzerdefinierte Servicetypen zu. Konfigurieren Sie die IP-Adressen für Quelle und Ziel, den DiffServ CodePoint und eigene Servicetypen.
UDP Bandbreite begrenzen	Diese Option dient zum Schutz der TCP Verbindungen. Aktivieren und begrenzen Sie die Bandbreite für breitband-intensive UDP Anwendungen.

Maximale Bandbreite für UDP Geben Sie hier die maximale Bandbreite für UDP an.

3.6 VPN und externe Einwahl

Ein Virtual Private Network (VPN) ist die Erweiterung eines privaten Netzwerks über ein öffentliches Netzwerk hinweg. Oder anders: Verwenden Sie die VPN Technologie, so können Sie Daten zwischen zwei Computern (VPN Peer) durch das Internet versenden und genießen dabei die Vorteile einer privaten Punkt-zu-Punkt Verbindung.

3.6.1 Einwahlmöglichkeiten

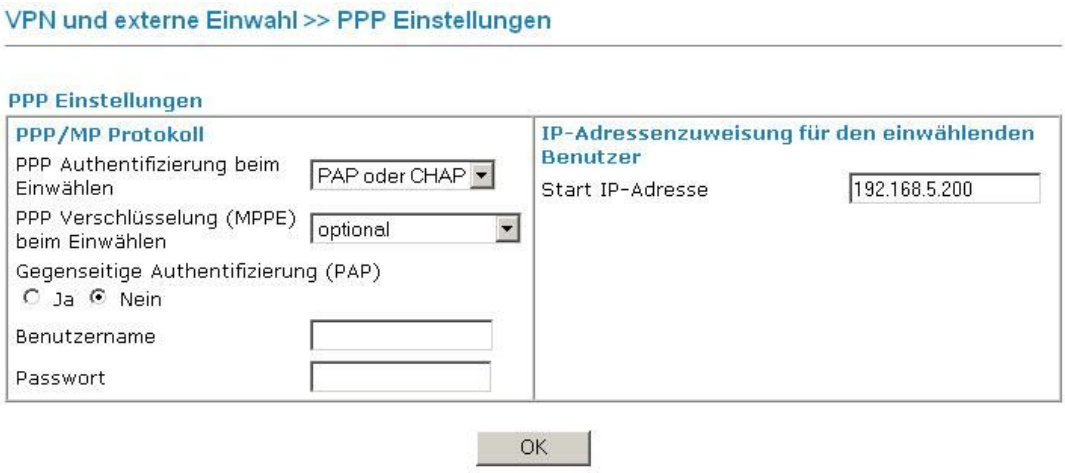
Aktivieren Sie hier die gewünschten VPN Dienste.

Falls in dem LAN des Vigors ein VPN Server aktiv ist, so muss der entsprechende Dienst im Vigor deaktiviert werden, da ansonsten der Vigor den Einwahlversuch bedient. Hierdurch wird ein Pass Through, also eine Weiterleitung in das LAN, des entsprechenden Dienstes ermöglicht. Außerdem sollten die relevanten NAT Einstellungen (u.a DMZ, Offene Ports) überprüft werden.

PPTP	Aktivieren Sie den PPTP Dienst, um die VPN Einwahl mit dem PPTP Protokoll zu erlauben.
IPSec	Aktivieren Sie den IPSec Dienst, um die VPN Einwahl mit dem IPSec Protokoll zu erlauben.
L2TP	Aktivieren Sie den L2TP Dienst, um die VPN Einwahl mit dem L2TP Protokoll zu erlauben.

3.6.2 PPP Einstellungen

Diese Untermenü behandelt nur PPP-bezogene VPN Verbindungen über PPTP, L2TP oder L2TP over IPSec. Die Einstellungen gelten global.



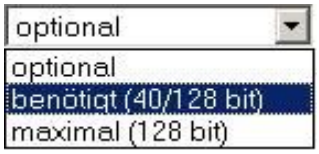
PPP Authentifizierung beim Einwählen

nur PAP – Wählen Sie diese Option, damit der Vigor die Authentifizierung des Einwählenden mittels PAP durchführt.

PAP oder CHAP – der Vigor versucht zunächst die Authentizität mittels CHAP herzustellen. Falls dies von der einwählenden Seite nicht unterstützt wird, so fällt der Vigor automatisch auf PAP zurück.

PPP Verschlüsselung (MPPE) beim Einwählen

optional – Wurde diese Option gewählt, so wird die Verschlüsselung der Daten durch MPPE abhängig von der einwählenden Seite. Falls die Gegenseite MPPE nicht unterstützt, so wird auf eine Verschlüsselung hierdurch verzichtet.



benötigt (40/128 bit) – Ist diese Option aktiv, so wird eine Verschlüsselung der Daten mittels MPPE durch den Vigor gefordert. Allerdings richtet es sich nach der Gegenseite, ob die 128 bit oder nur die 40 bit Verschlüsselung verwendet wird. Der Vigor fragt zunächst die höher verschlüsselte Methode ab.

maximal (128 bit) – Hier lässt der Vigor die Verbindung nur zu, wenn die einwählende Seite die MPPE Verschlüsselung mit 128 bit unterstützt.

Gegenseitige Authentifizierung (PAP)

Von einigen Routern oder Clients wird für einen Verbindungsaufbau eine bidirektionale Authentifizierung verlangt, um so die Sicherheit zu erhöhen. Verlangt die Gegenstelle eine solche gegenseitige Authentifizierung, so kann diese hier aktiviert werden und ein Benutzername sowie Passwort hinterlegt werden.

Start IP-Adresse

Die Start IP-Adresse gibt den Beginn des IP-Adressbereichs an, welcher den einwählende PPP Verbindungen vergeben wird. Daher ist es zwingend, dass eine IP-Adresse aus dem lokalen IP-Bereich angegeben wird.

3.6.3 IPSec Grundeinstellungen

In den **IPSec Grundeinstellungen** gibt es zwei Konfigurationsbereiche, welche sich auf die zwei Phasen bei IPSec beziehen:

➢**Phase 1** handelt die Authentizität sowie die Internet-Key-Exchange (IKE) Parameter aus. In letzteren werden Verbindungseinstellungen wie Verschlüsselung, Diffie-Hellman Parameter, Hash-Wert und eine Lifetime zum Schutz der IKE Verbindung festgehalten. Die Stelle, von der aus der Verbindungsaufbau initiiert wird, übermittelt ihre IKE Parameter an den VPN-Peer. Dieser sucht dann die Übereinstimmungen mit der höchsten Priorität heraus. Es werden in vier Nachrichten Schlüsselmaterialien ausgetauscht, um am Ende eine symmetrische Schlüssel-ID zu generieren. Aus dieser wird je ein Schlüssel zur Authentifizierung, für die anschließende Phase 2 und zur Verschlüsselung der folgenden IKE-Nachrichten abgeleitet. In den zwei folgenden, nun verschlüsselten, Nachrichten werden mittels Pre-shared Key (PSK) die VPN-Teilnehmer authentifiziert. Dabei kann der PSK als ein Passwort betrachtet werden, welches auf beiden Seiten gleich sein muss. Alternativ zum PSK kann auch durch eine digitale Signatur (X.509) authentifiziert werden. Schlussendlich ist ein sicherer Tunnel für Phase 2 hergestellt.

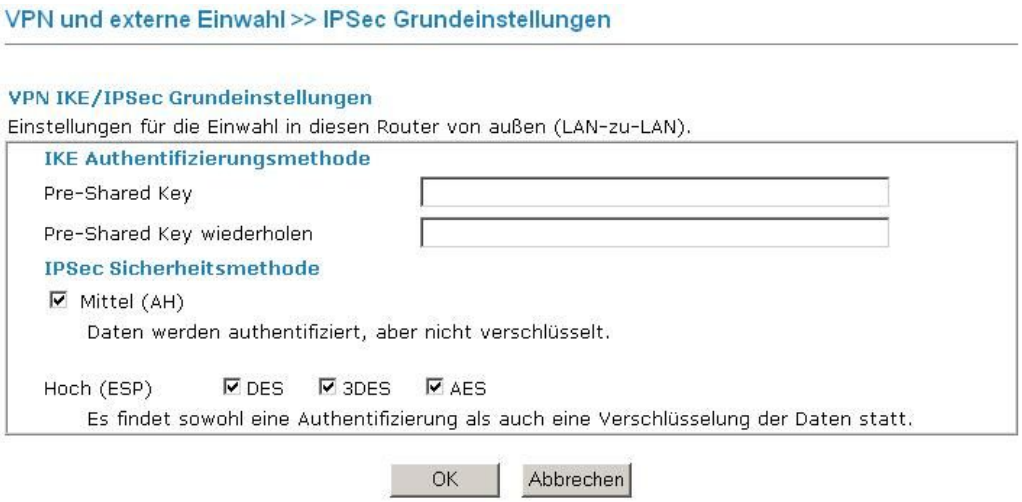
➢**Phase 2** handelt den symmetrischen Schlüssel sowie die Security Associations (SA) für die IPSec Verbindung aus. Die SAs beinhalten Sicherheitsmethoden wie Authentication Header (AH) oder Encapsulating Security Payload (ESP). Haben sich die VPN-Teilnehmer einigen können, steht der IPSec Tunnel.

Mit **AH** werden nur Echtheit und Integrität der Daten sichergestellt. Dies wird durch einen HMAC, welcher auf jedes versendete Paket angewandt wird, realisiert. Ein HMAC wird aus einer Hash-Funktion abgeleitet und beugt der Manipulation vor. Die Gegenseite ist ebenfalls in dem Besitz des HMACs und kann die Pakete wieder dekodieren. Im Gegensatz zu AH sorgt sich **ESP** auch um die Vertraulichkeit der Verbindung und verschlüsselt die Daten. Auch vor Manipulationen schützt ESP; allerdings ist der Schutz der Integrität nicht so hoch wie bei AH, da durch HMAC nicht die IP-Adresse in die Berechnung einfließt. Ein IP-Spoofing kann dennoch ausgeschlossen werden, da die VPN-Teilnehmer zu diesem Zeitpunkt bereits authentifiziert wurden.

Symmetrische Schlüssel verleihen AH und ESP ihre kryptografischen Funktionen. Damit diese nicht bereits im Voraus ausgetauscht werden müssen, handelt das IKE Protokoll den symmetrischen Schlüssel bereits beim Verbindungsaufbau dynamisch aus.

IPSec verwendet zwei Arten der Kapselung von Datenpakete – den Transport und den Tunnel Modus. Im **Transport Modus** werden die Nutzdaten (Payload) durch AH/ESP verschlüsselt, aber der original IP-Header bleibt erhalten. Daher kann es nur für lokale Pakete verwendet werden, z.B. L2TP over IPSec. Beim **Tunnel Modus** kapselt IPSec das komplette Datenpaket inklusive IP-Header und erzeugt einen neuen IP-Header. Dadurch ist die original IP-Adresse erst bei der Entschlüsselung auf der Gegenseite wieder sichtbar.

Werden entfernte Subnetze über ein unsicheres öffentliches Netzwerk miteinander gekoppelt, so sollte auf die Kombination ESP und Tunnel Modus zurückgegriffen werden. AH wird dagegen für die VPN-Verbindung innerhalb eines privaten lokalen Netzwerks empfohlen.



IKE Authentifizierungsmethode Üblicherweise verwenden VPN-Peers mit dynamischen IP-Adressen, wie Teleworker, welche die Einwahl mittels IPSec bzw. L2TP over IPSec.
Pre-Shared Key – Definieren Sie einen Schlüssel für die IKE Authentifizierung.
Pre-Shared Key wiederholen – Bestätigen Sie Ihre Eingabe.

IPSec Sicherheitsmethode **Mittel** – Der Authentication Header (AH) authentifiziert die Daten, verschlüsselt diese aber nicht. Diese Option ist mit den Werkseinstellungen aktiv.
Hoch – Das Encapsulating Security Payload (ESP) umschließt die Nutzdaten und verschlüsselt diese. Als Verschlüsselungs-Algorithmus können Data Encryption Standard (DES), Triple DES (3DES) und Advance Encryption Standard (AES) gewählt werden. Der Nachfolger des Verschlüsselungs-Standards um DES ist AES. 3DES gilt zwar noch immer als sicher, benötigt aber aufgrund der Dreifachverschlüsselung mehr Rechenleistung.

3.6.4 IPSec Identität

Um ditale Zertifikate zur Authentifizierung der VPN-Teilnehmern (Peer) für entweder LAN-zu-LAN Verbindungen oder VPN-Verbindungen externer Benutzer (Teleworker) zu verwenden, sollte an dieser Stelle eine Auswahl an Peer Zertifikaten in die Tabelle eingetragen werden. Es können bis zu 32 digitale Zertifikate generiert und gespeichert werden.

Auf Werkseinstellungen ... Löscht alle Profile.

Index Klicken Sie auf einen der Indezies, um die IPSec Identität zu konfigurieren.

Name Gibt die Bezeichnung des Profils an.

Weiter Klicken Sie hier, um weitere Profile angezeigt zu bekommen.

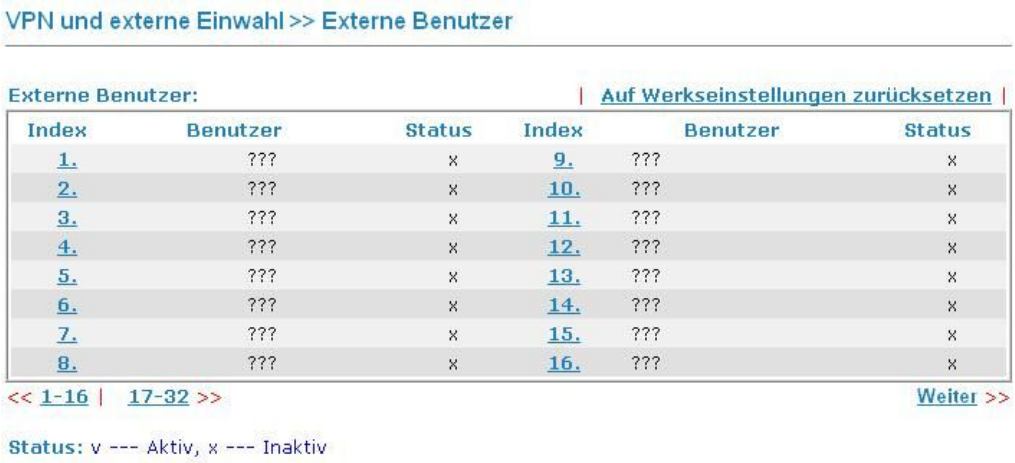
Jeder Index steht für ein Profil eines digitalen Zertifikats und kann mit einem Klick auf den Index editiert werden. Es gibt drei Sicherheitslevel für die Authentifizierung einer digitalen Signatur. Für eine korrekte Authentifizierung eines Peers müssen die relevanten Felder ausgefüllt werden:

Profil Name	Vergeben Sie eine Bezeichnung für dieses Profil.
Akzeptiere jede ID	Klicken Sie, um jeden Peer – unabhängig seiner Identität – zu akzeptieren.
Akzeptiere Subjekt mit übereinstimmenden Namen/Wert	Wählen Sie ein spezifisches Merkmal einer digitalen Signatur, um die Gegenstelle mit einer entsprechenden Übereinstimmung zu akzeptieren. Das Merkmal kann **IP-Adresse, Domain Name** oder **E-Mail** sein. Abhängig von Ihrer Wahl wird ein zusätzliches Feld erscheinen und weitere Angaben fordern.
Akzeptiere Subjekt mit Übereinstimmung in gewissen Feldern	Wählen Sie diesen Sicherheitslevel, um konkrete Merkmale einer digitalen Signatur einzutragen. Der Peer, welcher in allen angegebenen Merkmalen eine Übereinstimmung aufzeigen kann, wird der Zugang gewährt. Die Kürzel in den Klammern leiten sich aus den original Ausdrücken ab: **Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN)** und **Email (E)**.

3.6.5 Externe Benutzer

Um die Einwahl verschiedener externer Benutzer/Teleworker verwalten zu können, müssen für diese Benutzerprofile angelegt werden. Es müssen abhängig von der Art der gewünschten Verbindung entsprechende Angaben zu den IKE Parameter sowie SAs hinterlegt werden.

Der Vigor unterstützt 32 Teleworker-Profile. Außerdem können die Profile unter Verwendung des integrierten RADIUS Clients an einen RADIUS Server ausgeweitet werden.



Auf Werkseinstellungen ... Löscht alle Profile.

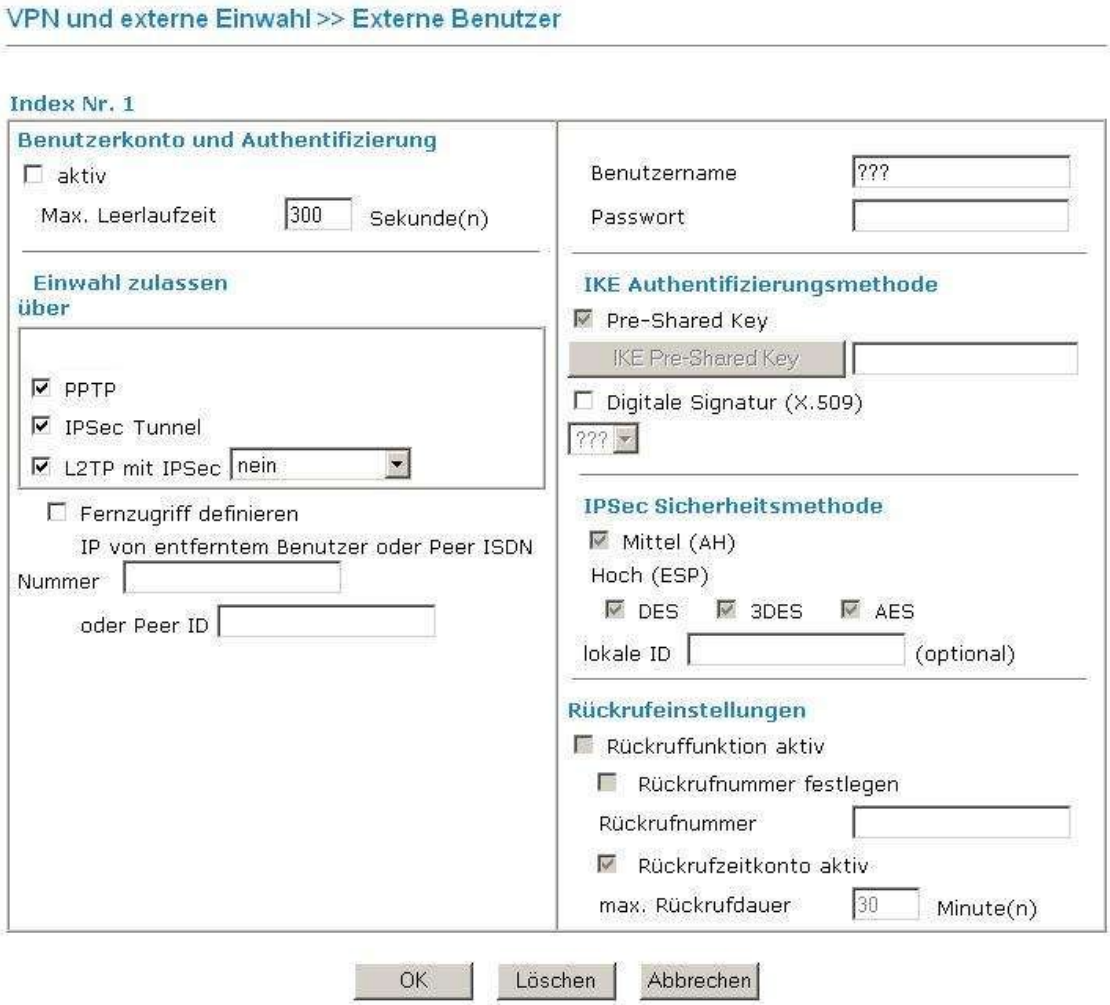
Index Klicken Sie auf einen der Indezies, um dieses Profil eines externen Benutzers zu konfigurieren.

Benutzer Gibt die Bezeichnung des Profils an. Ist die Bezeichnung **???**, so ist das Profil leer.

Status Die Statusanzeige gibt an, ob das Profil aktiv (V) oder inaktiv (X) ist.

Weiter Klicken Sie hier, um weitere Profile angezeigt zu bekommen.

Jeder Index steht für ein Profil eines Teleworkers und kann mit einem Klick auf den Index editiert werden. **Abhängig von der gewählten Verbindungsart, müssen entsprechend unterschiedliche Felder auf der rechten Seite ausgefüllt werden.** Falls das Feld ausgegraut ist, muss es nicht editiert werden. Es ist also nicht notwendig, alle Felder auszufüllen.



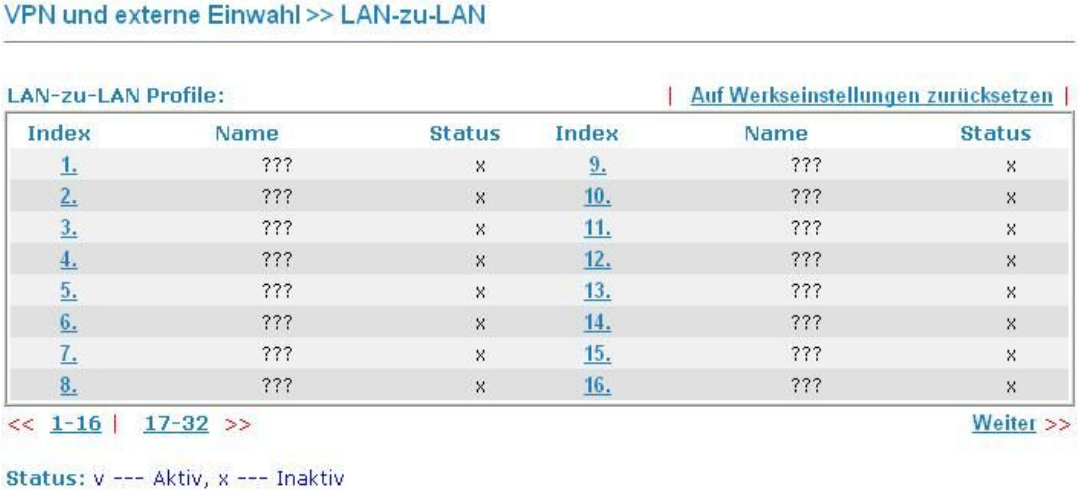
aktiv	Hiermit aktivieren Sie das Profil. **Max. Leerlaufzeit –** Verwendet der Teleworker den Tunnel für die angegebene Zeitspanne nicht, wird der Vigor die Verbindung trennen. Der Standardwert ist 300 Sekunden.
PPTP	Erlaubt die Einwahl in dieses Profil mit PPTP. Es werden die Angaben Benutzername und Passwort benötigt.
IPSec Tunnel	Erlaubt einem Teleworker eine IPSec VPN Verbindung durch das Internet herzustellen. Neben Benutzername und Passwort werden noch die Angaben zum Fernzugriff, Authentifizierungs- und Sicherheitsmethode verlangt.
L2TP	Erlaubt einem Teleworker eine L2TP VPN Verbindung durch das Internet herzustellen. L2TP kann alleine oder in Verbindung mit IPSec verwendet werden: **nein –** IPSec wird nicht implementiert. Dadurch kann die Verbindung als reiner L2TP Tunnel betrachtet werden. Es werden die Angaben Benutzername und Passwort benötigt. **falls vorhanden –** Die IPSec Policy wird zunächst hinzugefügt. Stellt sich beim Aushandeln mit der Gegenseite heraus, dass diese kein IPSec unterstützt, so fällt der Vigor zurück auf die reine L2TP Verbindung. Angaben wie beim IPSec Tunnel. **erforderlich –** Der Vigor besteht auf IPSec. Wenn die Gegenseite dies nicht unterstützt, kommt kein Tunnel zustande.

	Angaben wie beim IPSec Tunnel.
Fernzugriff definieren	**Box aktiviert –** Definieren Sie die IP-Adresse des Teleworkers oder eine Peer ID (verwendet für IKE Aggressive Mode). **Box deaktiviert –** Es werden Authentifizierungs- und Sicherheitsmethode aus den allgemeinen Einstellungen verwendet.
Benutzername	Dieses Feld müssen Sie ausfüllen, wenn Sie PPTP oder L2TP mit bzw. ohne IPSec Policy ausgewählt haben.
Passwort	Dieses Feld müssen Sie ausfüllen, wenn Sie PPTP oder L2TP mit bzw. ohne IPSec Policy ausgewählt haben.
IKE Authentifizierungsmethode	Die Angaben in den Feldern werden für IPSec Tunnel und L2TP mit IPSec Policy benötigt, sofern ein Fernzugriff definiert wurde. Die einzige Ausnahme hiervon betrifft die Digitale Signatur (X.509), welche auch dann aktiviert werden kann, wenn kein Fernzugriff definiert wurde. **Pre-Shared Key –** Aktivieren Sie die Option, um einen Pre-Shared Key mit 1-63 Zeichen einzugeben. **Digital Signatur (X.509) –** Aktivieren Sie die Option, um ein vordefiniertes X.509 Peer ID Profil als Digitale Signatur hinzuzufügen.
IPSec Sicherheitsmethode	Die Angaben in den Feldern werden für IPSec Tunnel und L2TP mit IPSec Policy benötigt, sofern ein Fernzugriff definiert wurde. Folgende Sicherheitsmethoden stehen zur Verfügung: **Mittel** – Der Authentication Header (AH) authentifiziert die Daten, verschlüsselt diese aber nicht. Diese Option ist mit den Werkseinstellungen aktiv. **Hoch** – Das Encapsulating Security Payload (ESP) umschließt die Nutzdaten und verschlüsselt diese. Als Verschlüsselungs-Algorithmus können Data Encryption Standard (DES), Triple DES (3DES) und Advance Encryption Standard (AES) gewählt werden. **lokale ID –** Definieren Sie eine lokale ID, welche in den Einstellungen zum Einwählen eines LAN-zu-LAN Profils verwendet werden kann. Diese Einstellung ist optional und ist nur in Verbindung mit dem IKE Aggressive Mode relevant.

3.6.6 LAN-zu-LAN

An dieser Stelle können LAN-zu-LAN VPN Verbindungen gestaltet und verwaltet werden. Diese Art der VPN Verbindung koppelt zwei lokale Netzwerke über ein öffentliches Netz wie das Internet.

Der Vigor bietet 32 Profile, welche auch alle gleichzeitig unterstützt werden können. Die folgende Ansicht zeigt die Tabelle aller LAN-zu-LAN Profile.



Auf Werkseinstellungen ... Löscht alle Profile.

Name Gibt die Bezeichnung des Profils an. Ist die Bezeichnung **???**, so ist das Profil leer.

Status Die Statusanzeige gibt an, ob das Profil aktiv (V) oder inaktiv (X) ist.

Weiter Klicken Sie hier, um weitere Profile angezeigt zu bekommen.

Jeder Index steht für ein Profil und kann mit einem Klick auf den Index editiert werden. Die LAN-zu-LAN Profile beinhaltet vier Abschnitte, welchen thematisch Konfigurationen zugeordnet sind. Falls ein Konfigurationsfeld ausgegraut ist, muss es nicht editiert werden. Es ist also nicht notwendig, alle Felder auszufüllen.

Da die Webseite mit dem LAN-zu-LAN Profil sehr umfangreich ist, wurde diese folgend in die jeweiligen Abschnitte unterteilt.

Profil Name Vergeben Sie eine Bezeichnung für das Profil.

Aktiv Hiermit aktivieren Sie das Profil.

Anrufrichtung Spezifizieren Sie die Wählrichtung, des Profils:
Beide – Initiator/Antworter

Raus – nur Initiator
Rein – nur Antworter

Immer im Betrieb Die VPN Verbindung wird immer aufrecht gehalten.

max. Leerlaufzeit Wird die Verbindung für die angegebene Zeitspanne nicht genutzt, trennt der Vigor die Verbindung. Der Standardwert ist 300 Sekunden.

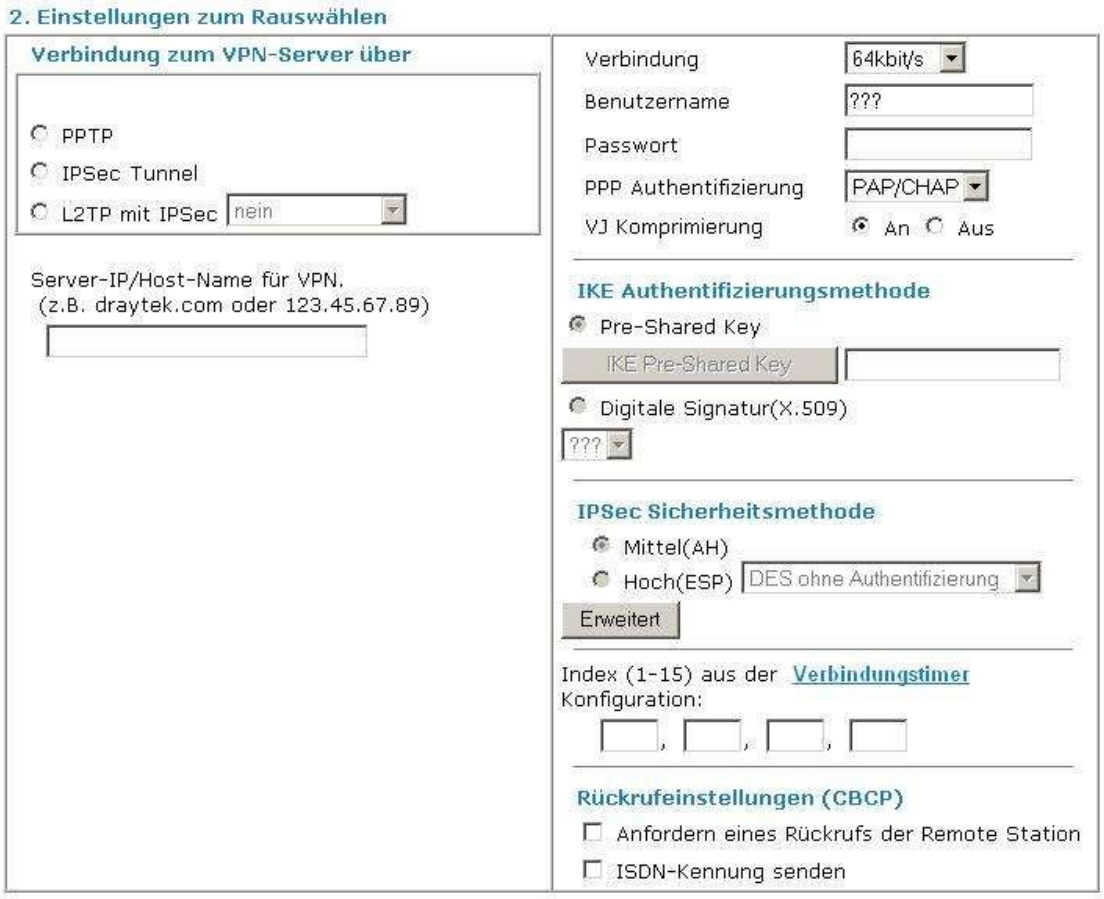
Dauerping zum Halten ... Diese Funktion hilft die Verbindung bei IPSec Verbindungen zu halten und wird bevorzugt bei ungewöhnlichen Störungen im IPSec Tunnel verwendet. Ist die Option aktiv, so werden PING Pakete kontinuierlich an die angegebene IP-Adresse gesendet. Weitere Informationen finden Sie in der folgenden Box.

PING auf IP Geben Sie die IP-Adresse eines Hosts auf der anderen Seites dieses VPN Tunnels an.

Die Option **Dauerping zum Halten der Verbindung** wird verwendet, um ungewöhnlichen Störungen im IPSec Tunnel zu begegnen. Sie unterstützt den Vigor den Zustand der VPN Verbindung aufrecht zu halten.

Wenn ein VPN Peer normalerweise die Verbindung beenden möchte, werden eine Reihe von Informationen zwischen den Teilnehmern ausgetauscht. Wird die Verbindung allerdings ohne diesen Austausch getrennt, so kann der Vigor seine Situation nicht definieren. Die Lösung dieses Problems ist, kontinuierlich PING Pakete an die Gegenstelle senden. So kennt der Vigor mit Gewissheit den Zustand der VPN Verbindung und kann entsprechend handeln.

Diese Funktion ist unterschiedlich zu DPD (dead peer detection).



PPTP	Erlaubt eine PPTP VPN Verbindung durch das Internet herzustellen. Es werden die Angaben Benutzername und Passwort benötigt, um sich auf dem entfernten Server einwählen zu können.
IPSec Tunnel	Erlaubt eine IPSec VPN Verbindung durch das Internet zu einem Server herzustellen. Neben Benutzername und Passwort werden noch die Angaben zur Server-IP, Authentifizierungs- und Sicherheitsmethode verlangt.
L2TP mit IPSec	Erlaubt die Abwahl mit L2TP zu einem Server. L2TP kann alleine oder in Verbindung mit IPSec verwendet werden: **nein –** IPSec wird nicht implementiert. Dadurch kann die Verbindung als reiner L2TP Tunnel betrachtet werden. Es werden die Angaben Benutzername und Passwort benötigt. **falls vorhanden –** Die IPSec Policy wird zunächst hinzugefügt. Stellt sich beim Aushandeln mit der Gegenseite heraus, dass diese kein IPSec unterstützt, so fällt der Vigor zurück auf die reine L2TP Verbindung. Angaben wie beim IPSec Tunnel. **erforderlich –** Der Vigor besteht auf IPSec. Wenn die Gegenseite dies nicht unterstützt, kommt kein Tunnel zustande. Angaben wie beim IPSec Tunnel.
Benutzername	Dieses Feld müssen Sie ausfüllen, wenn Sie PPTP oder L2TP mit bzw. ohne IPSec Policy ausgewählt haben.
Passwort	Dieses Feld müssen Sie ausfüllen, wenn Sie PPTP oder L2TP mit bzw. ohne IPSec Policy ausgewählt haben.

PPP Authentifizierung Für PPTP oder L2TP mit/ohne IPSec Policy wählen Sie hier das bevorzugte Authentifizierungsprotokoll. Allgemein fällt die Wahl auf PAP/CHAP, da dies die höchste Kompatibilität bietet.

VJ Komprimierung Für PPTP oder L2TP mit/ohne IPSec Policy wählen Sie hier, ob der TCP/IP Header komprimiert werden soll. Um Bandbreite zu sparen wird diese Option allgemein auf **Ja** gesetzt. Beachten Sie, dass diese Option auf der Gegenseite genau so gesetzt ist!

IKE Authentifizierungsmethode Die Angaben in den Feldern werden für IPSec Tunnel und L2TP mit IPSec Policy benötigt

Pre-Shared Key – Aktivieren Sie die Option, um einen Pre-Shared Key mit 1-63 Zeichen einzugeben.
Digital Signatur (X.509) – Aktivieren Sie die Option, um ein vordefiniertes X.509 Peer ID Profil als Digitale Signatur hinzuzufügen.

IPSec Sicherheitsmethode Die Angaben in den Feldern werden für IPSec Tunnel und L2TP mit IPSec Policy benötigt.

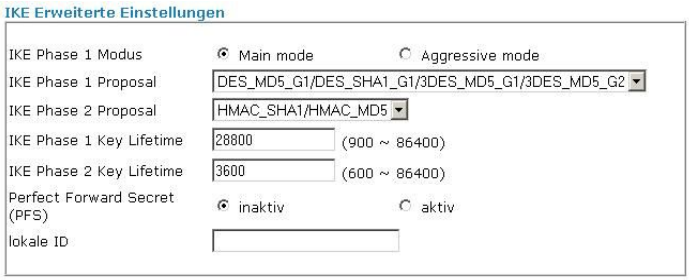
Mittel Der *Authentication Header* (AH) authentifiziert die Daten, verschlüsselt diese aber nicht. Diese Option ist mit den Werkseinstellungen aktiv.

Hoch Das *Encapsulating Security Payload* (ESP) umschließt die Nutzdaten, authentifiziert und verschlüsselt diese. Wählen Sie einen der folgenden Verschlüsselungs-Algorithmen:

- *DES ohne Authentifizierung*
- *DES mit Authentifizierung*
- *3DES ohne Authentifizierung*
- *3DES mit Authentifizierung*
- *AES ohne Authentifizierung*
- *AES mit Authentifizierung*

Die zusätzliche Authentifizierung wird durch MD5 oder SHA-1 realisiert.

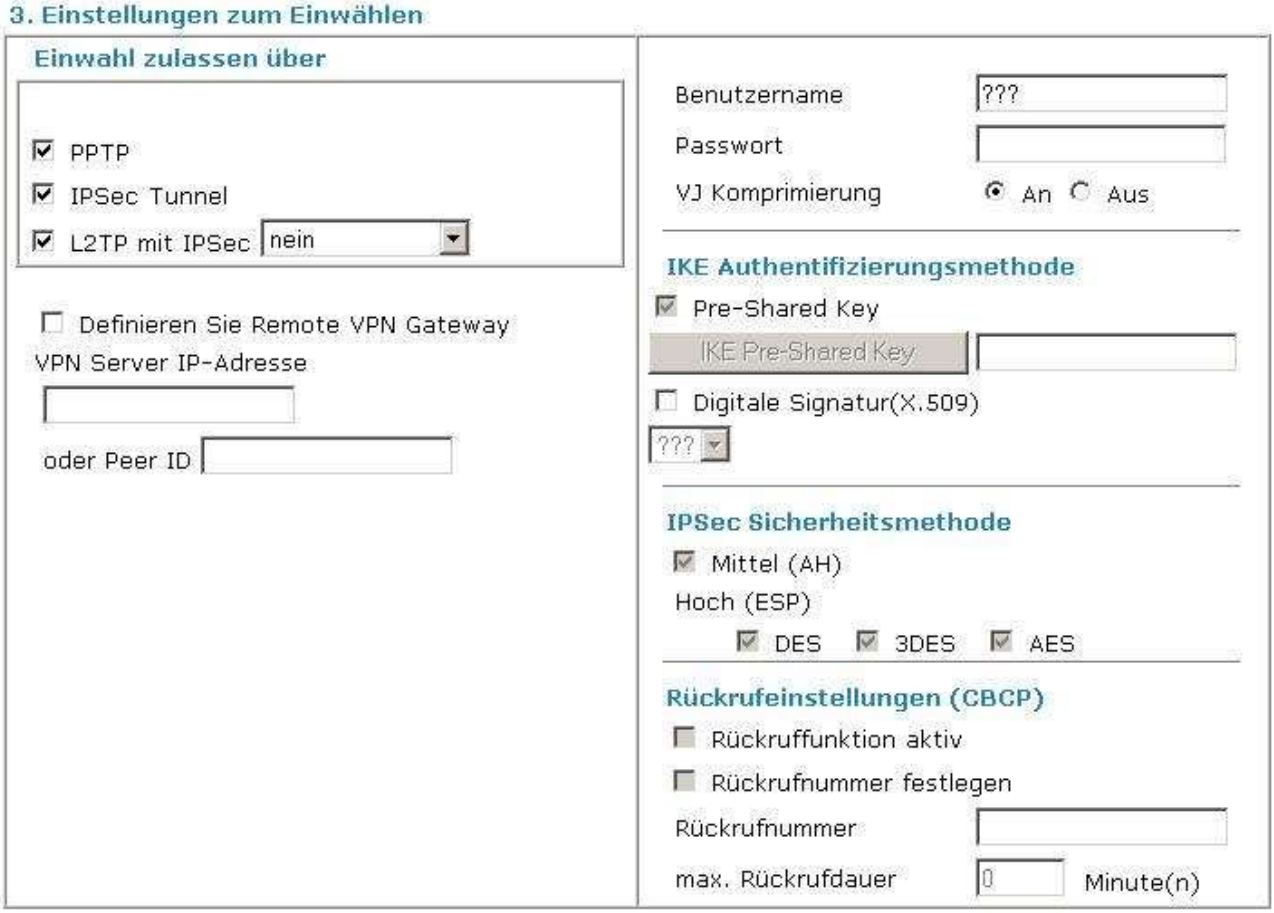
Erweitert Hier haben Sie Einfluss auf Modus, Proposal und Key Lifetime jeder IKE Phase, Gateway etc.
Das Fenster der erweiterten Einstellungen wird folgend angezeigt:



IKE Phase 1 Modus – Wählen Sie zwischen **Main** mode und **Aggressive** mode. Das Endergebnis ist bei beiden Modi gleich: Es werden Sicherheitsanträge (Proposals) ausgehandelt, um einen sicheren geschützten Tunnel zu erzeugen. Der **Main** mode ist sicherer als der **Aggressive** mode, da hierbei mehr

kommuniziert wird bis die IPSec Sitzung etabliert wird. Dafür ist der **Aggressive** mode schneller. Als Standard wird der Main mode verwendet.
IKE Phase 1 Proposal – Definieren Sie die lokal verfügbaren Techniken zur Authentizität und Verschlüsselung dieses VPN Peers. Diese werden der Gegenseite vorgeschlagen und es wird sich schließlich auf eine Übereinstimmung geeinigt werden. Zwei Optionen sind für den Aggressive mode und neun im **Main** mode verfügbar. Die Bezeichnungen G1 bzw. G2 beschreiben die Länge des Diffie-Hellman Schlüssels mit 768 bits bzw. 1024 bits. Die CPU wird bei großen Schlüsseln nicht mehr belastet als bei kleineren - es treten also keine Performanz Einbußen auf. Allerdings dauert der Schlüsselaustausch entsprechend länger. Wähle Sie am Besten die Optionen, welche die meisten Techniken beinhaltet, um so eine hohe Akzeptanz zu erreichen.

IKE Phase 2 Proposal – Definieren Sie die lokal verfügbaren Algorithmen, welche vorgeschlagen und über die abgestimmt werden sollen. Sie können für beide Modi zwischen drei Optionen wählen. Wähle Sie am Besten die Option, welche die meisten Algorithmen beinhaltet.
IKE Phase 1 Key Lifetime – Aus Sicherheitsgründen sollte die Zeit, in welcher der Schlüssels gültig ist definiert werden. Ab Werk sind 3600 Sekunden gesetzt. Der Wert kann beliebig zwischen 900 und 86400 Sekunden gewählt werden.
IKE Phase 2 Key Lifetime - Aus Sicherheitsgründen sollte die Zeit, in welcher der Schlüssels gültig ist definiert werden. Ab Werk sind 28800 Sekunden gesetzt. Der Wert kann beliebig zwischen 600 und 86400 Sekunden gewählt werden.
Perfect Forward Secret (PFS) – Ist die Option **aktiv** wird der IKE Phase 1 Key auch für die Phase 2 verwendet, um so aufwendige Rechnleistung zu minimieren. Ab Werk ist die Option **inaktiv**.
lokale ID – Im **Aggressive** mode, wird die lokale ID anstelle einer IP-Adresse zur Authentifizierung am Server verwendet. Die Länge der ID ist auf 47 Zeichen begrenzt.



Einwahl zulassen über	Bestimmen Sie, welche Art der Einwahl zugelassen ist.
PPTP	Erlaubt eine PPTP VPN Verbindung herzustellen. Es werden die Angaben Benutzername und Passwort benötigt, mit welchen sich der Client authentifizieren muss.
IPSec Tunnel	Erlaubt eine IPSec VPN Verbindung von einem entfernten Netzwerk herzustellen. Neben Benutzername und Passwort werden noch die Angaben zur Server-IP, Authentifizierungs- und Sicherheitsmethode verlangt.
L2TP	Erlaubt die Einwahl mit L2TP von einem Client. L2TP kann alleine oder in Verbindung mit IPSec verwendet werden: **nein** – IPSec wird nicht implementiert. Dadurch kann die Verbindung als reiner L2TP Tunnel betrachtet werden. Es werden die Angaben Benutzername und Passwort benötigt. f**alls vorhanden** – Die IPSec Policy wird zunächst hinzugefügt. Stellt sich beim Aushandeln mit der Gegenseite heraus, dass diese kein IPSec unterstützt, so fällt der Vigor zurück auf die reine L2TP Verbindung. Angaben wie beim IPSec Tunnel. e**rforderlich** – Der Vigor besteht auf IPSec. Wenn die Gegenseite dies nicht unterstützt, kommt kein Tunnel zustande. Angaben wie beim IPSec Tunnel.
Definieren Sie Remote VPN Gateway ...	Definieren Sie die IP-Adresse des Einwählenden oder dessen Peer ID. Definieren Sie des Weiteren die Sicherheitsmethode

	auf der rechten Seite. Ist die Box deaktiviert, werden Authentifizierungs- und Sicherheitsmethode aus den allgemeinen Einstellungen verwendet.
Benutzername	Dieses Feld müssen Sie ausfüllen, wenn Sie PPTP oder L2TP mit bzw. ohne IPSec Policy ausgewählt haben.
Passwort	Dieses Feld müssen Sie ausfüllen, wenn Sie PPTP oder L2TP mit bzw. ohne IPSec Policy ausgewählt haben.
VJ Komprimierung	Für PPTP oder L2TP mit/ohne IPSec Policy wählen Sie hier, ob der TCP/IP Header komprimiert werden soll. Um Bandbreite zu sparen wird diese Option allgemein auf **Ja** gesetzt. Beachten Sie, dass diese Option auf der Gegenseite genau so gesetzt ist!
IKE Authentifizierungsmethode	Die Angaben in den Feldern werden für IPSec Tunnel und L2TP mit IPSec Policy benötigt, sofern eine Peer VPN Server IP definiert wurde. Die einzige Ausnahme hiervon betrifft die Digitale Signatur (X.509), welche auch dann aktiviert werden kann, wenn Sie einen IPSec Tunnel mit bzw. ohne die Definition einer IP-Adresse für die Gegenstelle. **Pre-Shared Key –** Aktivieren Sie die Option, um einen Pre-Shared Key mit 1-63 Zeichen einzugeben. **Digital Signatur (X.509) –** Aktivieren Sie die Option, um ein vordefiniertes X.509 Peer ID Profil als Digitale Signatur hinzuzufügen.
IPSec Sicherheitsmethode	Die Angaben in den Feldern werden für IPSec Tunnel und L2TP mit IPSec Policy benötigt, sofern ein Fernzugriff definiert wurde. Folgende Sicherheitsmethoden stehen zur Verfügung: **Mittel** – Der Authentication Header (AH) authentifiziert die Daten, verschlüsselt diese aber nicht. Diese Option ist mit den Werkseinstellungen aktiv. **Hoch** – Das Encapsulating Security Payload (ESP) umschließt die Nutzdaten und verschlüsselt diese. Als Verschlüsselungs-Algorithmus können Data Encryption Standard (DES), Triple DES (3DES) und Advance Encryption Standard (AES) gewählt werden.

Meine WAN IP Dieses Feld ist nur auszufüllen, wenn IPSec oder L2TP mit IPSec Policy gewählt wurde. Der Standardwert ist 0.0.0.0 und bedeutet, dass der Vigor eine PPP IP-Adresse von dem entfernten Peer während der IPCP Negotiation Phase erhalten wird. Ist die PPP IP-Adresse durch den entfernten Peer festgelegt, so definieren Sie diese feste IP-Adresse hier.

Remote Gateway-IP Dieses Feld ist nur auszufüllen, wenn IPSec oder L2TP mit IPSec Policy gewählt wurde. Der Standardwert ist 0.0.0.0 und bedeutet, dass der Vigor eine Remote Gateway IP-Adresse von dem entfernten Peer während der IPCP Negotiation Phase erhalten wird. Ist die PPP IP-Adresse durch den entfernten Peer festgelegt, so definieren Sie diese feste IP-Adresse hier.

Remote Netzwerk-IP/ Remote Netzwerk -Mask Geben Sie einen statischen Peer mit IP-Adresse und Maske an, an welchen der komplette Datenverkehr geleitet werden soll – also das andere Ende des Tunnels. Bei IPSec wird hier die Ziel Client ID der Phase 2 (quick mode) angegeben.

Mehr Fügen Sie einen statischen Peer hinzu, um den Datenverkehr zu weiteren Remote Netzwerk IP-Adressen / Remote Netzwerk Masken durch die VPN Verbindung zu leiten. Im Allgemeinen wird diese Funktion verwendet, um Subnetze in dem entfernten Netzwerk zu erreichen.

RIP Richtung Definieren Sie den Weg der RIP (Routing Information Protocol) Pakete. Als Optionen stehen *beide (TX/RX)*, *nur Empfangen*, *nur Senden* und *inaktiv* zur Verfügung.

RIP Version Wählen Sie die zu verwendene Version des RIP Protokolls. Die *Ver. 2* erzielt die höchste Kompatibilität.

Im NAT-Betrieb, betrachte entfernte Subnetze als Für die Kommunikation mit dem entfernten Netzwerk kann der Vigor dieses als lokales Subnetz behandeln und Pakete mit seiner privaten IP-Adresse senden. Alternativ kann der Vigor seine öffentliche IP-Adresse verwenden und damit das entfernte Netz wie ein öffentliches handhaben.

3.6.7 Verbindungsmanagement

Dieser Menüpunkt zeigt eine komplette Übersicht über alle VPN Verbindungen. In dem Pull-Down Feld finden Sie alle aktiven Profile mit der Wählrichtung *Beide* oder *Raus*. Durch das Klicken auf den **Wählen** Button verbindet sich der Vigor mit dem Server. In der nachfolgenden Liste finden sich alle VPN Tunnel, welche zurzeit aktiv sind. Um eine

Verbindung zu beenden, verwenden Sie den **Trennen** Button.

Wählen	Klicken Sie auf diesen Button, um einen VPN Tunnel zu aktivieren.
Aktualisierungsintervall	Wählen Sie die Abstände, in denen sich die Seite aktualisiert.
Aktualisieren	Klicken Sie den Button zum Aktualisieren des Verbindungs-Status.

3.7 Zertifikatsverwaltung

Ein digitales Zertifikat ist eine elektronische ID, welche von einer Certification Authority (CA) vergeben wird. Es beinhaltet Informationen wie Name, Seriennummer, Verfallsdatum, usw. und natürlich die eigentliche digitale Signatur, welche von einer berechtigten Autorität herausgegeben wurde und womit der Empfänger verifizieren kann, dass das Zertifikat echt ist. Der Vigor unterstützt digitale Zertifikate nach dem Standard X.509.

Möchte eine Instanz ein digitales Zertifikat anwenden, so muss diese zunächst nach einem gültigen Zertifikat bei einem CA Server anfragen. Es ist durchaus sinnvoll Zertifikate von mehreren Servern zu besitzen, um sich so auch bei Peers mit Zertifikaten von diesen Servern authentifizieren zu können.

Unter diesem Menüpunkt können Sie die Zertifikate verwalten, lokale digitale Zertifikate generieren und vertrauenswürdige CA Zertifikate setzen. Justieren Sie bitte die Einstellungen in *Systemmanagement >> Zeit und Datum*, damit die Berechnung der Lebensdauer eines Zertifikates korrekt ist.

3.7.1 lokales Zertifikat

Generieren Klicken Sie auf diesen Button, um einen Zertifikatsauftrag zu erstellen.

Geben Sie alle relevanten Informationen ein und klicken Sie auf **Generieren**.

Importieren Hier können Sie ein gespeichertes Zertifikat laden.

Aktualisieren Hiermit wird die Seitenansicht aktualisiert.

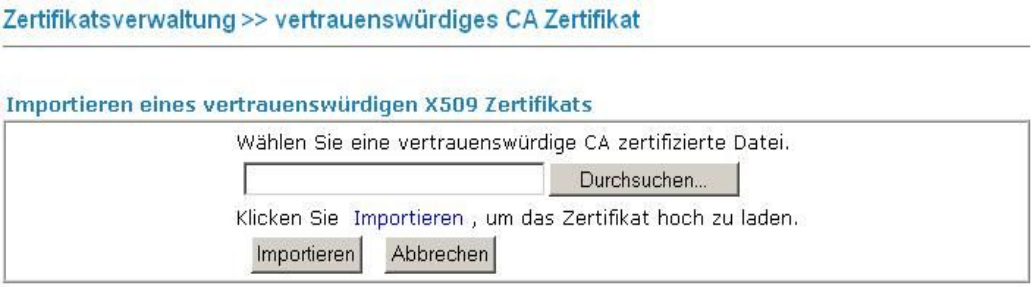
Ansicht Über diesen Button erhalten Sie die detaillierten Informationen zu dem Zertifikatsauftrag.

Nachdem Sie auf **Generieren** geklickt haben, werden die generierten Informationen in dem Fenster angeszeigt:

3.7.2 vertrauenswürdiges CA Zertifikat

Dieser Punkt listet drei vertrauenswürdige CA Zertifikate.

Um ein zuvor gespeichertes vertrauenswürdiges CA Zertifikat zu importieren, klicken Sie bitte auf **Importieren**. Im folgenden Fenster wählen Sie die entsprechende Datei und klicken wieder auf **Importieren**. Nun wird die gewählte Datei im vorherigen Fenster gelistet. Klicken Sie dort nun ein letztes Mal **Importieren**, um die Datei verwenden zu können.



Detaillierte Informationen über jedes vertrauenswürdige CA Zertifikat erhalten Sie über die **Ansicht**. Mit **Löschen** können Sie ein importiertes Zertifikat entfernen.

3.8 Systemmanagement

Mit den Unterpunkten in diesem Menü kann das System im Einzelnen konfiguriert werden.

3.8.1 Systemstatus

Der Systemstatus zeigt die grundlegenden Netzwerkeinstellungen des Vigors.

Modell Name	Zeigt die Bezeichnung von Modell oder Serie des Vigors.
Firmware Version	Zeigt die aktuelle Firmware Version.
Erstellungsdatum	Zeigt das Datum und die Zeit als die Firmware erstellt wurde.
MAC-Adresse	Zeigt die MAC-Adresse der LAN Schnittstelle.
1te IP-Adresse	Zeigt die IP-Adresse der LAN Schnittstelle.
1te Subnetz Maske	Zeigt die Subnetz Maske der LAN Schnittstelle.
DHCP Server	Zeigt, ob der DHCP Server der LAN Schnittstelle aktiv/inaktiv ist.
Link Status	Zeigt den Verbindungsstatus der WAN Schnittstelle.
MAC-Adresse	Zeigt die MAC-Adresse der WAN Schnittstelle.
Verbindung	Zeigt die Verbindungsart (PPPoE, PPPoA, ...).
IP-Adresse	Zeigt die IP-Adresse der WAN Schnittstelle.
Standard Gateway	Zeigt die zugewiesene IP-Adresse des Standard Gateways.
DNS	Zeigt die zugewiesene IP-Adresse des primären DNS.

3.8.2 Administrator Passwort

Diese Seite erlaubt die Modifikation des Zugangspasswort.

Altes Passwort Geben Sie das alte Passwort ein. Kein Standardwert gesetzt.

Neues Passwort Geben Sie das neue Passwort ein.

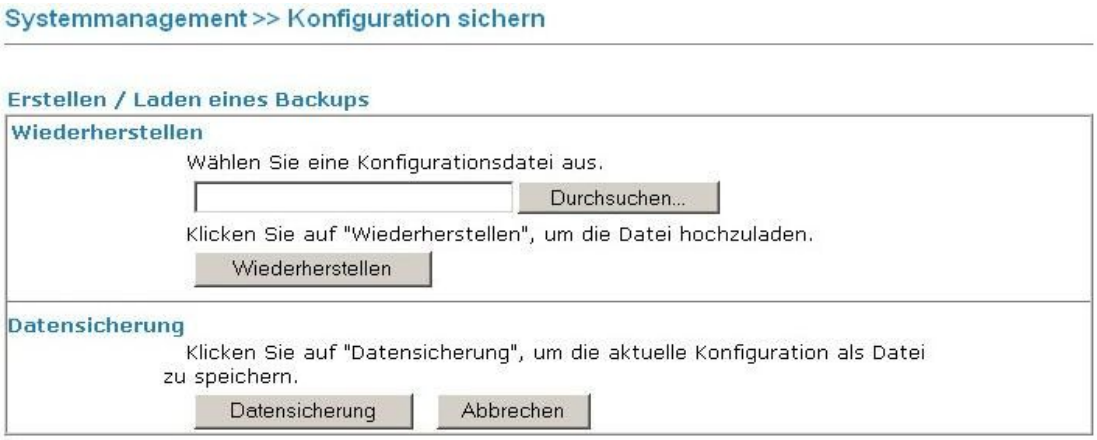
Neues Passwort wiederholen Wiederholen Sie das neue Passwort.

Klicken Sie auf **OK**, um die Konfiguration zu speichern. Anschließend wird das Login Fenster erscheinen und nach der Eingabe eines Passwortes fragen. Geben Sie das neue Passwort an.

3.8.3 Konfiguration sichern

Wiederherstellen

1.Navigieren Sie zu **Systemmanagement** >> **Konfiguration sichern**.



2.Klicken Sie auf **Durchsuchen**, um den Pfad eines gespeicherten BackUp zu wählen.

3.Klicken Sie auf **Wiederherstellen**, um die BackUp-Datei in den Vigor zu laden. Sie werden über den Erfolg informiert.

Datensicherung

1.Navigieren Sie zu **Systemmanagement** >> **Konfiguration sichern**.

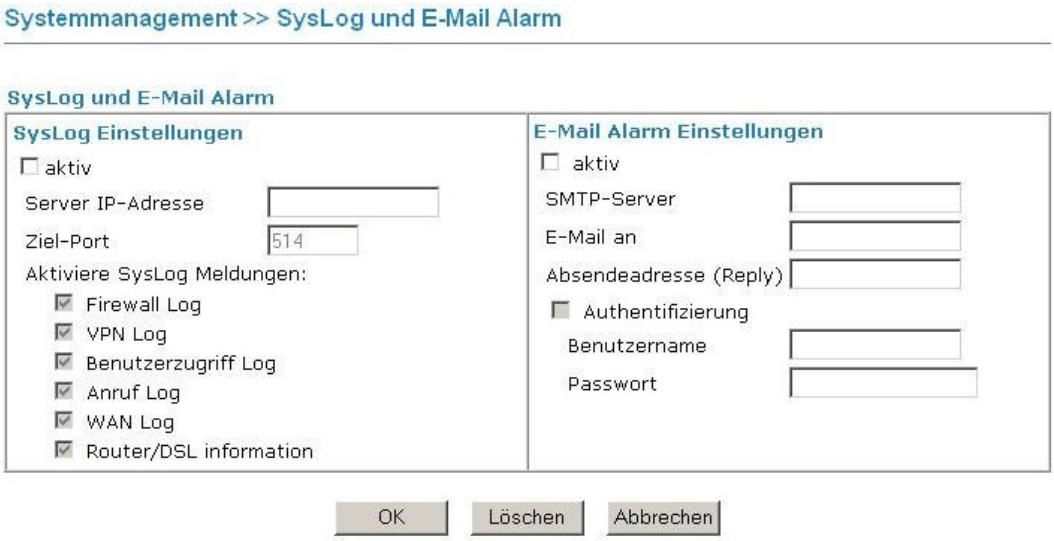
2.Klicken Sie auf **Datensicherung** und im folgenden Dialogfenster auf **Speichern**.

3.Es öffnet sich wieder ein Fenster, in welchem Sie den Ort und Namen der BackUp-Datei bestimmen können. Der Standardname für das BackUp ist **config.cfg**.

4.Klicken Sie den **Speichern** Button, um die Konfiguration auf Ihrem Computer zu sichern.

3.8.4 SysLog und E-Mail Alarm

Die SysLog Funktion hilft die einzelnen Prozesse im Vigor anzuzeigen und dient dem Debuggen.



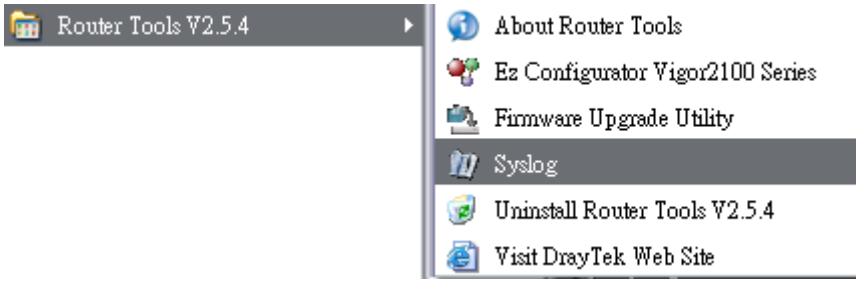
aktiv	Zum Aktivieren der jeweiligen Funktion.
Server IP-Adresse	Definieren Sie die IP-Adresse des SysLog Servers.
Ziel-Port	Weisen Sie einen Port zu. Der Standardwert ist 514.
Aktiviere SysLog Meldungen	Definieren Sie die benötigten Informationen.
SMTP-Server	Definieren Sie die IP-Adresse des SMTP Servers.
E-Mail an	Vergeben Sie die E-Mail Adresse zum Senden von Mails
Absendeadresse (Reply)	Weisen Sie einen Pfad zum Empfangen von Mails zu.
Authentifizierung	Vergeben Sie Benutzername und Passwort.

Klicken Sie auf **OK**, um die Konfiguration zu speichern.

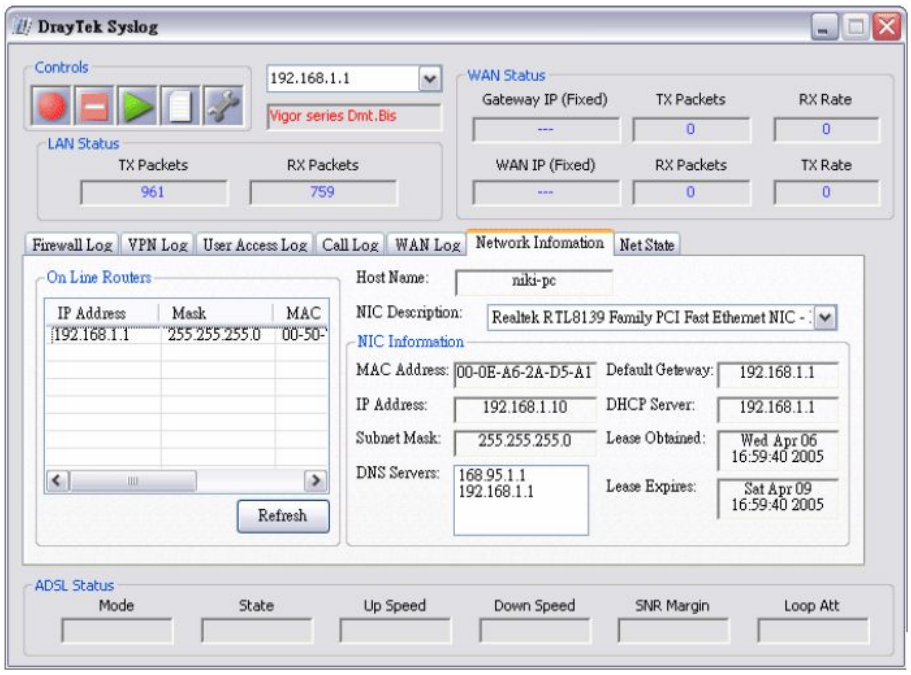
Um das SysLog auslesen zu können, befolgen Sie bitte folgende Schritte (Windows-Beispiel):

1.Setzen Sie die IP-Adresse Ihres Computers in das Feld ***Server IP-Adresse***.

2.Installiere Sie die Router Tools. Diese finden Sie zum Einen auf der beiliegenden CD oder aber auf unserer Homepage www.draytek.de. Nach der Installation navigieren Sie vom *Programme* Menü aus zu *Router Tools >> Syslog*.



3.Im SysLog Fenster wählen Sie bitte zunächst den Vigor, welche Sie untersuchen möchten. Beachten Sie, dass unter dem Reiter **Network Information** die korrekte Netzwerkkarte Ihres Computers angegeben ist.



3.8.5 Zeit und Datum

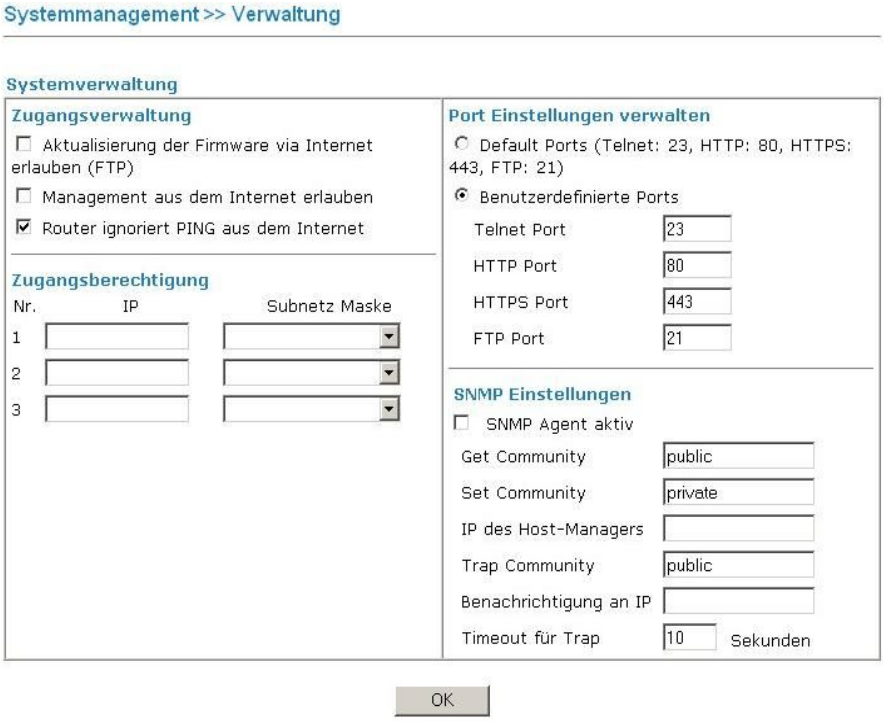
Hier können Sie bestimmen, wie bzw. woher der Vigor die Systemzeit bezieht.

Aktuelle Systemzeit	Klicken Sie auf **Zeit abrufen**, um die Zeitangabe zu aktualisieren.
Rechner/Browser-Zeit	Ist diese Option aktiv, wird als Systemzeit die Browser-Zeit des Administrator Computers übernommen.
Internet-Zeit	Ist diese Option aktiv, wird die Systemzeit von einem Time Server aus dem Internet bezogen.
Zeitprotokoll	Wählen Sie ein Zeitprotokoll.
Server IP-Adresse	Definieren Sie die IP-Adresse des Time Servers.
Zeitzone	Wählen Sie die Zeitzone, in welcher der Vigor sich befindet.
automatisch auf Sommer-/Winterzeit ...	Aktivieren Sie diese Option, sofern der Vigor von der Zeitumstellung betroffen ist.
Aktualisierungsintervall	Wählen Sie die Abstände, in denen sich die Seite aktualisiert.

Klicken Sie auf **OK**, um die Konfiguration zu speichern.

3.8.6 Verwaltung

Diese Seite erlaubt Ihnen, Modifikationen und Restriktionen für die Verwaltung des Vigors zu definieren.



Aktualisierung der Firmware via ...	Aktivieren Sie die Funktion, um ein Firmware Update mittels FTP Client über das Internet durchführen zu können. Ab Werk ist die Funktion inaktiv.
Management aus dem Internet erlauben	Aktivieren Sie die Funktion, um sich aus dem Internet heraus auf den Vigor einloggen zu können. Ab Werk ist die Funktion inaktiv.
Router ignoriert Ping aus dem Internet	Aktivieren Sie die Funktion und der Vigor wird alle PING Anfragen aus dem Internet verwerfen. Aus Sicherheitsgründen ist Funktion ab Werk aktiv.
Zugangsberechtigung	Definieren Sie, von welchen IP-Adressen die Konfiguration des Vigors möglich sein darf. **IP** – Die IP-Adressen mit Erlaubnis zum Login. **Subnetz Maske –** Die zu der definierte IP gehörende Maske.
Default Ports	Aktivieren Sie die Option, um die Standard Ports zu verwenden.
Benutzerdefinierte Ports	Definieren Sie die Ports für Telnet, HTTP, HTTPS und FTP Server.
SNMP Agent aktiv	Aktivieren Sie die SNMP Funktionen.
Get Community	Ändern Sie den Namen der Community. Der Standardwert ist **public.**
Set Community	Ändern Sie den Namen der Community. Der Standardwert ist **private.**
IP des Host-Managers	Definieren Sie den Manager, welcher die SNMP Funktionen ausführt.
Trap Community	Ändern Sie den Namen der Community. Der Standardwert ist **public.**
Benachrichtigung an IP	Definieren Sie den Empfänger eines Traps.
Timeout für Trap	Definieren Sie die Verspätung, ab wann ein Trap nutzlos wird. Der

Standardwert sind 10 Sekunden.

3.8.7 Neustart

Es ist möglich, einen Neustart des Vigors zu initiieren oder ihn sogar auf Werkseinstellungen zurückzusetzen.

Wollen Sie den Vigor neu starten und weiterhin die ***Aktuelle Konfiguration verwenden***, so wählen Sie bitte die erste Option. Soll nach dem Neustart Ihre Konfiguration verloren sein wählen Sie bitte ***Auf Werkseinstellungen zurücksetzen***.

Klicken Sie in beiden Fällen auf **OK**. Sie erreichen den Vigor wieder nach fünf bis zehn Sekunden über die entsprechende LAN IP-Adresse.

3.8.8 Firmware aktualisieren

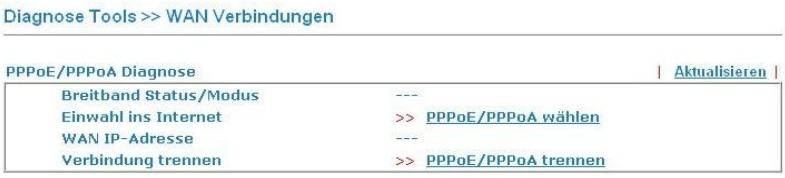
Bevor Sie die Firmware Ihres Vigors ändern können, müssen Sie die DrayTek Router Tools installieren. Verwenden Sie das in den Tools integrierte *Firmware Upgrade Utility*, um die Firmware in den Vigor zu laden.

Klicken Sie auf **OK** und der Vigor befindet sich für etwa zwei Minuten im TFTP Modus. Sie erkennen diesen Zustand, wenn die beiden linken LEDs synchron blinken. Nur in diesem Modus kann der Vigor eine neue Firmware empfangen.

3.9 Diagnose Tools

Die Diagnose Tools bieten die Möglichkeit, den Zustand des Vigors zu erkennen oder festzustellen.

3.9.1 WAN Verbindungen



Aktualisieren Aktualisiert die Informationen auf dieser Seite.

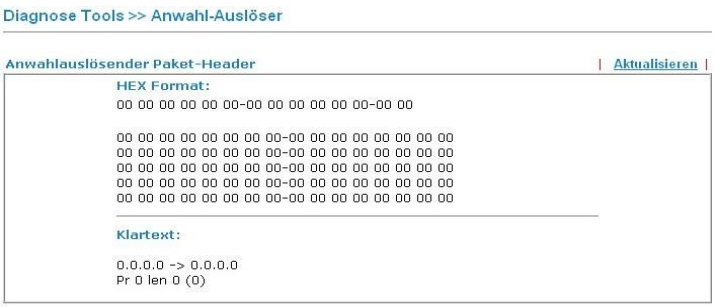
Breitband Status/Modus Zeigt die Art der Verbindung wie ***PPPoE***, ***PPPoA*** oder aber **---**, falls WAN inaktiv ist.

WAN IP-Adresse Die WAN IP-Adresse einer aktiven Verbindung.

PPPoE/PPPoA wählen / trennen Zum Verbinden / Trennen eine WAN Verbindung.

3.9.2 Anwahl-Auslöser

Wird die Einwahl ins Internet (PPPoE, PPPoA, usw.) von einer lokalen Quelle (Host im LAN) ausgeführt, so werden die Quell-IP und das auslösende Paket angezeigt.

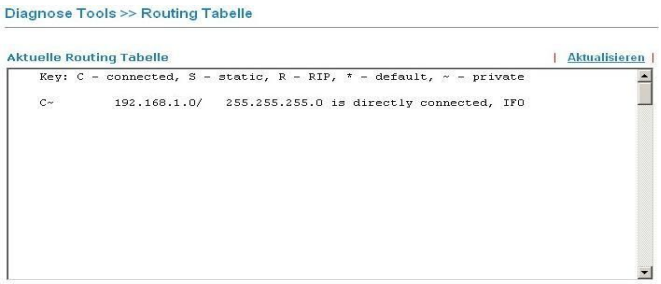


Klartext Zeigt die Quell-IP des lokalen Hosts, die Ziel-IP der entfernten Stelle, das verwendete Protokoll und die Länge des Pakets.

Aktualisieren Aktualisiert die Informationen auf dieser Seite.

3.9.3 Routing Tabelle

Die Tabelle zeigt die Wegewahl für IP-Pakete zu benachbarten Netzen.



Aktualisieren Aktualisiert die Informationen auf dieser Seite.

IF Der Interface Code ist repräsentativ für eine Schnittstelle:
0 => LAN, 1~2 => ISDN, 3 => WAN, 4 oder höher => VPN

3.9.4 ARP Cache Tabelle

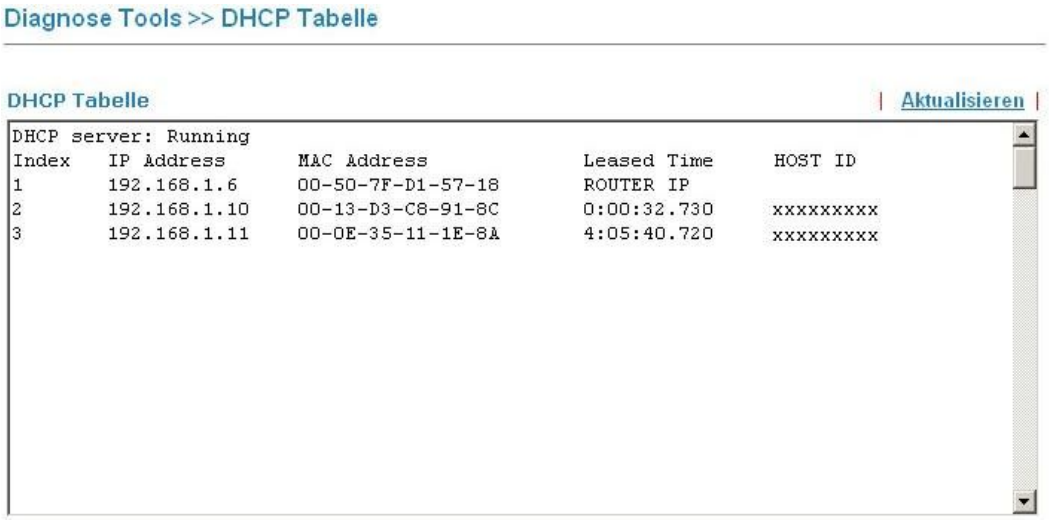
Die **ARP Cache Tabelle** zeigt die gespeicherten ARP-Informationen (Address Resolution Protocol). Das ARP ordnet IP- und MAC-Adressen zu.

Aktualisieren Aktualisiert die Informationen auf dieser Seite.

Löschen Löscht die komplette Liste.

3.9.5 DHCP Tabelle

Hier werden die Informationen der IP Adresszuweisung angezeigt. Diese sind besonderst bei Netzwerkproblemen in Verbindung mit IP Konflikten hilfreich.



Index Nummeriert die Verbindungen.

IP Address Zeigt die vom Vigor zugewiesene IP-Adresse.

MAC Address Zeigt die MAC-Adresse, welcher die IP-Adresse zugewiesen wurde.

Leased Time Zeigt die Dauer der IP Adresszuweisung.

HOST ID Zeigt die Host ID bzw. den Namen des Besitzers der MAC-Adresse.

Aktualisieren Aktualisiert die Informationen auf dieser Seite.

3.9.6 NAT Tabelle

Private IP:Port Zeigt die Quell-IP und Port eines lokalen Hosts.

#Pseudo Port Zeigt den temporär vom Vigor zugewiesenen NAT-Port.

Peer IP:Port Zeigt die Ziel-IP und Port des entfernten Hosts.

Ifno Der Interface Code ist repräsentativ für eine Schnittstelle:

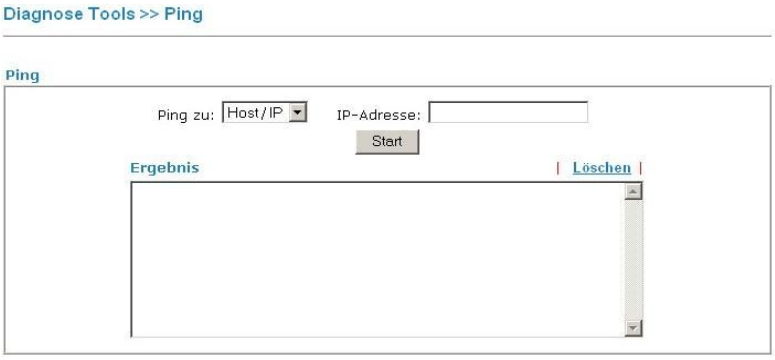
0:	LAN
1~2:	ISDN
3:	WAN
4 oder höher:	VPN

Status Die Werte sind wie folgt definiert:

0:	other TCP status
1:	TCP fin incoming
2:	TCP fin out
3:	TCP fin closing
4:	TCP syn
5:	TCP syn,ack
6:	TCP ack

Aktualisieren Aktualisiert die Informationen auf dieser Seite.

3.9.7 Ping



Ping zu Wählen Sie das Ziel, welches angepingt werden soll.

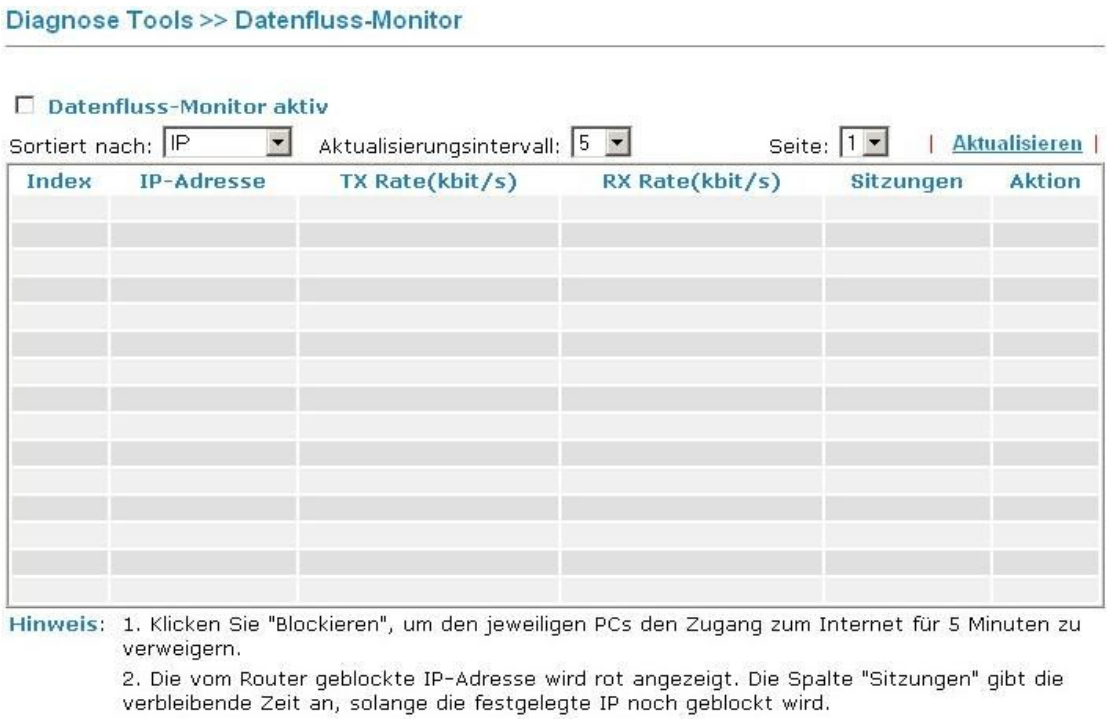
IP-Adresse Definieren Sie die anzupingende Host/IP.

Start Führt den Ping aus und zeigt das Ergebnis im Fenster.

Löschen Löscht das Ergebnis aus dem Fenster.

3.9.8 Datenfluss-Monitor

Diese Seite zeigt die laufenden IP-Prozeduren. Um dieses Tool nutzen zu können, müssen die zu überwachenden IP-Adressen zuvor im Bandbreite Management definiert sowie eine Begrenzung von Sitzungen und Bandbreite definiert und aktiviert werden.



Datenfluss-Monitor aktiv Aktivieren Sie diese Funktion.

Sortiert nach Wählen Sie die Reihenfolge der Daten für Ihre Übersicht.

Aktualisierungsintervall Wählen Sie die Abstände, in denen sich die Seite aktualisiert.

Aktualisieren Aktualisiert die Informationen auf dieser Seite.

Index Zeigt die Nummer des Datenfluss.

IP-Adresse Zeigt die IP-Adresse des überwachten Hosts.

TX Rate (kbit/s) Zeigt die Sendegeschwindigkeit des überwachten Hosts.

RX Rate (kbit/s) Zeigt die Empfangsgeschwindigkeit des überwachten Hosts.

Sitzungen Zeigt die im Menü *Bandbreite Management >> Sitzungen begrenzen* definierten maximal möglichen Sitzungen.

Aktion Klicken Sie **Blockieren**, um dem Host den Zugang ins WAN für etwa fünf Minuten zu verweigern. Mit **Freigeben** können Sie die Wartezeit sofort beenden.

3.9.9 Trace Route

Dieses Tool hilft Ihnen die Wegewahl des Routers zu einem Ziel zu verfolgen.

Host / IP-Adresse	Definieren Sie die IP-Adresse des Ziels.
Start	Führt den Trace aus und zeigt das Ergebnis im Fenster.
Löschen	Löscht das Ergebnis aus dem Fenster.