

Fernwartung mit WinCC flexible  
Kommunikation via Wide Area Network (WAN)

Virtual Privat Network

Ausgabe 12/04

## Vorwort

Diese Dokumentation beschreibt die Verbindung zweier Local Area Networks (LAN) auf Basis von Virtual Privat Network (VPN).

Des Weiteren wird das IPSec Protokoll erklärt. IPSec. ist ein Protokoll, das zum Aufbau einer sicheren IP-Verbindung verwendet werden kann.

## Haftung

Eine Haftung der Siemens AG, gleich aus welchem Rechtsgrund, für durch die Verwendung des vorliegenden Beitrags verursachte Schäden ist ausgeschlossen, soweit nicht z.B. bei Schäden an privat genutzten Sachen, Personenschäden oder wegen Vorsatzes oder grober Fahrlässigkeit zwingend gehaftet wird.

## Gewährleistung

Bei den Beiträgen handelt es sich um ausgewählte Lösungsvorschläge zu Anfragen mit komplexen Aufgaben, die im Customer Support erarbeitet wurden. Wir weisen außerdem darauf hin, dass es nach dem Stand der Technik nicht möglich ist, Fehler in Softwareprogrammen unter allen Anwendungsbedingungen auszuschließen. Die Beiträge wurden nach bestem Wissen erstellt. Eine Haftung die über die übliche Gewährleistung für Software der Klasse C entsprechend unseren "Allgemeinen Bedingungen für die Überlassung von Softwareprodukten für Automatisierungs- und Antriebstechnik" hinaus geht, können wir jedoch nicht übernehmen. Die Programme werden im Internet als Einzellizenzen angeboten. Eine Weitergabe an Dritte ist nicht gestattet.

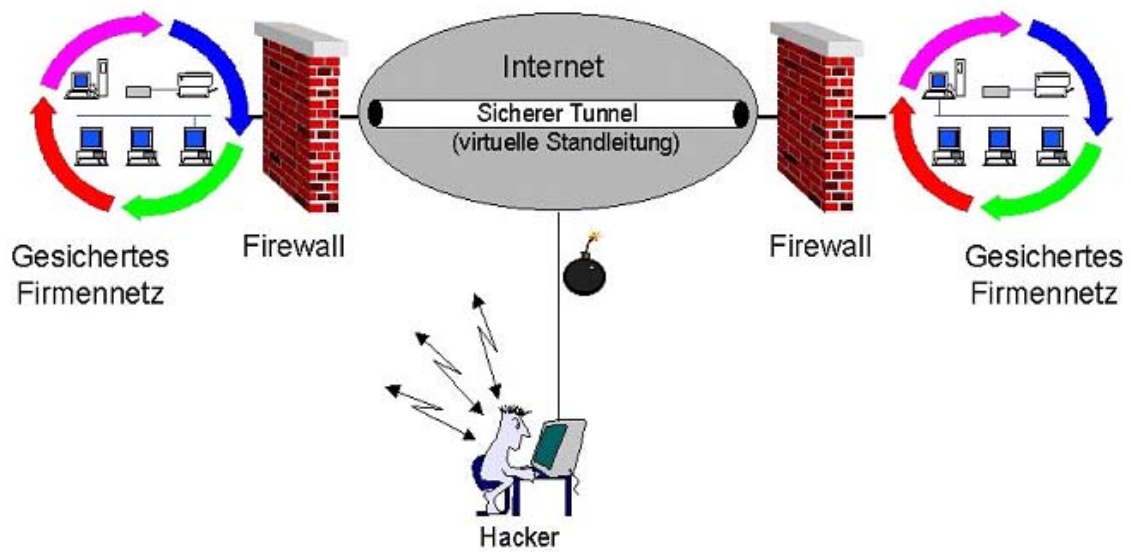
## Inhaltsverzeichnis

<b>1</b>	<b>Virtual Privat Network (VPN)</b> .....	<b>5</b>
1.1	Übersicht.....	5
1.2	Einleitung .....	6
1.2.1	Verbindung zweier LAN auf Basis von VPN .....	6
<b>2</b>	<b>Virtual Private Network mit IPSec Protokoll</b> .....	<b>7</b>
2.1	Einleitung .....	7
2.2	Kommunikation über IPSec. ....	8
2.3	Einstellung von IPSec.....	8
2.3.1	Lizenzschlüssel generieren .....	9
2.3.2	Einrichten von VPN über das Setup Tool .....	11
2.3.3	Internet Key Exchange .....	16
2.3.4	Anlegen der PC-Client Partnerverbindung .....	24
2.4	Einrichtung des IPSec Clients auf dem PC. ....	31
2.4.1	Installation der Client Software .....	31
2.5	Test der neu erstellten Verbindung:.....	43
<b>3</b>	<b>Glossar</b> .....	<b>48</b>
<b>4</b>	<b>Gewährleistung und Support</b> .....	<b>53</b>

## 1 Virtual Privat Network (VPN)

### 1.1 Übersicht

Abbildung 1-1



## 1.2 Einleitung

### 1.2.1 Verbindung zweier LAN auf Basis von VPN

Bei hohen Sicherheitsanforderungen sind geschützte Kommunikationsverbindungen, damit Maschinendaten nicht in falsche Hände geraten.

Der Router bietet dafür mehrere Verschlüsselungssysteme an, welche unter dem Hauptbegriff Virtual Private Network zusammengefasst sind (VPN).

Achten Sie beim Kauf eines Routers darauf, dass Ihr Router die Verschlüsselung in beide Richtungen unterstützt. Local --> Extern und Extern --> Lokal.

Bekannt ist das PPTP (Point-to-Point Tunneling Protocol) und das etwas neuere IPsec (Internet Protokoll Security) Protokoll.

Mit dieser Verschlüsselung schaffen Sie sich zwischen zwei Routern eine Verbindung, die von Außen geschützt ist und Ihnen intern die Möglichkeit gibt, alle Teilnehmer über den Namen oder die lokale IP Adresse anzusprechen.

Nach der Konfiguration des VPN IPsec Tunnels ist das Handling genau so, als hätten Sie zwischen Ihren Teilnehmern ein gekreuztes Netzkabel.

In den folgenden Dialogen erhalten Sie eine schrittweise Anleitung, wie Sie Ihr Netzwerk von Außen schützen können.

## 2 Virtual Private Network mit IPSec Protokoll

### 2.1 Einleitung

IPSec ist ein Protokoll, das zum Aufbau einer sicheren IP-Verbindung verwendet werden kann.

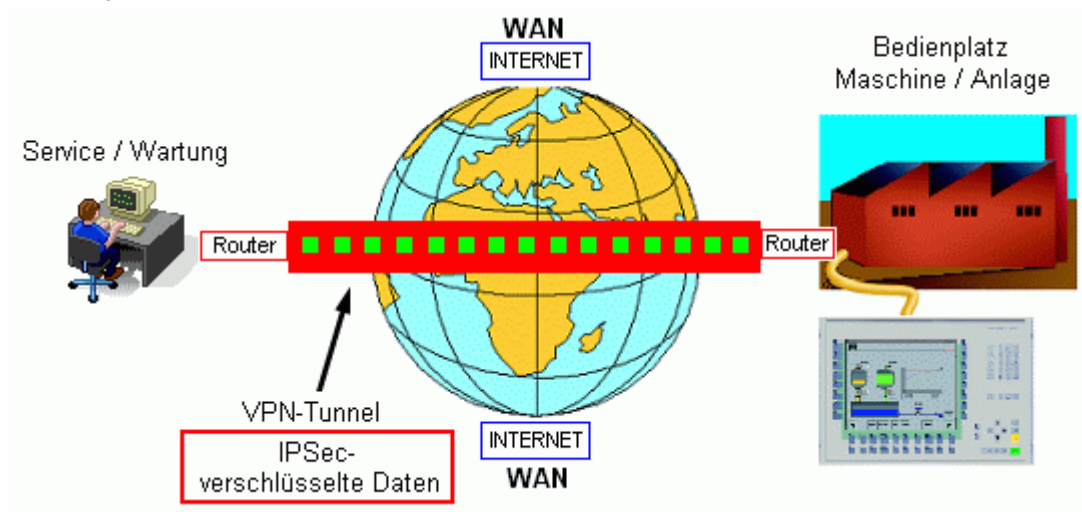
Die Basiskonfiguration des Routers für die Kommunikation über ISDN / DSL ist den folgenden Dokumenten zu entnehmen.

- Bediengerät kommuniziert über ISDN mit Router
- Bediengerät kommuniziert über DSL mit Router

Die Datensicherheit wird durch folgende 4 Funktionen gewährleistet:

- Verschlüsselung (mittels ESP = Encapsulation Security Payload)
- Nachrichtenintegrität (sicherstellen, dass die Nachricht nicht verändert wurde)
- Authentisierung des Senders
- Schlüsselverwaltung.

Abbildung 2-1



## 2.2 Kommunikation über IPSec.

### Anwendung

IPSec verwenden Sie, um zwei Router und auch externe Internetrechner mit einander zu verbinden.

Durch die Verschlüsselung entsteht ein so genannter Virtueller Tunnel (VPN Tunnel) zwischen den Routern. Es bietet Ihnen die Möglichkeit in den Netzwerken so zu arbeiten, als ob Sie sich in einem lokalen Netzwerk befinden.

Nach dem die Verbindung aufgebaut ist, werden alle Telegramme mit einem zusätzlichen „Header“ versehen, der zur Verschlüsselung dient.

Eine VPN IPSec Verbindung ist immer dann zu empfehlen, wenn Dritte keinen Zugriff auf Ihr Netzwerk bekommen sollen.

## 2.3 Einstellung von IPSec.

Damit die IPSec Dialoge auf Ihrem Rechner dargestellt werden können müssen Sie zuerst die Lizenz Schlüssel über das Setup Tool eintragen.

Beim Kauf des Routers wird in den meisten Fällen eine IPSec. Lizenz mitgeliefert.

Zu dieser Lizenz erhalten Sie drei Nummern:

- Type of license
- LicenseSerialNumber
- PIN-code

Die LicenseSerialNumber und den PIN-code benötigen Sie, um auf der Internetseite der Firma Bintec den Lizenzschlüssel zu generieren.

Starten Sie über Ihren Internet Explorer die Internet Seite der Firma Bintec [www.bintec.de](http://www.bintec.de) .



## 2.3.1 Lizenzschlüssel generieren

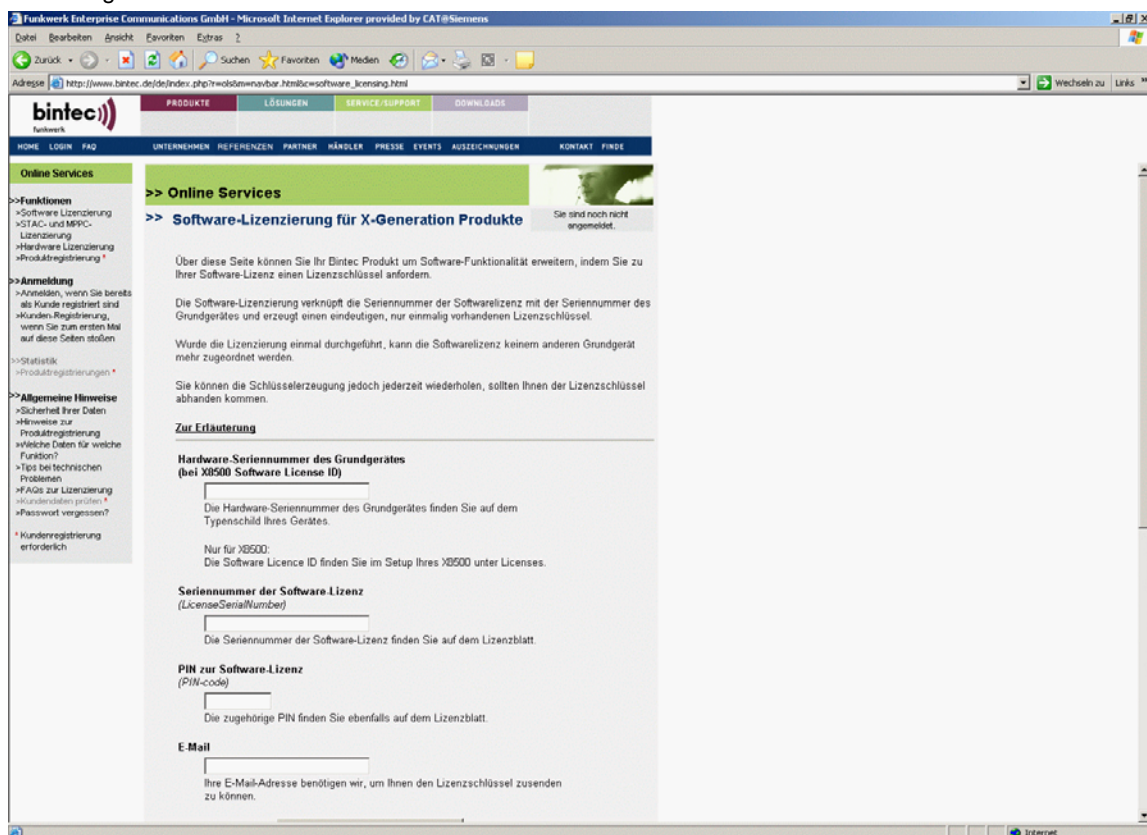
Von der Startseite der Firma Bintec, gehen Sie auf den Register Service/Support.

An dieser Stelle finden Sie den Eintrag **Online Services**, darunter klicken Sie auf **Lizenzierung**.

Sie befinden sich nun auf der hier aufgezeigten Seite und können die geforderten Daten eintragen.

Dieser Vorgang kann u.U. bei jedem Hersteller anders gelöst sein.

Abbildung 2-2



Über diese Seite können Sie auch Ihr Bintec Produkt um Software-Funktionalität erweitern, indem Sie zu Ihrer Software-Lizenz einen Lizenzschlüssel anfordern.

Die Software-Lizenzierung verknüpft die Seriennummer der Softwarelizenz mit der Seriennummer des Grundgerätes und erzeugt einen eindeutigen, nur einmalig vorhandenen Lizenzschlüssel. Wurde die Lizenzierung einmal durchgeführt, kann die Softwarelizenz keinem anderen Grundgerät mehr zugeordnet werden. Sie können die Schlüsselerzeugung jedoch jederzeit wiederholen, sollten Ihnen der Lizenzschlüssel abhanden kommen.

Sie benötigen zur Software-Lizenzierung:

- Die Hardware-Seriennummer des Grundgerätes, die Sie auf dem Typenschild Ihres Gerätes finden, bzw. bei X8500 die Software License ID aus dem Setup-Menü
- Die Seriennummer der Softwarelizenz
- Die PIN zur Ihrer Absicherung, damit die von Ihnen gekaufte Lizenz auch Ihnen zugeordnet wird, z.B. für Support.  
Die PIN erhalten Sie zusammen mit der Seriennummer der Softwarelizenz.

Ihnen wird der Lizenzschlüssel auf der Webseite angezeigt und parallel dazu erhalten Sie von der Firma Bintec eine Benachrichtigung per E-Mail.

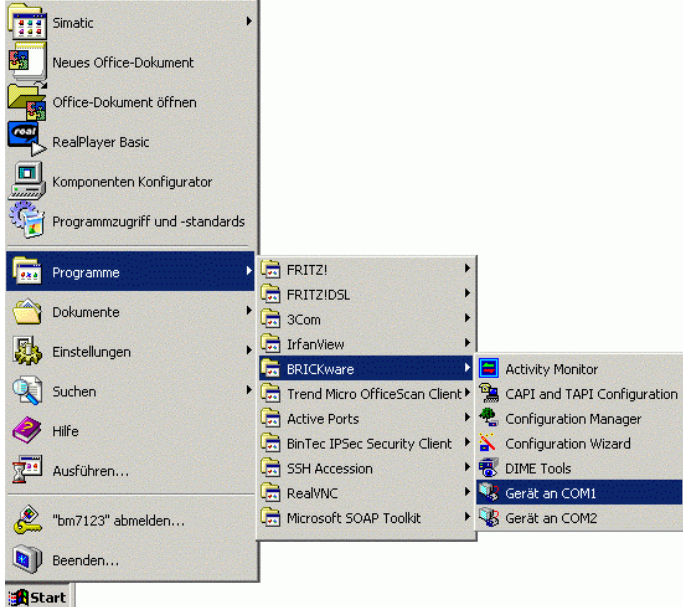
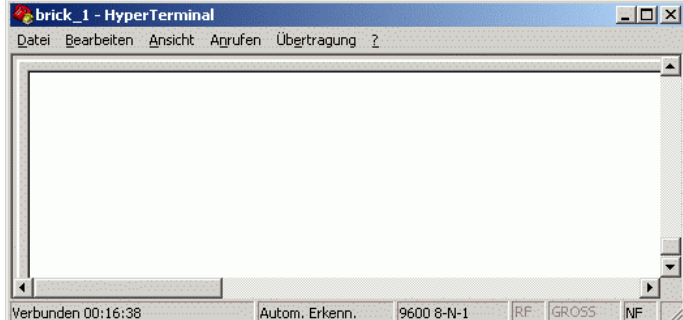
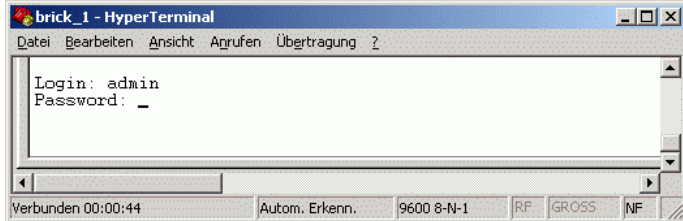
Dieser Schlüssel wird nun in Ihrem Router konfiguriert, um die Software-Funktionalität frei zu schalten.

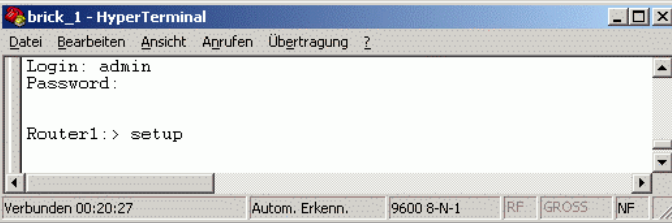
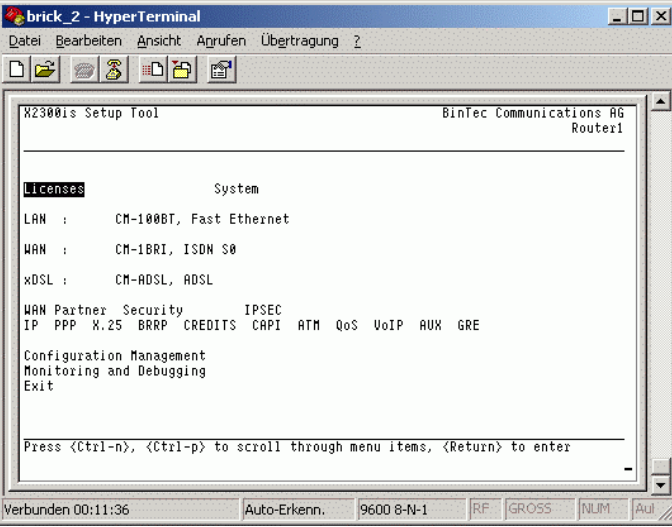
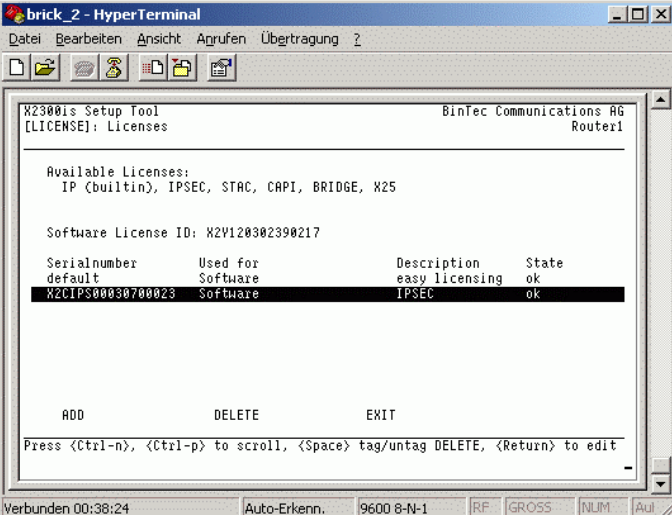
Hinweise dazu finden Sie auch in den FAQs der Firma Bintec.

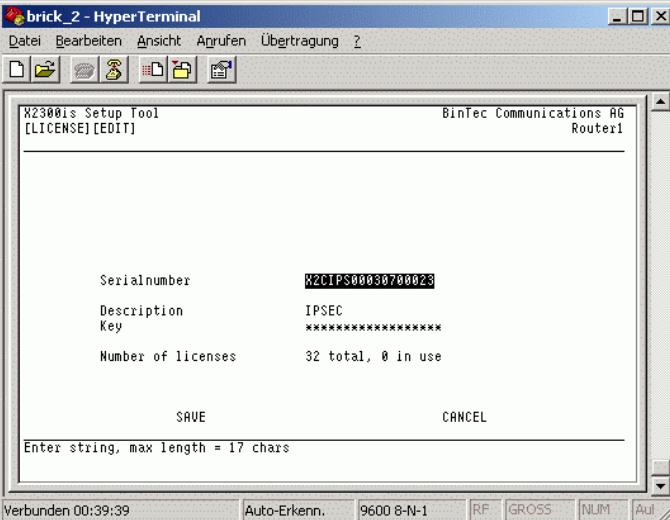
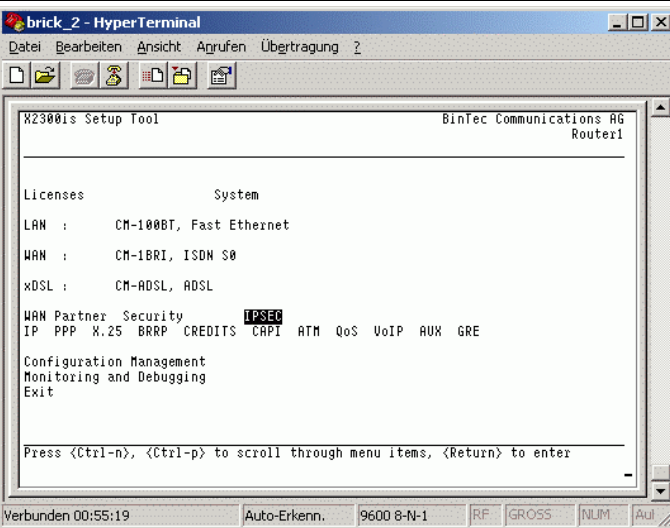
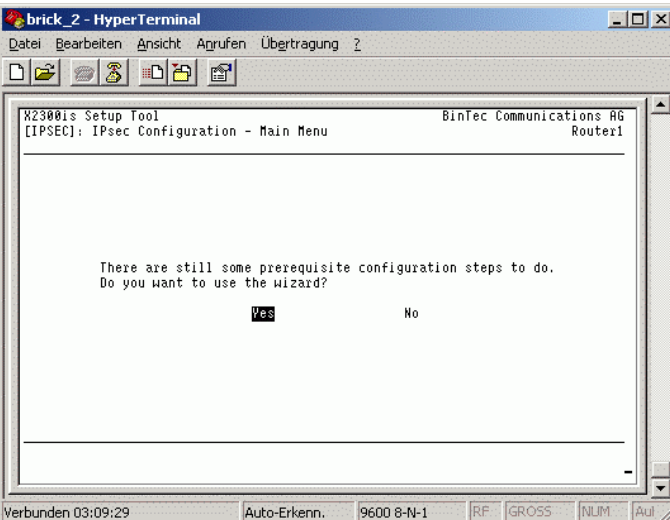
Um die Lizenzschlüssel einzutragen, starten Sie wieder das Setup Tool der Firma Bintec und öffnen das Menü **Licenses**.

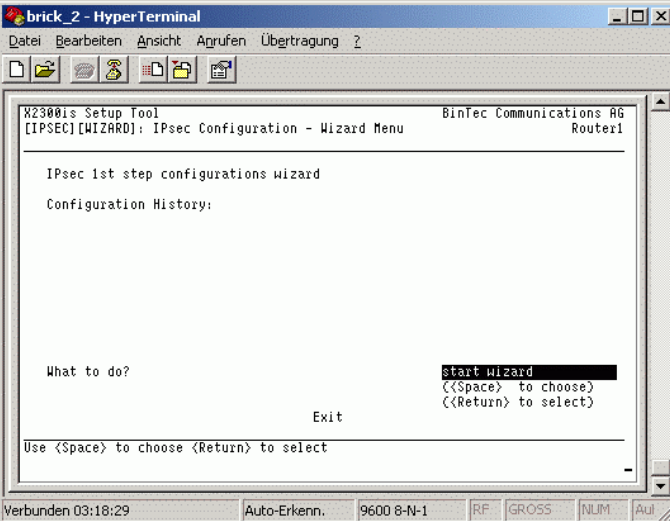
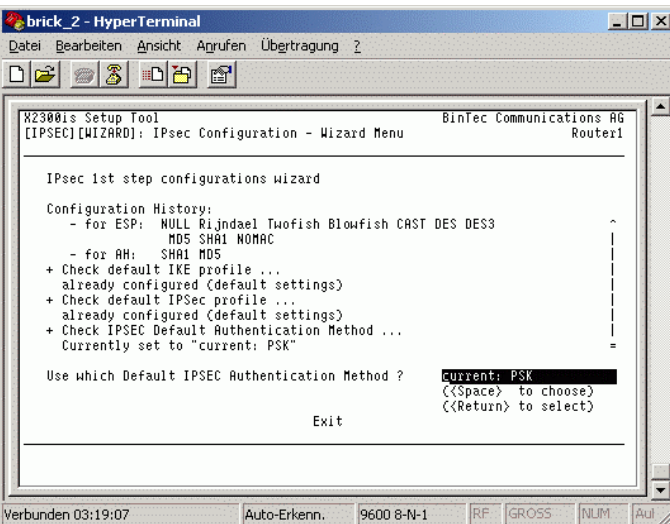
## 2.3.2 Einrichten von VPN über das Setup Tool

Tabelle 2-1

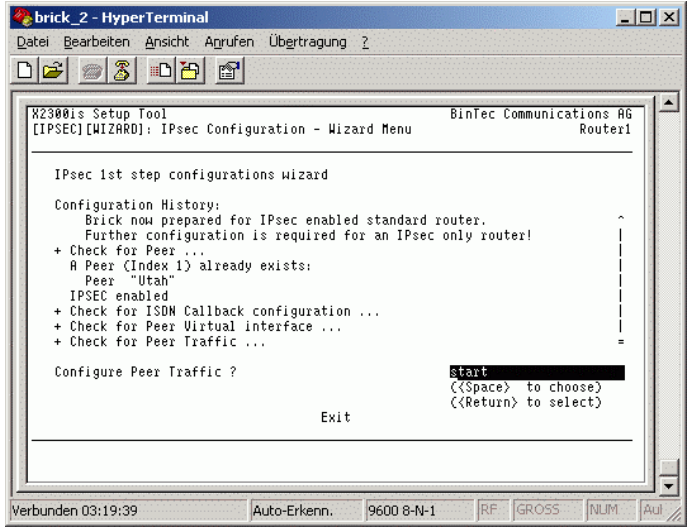
Nr.	Aktion	Anmerkung
1	<p>Die bereits installierte BRICKware der Firma Bintec beinhaltet schon zwei vordefinierte Verbindungen zu Ihrem Router.</p> <p>Je nach verwendeter COM Schnittstelle, wählen Sie nun eine Verbindung aus und es öffnet sich der Windows Hyper Terminal.</p> <p>Start &gt; Programme &gt; BRICKware &gt; <b>Gerät an COM1</b></p>	
2	<p>Hyper Terminal Weiter mit <b>ENTER</b>.</p>	
3	<p>Nach Betätigung der Eingabetaste erscheint ein Anmeldeprompt, in dem Sie die in Ihrer Grundkonfiguration festgelegten Benutzerdaten eintragen.</p> <p>Als <b>Login</b> tragen Sie beispielsweise <b>admin</b> ein und nach betätigen der Entertaste das zugehörige <b>Passwort</b>.</p>	

4	Nach der Anmeldung geben Sie <b>setup</b> ein und gelangen damit in das Setup Tool.													
5	Setup Tool. Öffnen Sie das Menü <b>Licenses</b> .													
6	An dieser Stelle finden Sie schon eine Default Lizenz und können nun über den Punkt <b>ADD</b> Ihre IPSec Schlüsselnummern eintragen.	 <table border="1" data-bbox="710 1361 1316 1422"> <thead> <tr> <th>Serialnumber</th> <th>Used for</th> <th>Description</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>default</td> <td>Software</td> <td>easy licensing</td> <td>ok</td> </tr> <tr> <td>XZCIPS00030700023</td> <td>Software</td> <td>IPSEC</td> <td>ok</td> </tr> </tbody> </table>	Serialnumber	Used for	Description	State	default	Software	easy licensing	ok	XZCIPS00030700023	Software	IPSEC	ok
Serialnumber	Used for	Description	State											
default	Software	easy licensing	ok											
XZCIPS00030700023	Software	IPSEC	ok											

<p>7</p>	<p>Tragen Sie die Seriennummer und den im Internet generierten Schlüssel ein, um die IPsec-Funktionalitäten freizuschalten.</p> <p>Beenden Sie den Dialog mit <b>Save</b> und kehren Sie zum Hauptmenu zurück.</p>	
<p>8</p>	<p>In Ihrem Hauptmenu finden Sie nun einen neuen Auswahlpunkt <b>IPSEC</b>. Starten Sie <b>IPSec</b>.</p>	
<p>9</p>	<p>Mit dem Wizard legen Sie die Grundeinstellungen für Ihre VPN IPsec Verbindungen in Ihrem Firmennetzwerk fest.</p> <p>Bestätigen Sie mit <b>Yes</b>.</p>	

<p>10</p>	<p>Wählen Sie hier <b>start wizard</b>.</p>	 <pre> X2300is Setup Tool                               BinTec Communications AG [IPSEC][WIZARD]: IPsec Configuration - Wizard Menu Router1  IPsec 1st step configurations wizard  Configuration History:  What to do?                                     start wizard   ((\$pace) to choose)   ((\$Return) to select)  Exit  Use &lt;Space&gt; to choose &lt;Return&gt; to select     </pre>
<p>11</p>	<p>Zunächst wählen Sie die Identifizierungsmethode, die Sie verwenden möchten.</p> <p>In diesem Beispiel wurde PSK (Pre-shared Key) ausgewählt.</p> <p>Durch dieses Verfahren werden bei beiden Verbindungspartnern die gleichen Schlüsseldaten eingetragen und somit kann eine Identifizierung stattfinden.</p>	 <pre> X2300is Setup Tool                               BinTec Communications AG [IPSEC][WIZARD]: IPsec Configuration - Wizard Menu Router1  IPsec 1st step configurations wizard  Configuration History: - for ESP:  NULL Rijndael Twofish Blowfish CAST DES DES3              MD5 SHA1 NOMAC - for AH:   SHA1 MD5 + Check default IKE profile ...   already configured (default settings) + Check default IPsec profile ...   already configured (default settings) + Check IPSEC Default Authentication Method ...   Currently set to "current: PSK"  Use which Default IPSEC Authentication Method ?  current: PSK   ((\$pace) to choose)   ((\$Return) to select)  Exit     </pre>



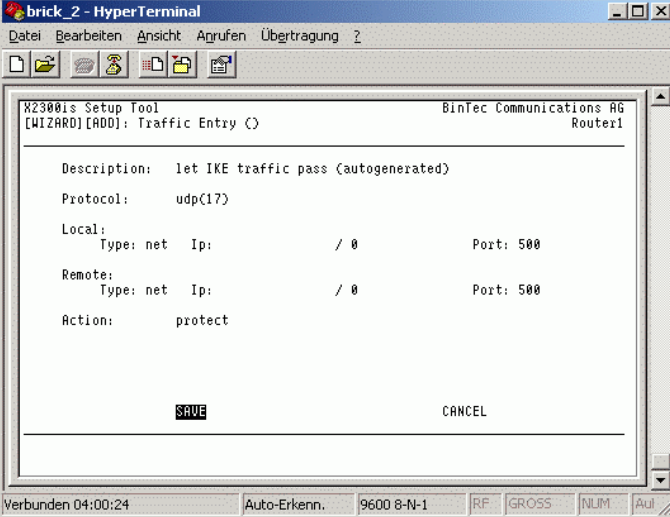
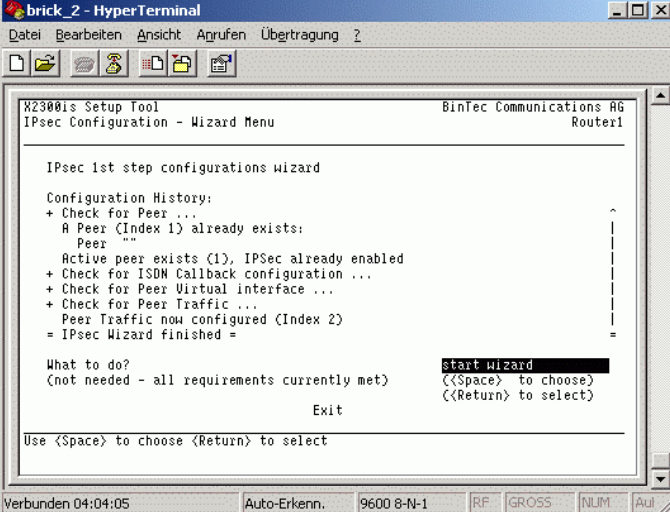
<p>12</p>	<p>Nach dieser Auswahl muss am Router eine Default Route über UDP Protokoll Port 500 erstellt werden, über die die Schlüsseldaten zwischen den Routern ausgetauscht und verglichen werden können.</p> <p><b>Hinweis:</b>          UDP ist die Abkürzung für User Datagram Protocol. Es bezeichnet ein Übertragungsprotokoll.          Es kann anstatt des TCP auf Basis des IP-Protokolls verwendet werden.          UDP arbeitet nicht Verbindungsorientiert. Das bedeutet, ein UDP Datenpaket kann auch ohne eine bestehende Verbindung gesendet werden.</p>
<p>13</p>	<p>Bestätigen Sie <b>Start</b> mit Enter. Nach dem Start, nehmen Sie die nachfolgend in der Tabelle aufgeführten Einstellungen vor.</p> <p>Die Description ist immer frei wählbar und sollte nach der Funktionalität der Verbindung benannt werden.          Mit der Default Route wird den Routern oder PC-Clients ermöglicht, über IKE die Verbindungsparameter auszutauschen.</p> 

### 2.3.3 Internet Key Exchange

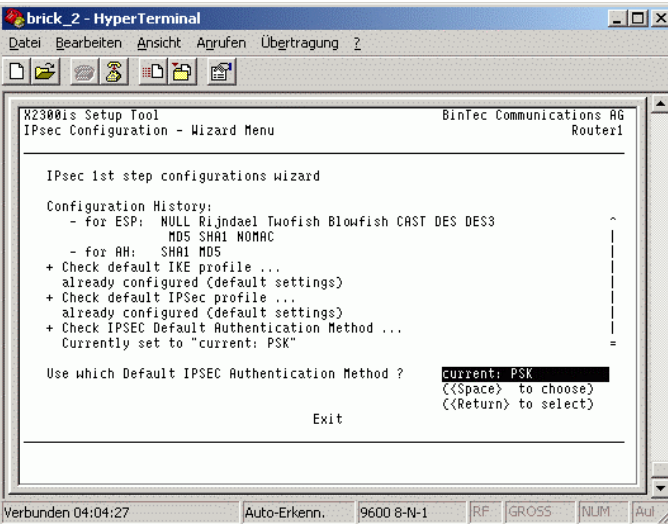
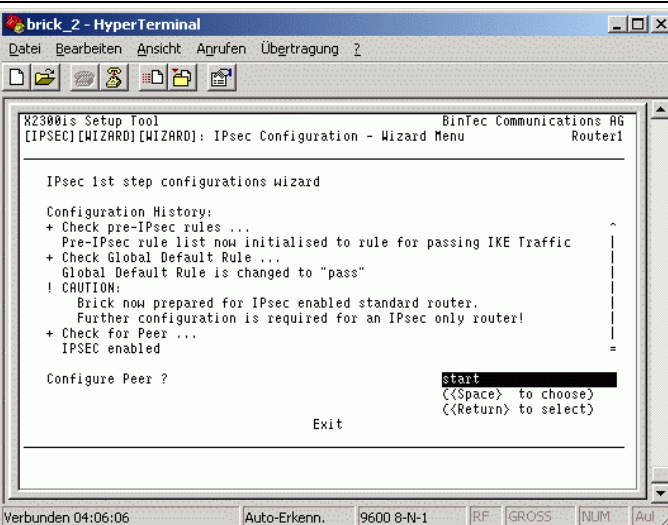
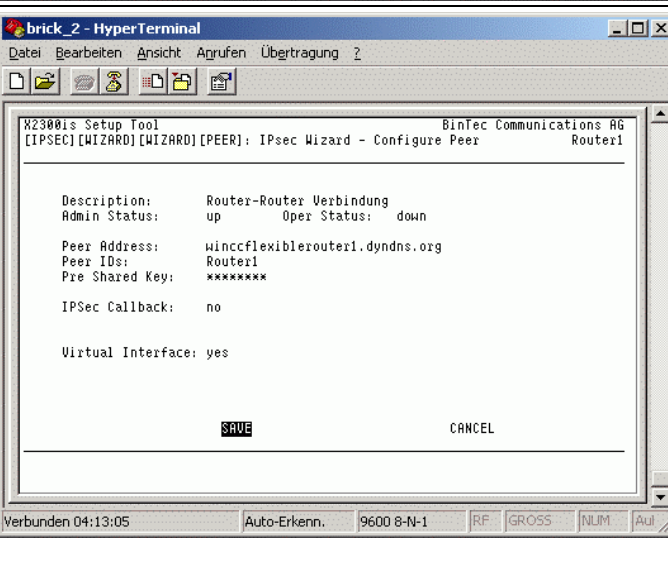
Internet Key Exchange (IKE) ist ein Protokoll, das der Verwaltung von Security Associations innerhalb von mit IPSec realisierten VPN Verbindungen dient.

IKE wird gebraucht, da IPSec die zur Verschlüsselung notwendigen Informationen (Algorithmen, Schlüssel, Gültigkeitsdauer etc.) nicht selbst überträgt, sondern sie aus einer lokalen SAD (Security Association Database Tabelle aller aktiven Security Associations auf einem Rechner der zu einem VPN nach IPSec Richtlinien gehört.) nimmt.

Tabelle 2-2

Nr.	Aktion	Anmerkung
14	Bestätigen Sie die Eingabe mit <b>Save</b> und fahren Sie mit dem Wizard fort.	
15	Schalten Sie auf <b>Start Wizard</b> um, damit Sie die einzelnen Routen zu Ihren Netzwerkteilnehmern aufbauen können.	



<p>16</p>	<p>Wählen Sie jetzt wieder die Verschlüsselung über <b>Current: PSK</b> (Pre-shared Key) aus.</p>	 <pre> X2300is Setup Tool                               BinTec Communications AG IPsec Configuration - Wizard Menu                 Router1  IPsec 1st step configurations wizard  Configuration History: - for ESP:  NULL Rijndael Twofish Blowfish CAST DES DES3 - for AH:   SHA1 MD5 + Check default IKE profile ... already configured (default settings) + Check default IPsec profile ... already configured (default settings) + Check IPSEC Default Authentication Method ... Currently set to "current: PSK"  Use which Default IPSEC Authentication Method ?  current: PSK   ((\$space) to choose)   ((\$Return) to select)  Exit     </pre>
<p>17</p>	<p>Die Konfiguration der ersten Partnerinstanz startet.  Bestätigen Sie <b>Start</b> mir Enter.</p>	 <pre> X2300is Setup Tool                               BinTec Communications AG [IPSEC] [WIZARD] [WIZARD]: IPsec Configuration - Wizard Menu  Router1  IPsec 1st step configurations wizard  Configuration History: + Check pre-IPsec rules ... Pre-IPsec rule list now initialised to rule for passing IKE Traffic + Check Global Default Rule ... Global Default Rule is changed to "pass" ! CAUTION:   Brick now prepared for IPsec enabled standard router.   Further configuration is required for an IPsec only router! + Check for Peer ... IPSEC enabled  Configure Peer ?                                start   ((\$space) to choose)   ((\$Return) to select)  Exit     </pre>
<p>18</p>	<p>Die hier abgebildeten Einstellungen sind ebenfalls beim Partner einzutragen. Nur die <b>Peer Adress</b> und die <b>Peer ID</b> unterscheiden sich.</p>	 <pre> X2300is Setup Tool                               BinTec Communications AG [IPSEC] [WIZARD] [WIZARD] [PEER]: IPsec Wizard - Configure Peer  Router1  Description:      Router-Router Verbindung Admin Status:    up      Oper Status:  down  Peer Address:    winccflexiblerouter1.dyndns.org Peer IDs:        Router1 Pre Shared Key:  *****  IPSec Callback:  no  Virtual Interface: yes  SAVE                                CANCEL     </pre>

19 **Hinweis:**

Die Parameter sind frei gewählt und können meistens aus bis zu 50 Zeichen bestehen. Konfigurieren Sie zuerst die Router --> Router Verbindung. Sie benötigen dazu im einzelnen die folgenden Informationen:

- Name des Partners im Internet, falls die IP-Adresse, wie in unserem Beispiel immer dynamisch ist (Peer Address)
- Der lokalen Namen des Partners (Peer ID)
- Der Verbindungsname (Description) und der Pre Shared Key müssen bei beiden Teilnehmern gleich eingestellt sein.

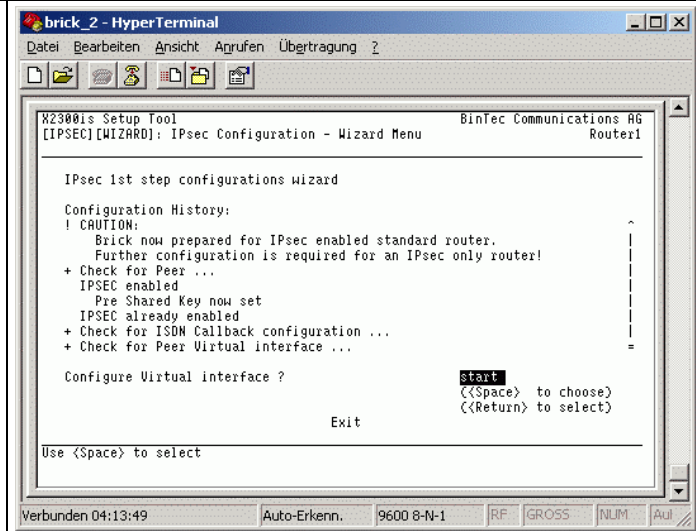
Der Pre Shared Key (PSK) muss zweimal hintereinander eingegeben werden, um die Eingabe sichern zu können.

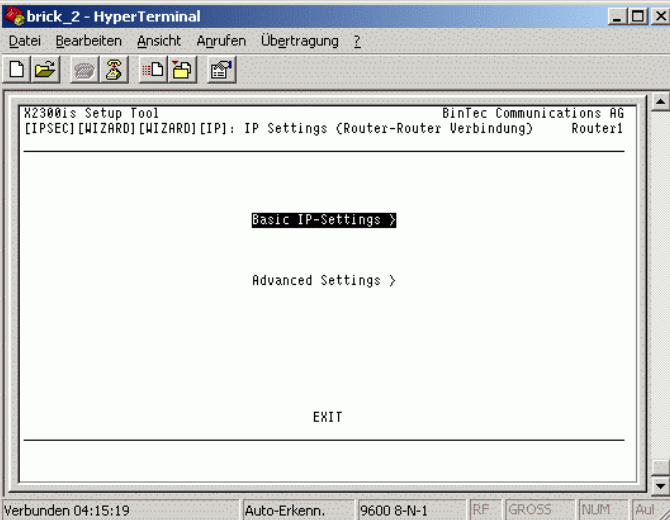
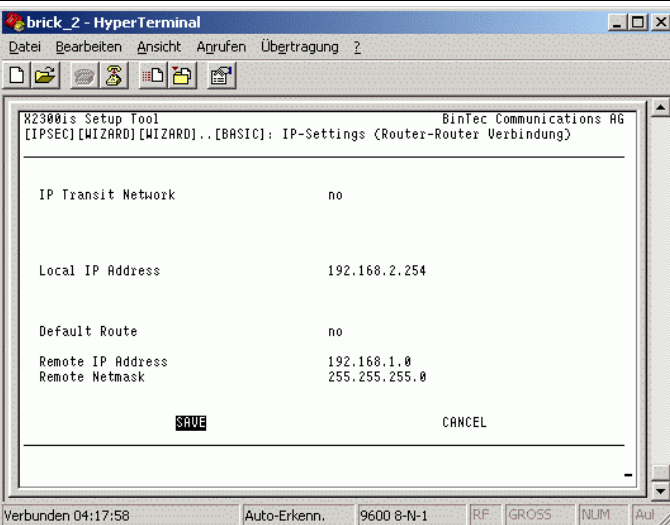
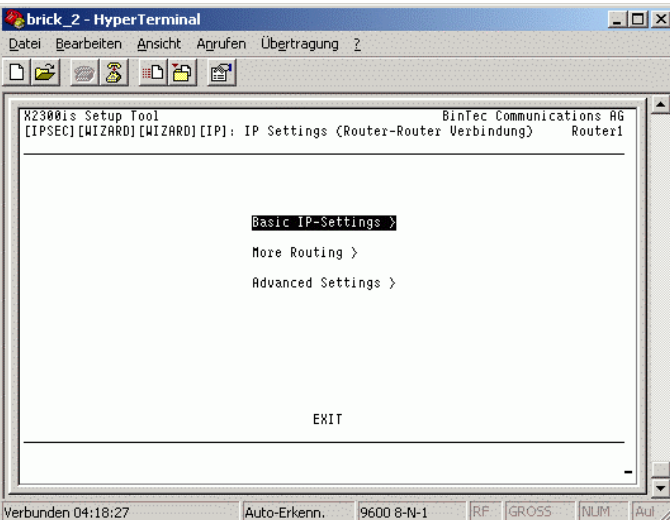
Wenn Sie eine Verbindung zwischen zwei Routern aufbauen und an Ihrem Router ISDN und DSL gleichzeitig angeschlossen ist, dann können Sie die Funktion ISDN Callback nutzen.

Die Funktion sorgt bei Ausfall der DSL Leitung für einen neuen IPSec Tunnel über die ISDN Leitung. Dies schafft eine größere Sicherheit für Ihren Datenaustausch.

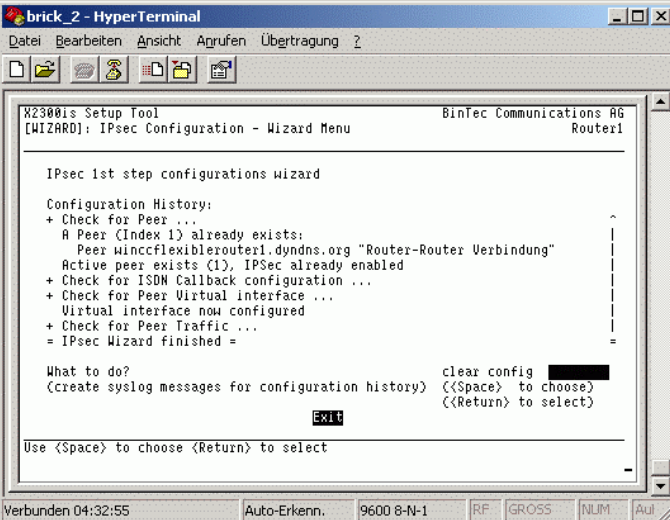
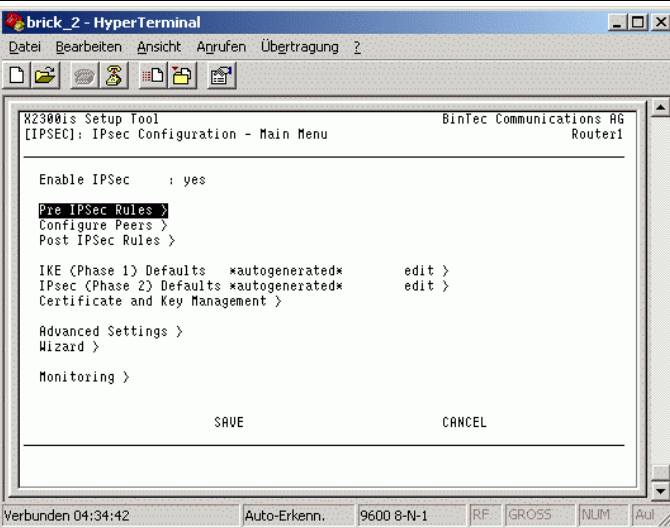
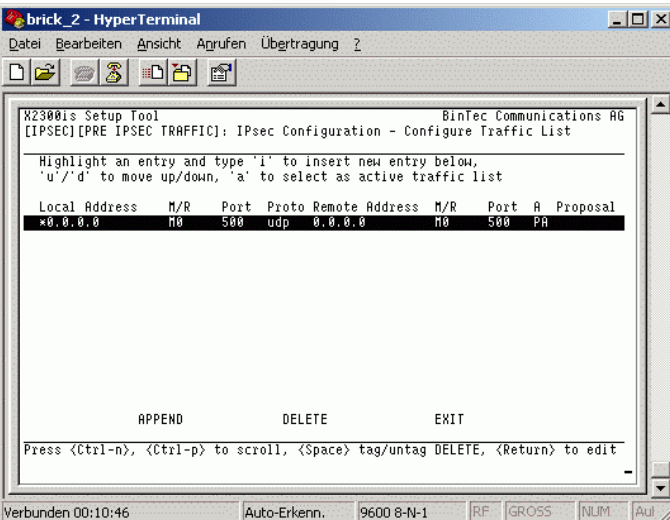
Wenn Sie den Callback nutzen möchten, muss dieser auch auf beiden Seiten eingeschaltet werden.

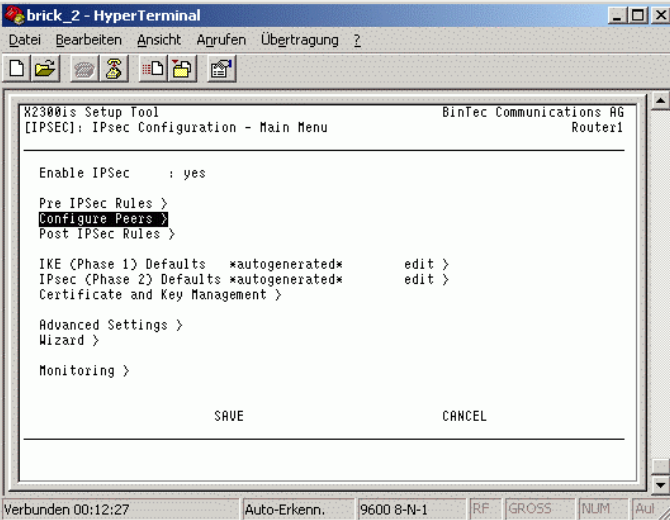
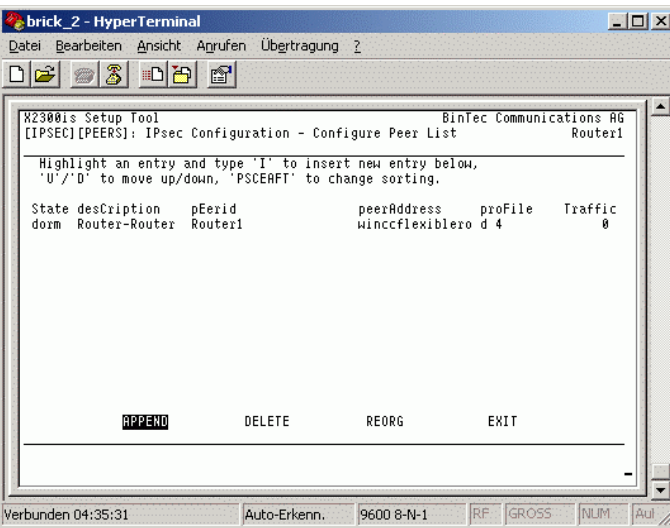
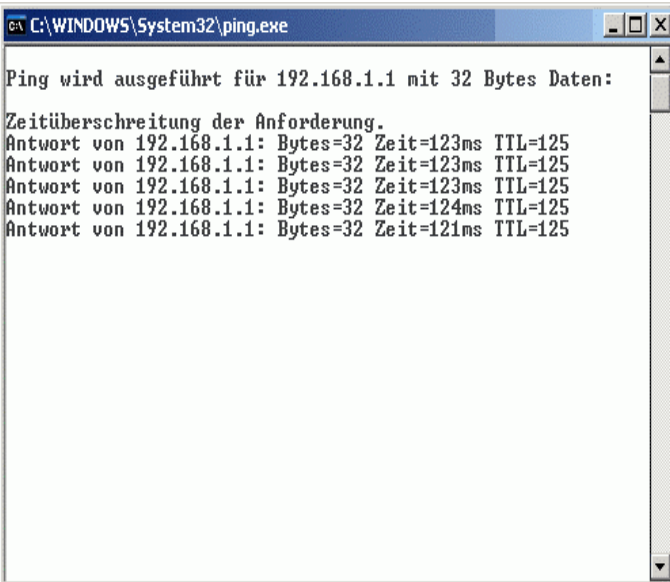
20 Zu der jetzt erstellten Route werden noch einige Verbindungsdaten vom Partnernetz eingetragen.



<p>21</p>	<p>Unter <b>Basic IP-Settings</b> tragen Sie die Werte Ihres Partnernetzes ein.</p>	 <p>The screenshot shows a HyperTerminal window titled 'brick_2 - HyperTerminal'. The main window displays the 'X2300is Setup Tool' interface. At the top, it says 'BinTec Communications AG [IPSEC] [WIZARD] [WIZARD] [IP]: IP Settings (Router-Router Verbindung) Router1'. The main menu has three options: 'Basic IP-Settings &gt;', 'Advanced Settings &gt;', and 'EXIT'. The 'Basic IP-Settings' option is highlighted with a mouse cursor.</p>										
<p>22</p>	<p>Sie benötigen dafür nur die Startadresse und die Subnetmask. Damit kann der Router erkennen, wie groß das IP-Band des Partnernetzes ist.</p>	 <p>The screenshot shows the same HyperTerminal window. The main window displays the configuration details for 'IP Settings (Router-Router Verbindung)'. The settings are as follows:</p> <table border="1"> <tr> <td>IP Transit Network</td> <td>no</td> </tr> <tr> <td>Local IP Address</td> <td>192.168.2.254</td> </tr> <tr> <td>Default Route</td> <td>no</td> </tr> <tr> <td>Remote IP Address</td> <td>192.168.1.0</td> </tr> <tr> <td>Remote Netmask</td> <td>255.255.255.0</td> </tr> </table> <p>At the bottom of the configuration screen, there are 'SAVE' and 'CANCEL' buttons. The 'SAVE' button is highlighted.</p>	IP Transit Network	no	Local IP Address	192.168.2.254	Default Route	no	Remote IP Address	192.168.1.0	Remote Netmask	255.255.255.0
IP Transit Network	no											
Local IP Address	192.168.2.254											
Default Route	no											
Remote IP Address	192.168.1.0											
Remote Netmask	255.255.255.0											
<p>23</p>	<p>Nach dieser Eingabe wurde schon automatisch eine Routingstrecke erstellt, die Sie unter dem Menüpunkt <b>More Routing</b> nochmals kontrollieren können.</p>	 <p>The screenshot shows the same HyperTerminal window. The main window displays the 'X2300is Setup Tool' interface. At the top, it says 'BinTec Communications AG [IPSEC] [WIZARD] [WIZARD] [IP]: IP Settings (Router-Router Verbindung) Router1'. The main menu has three options: 'Basic IP-Settings &gt;', 'More Routing &gt;', and 'Advanced Settings &gt;'. The 'More Routing &gt;' option is highlighted with a mouse cursor.</p>										

<p>24</p>	<p>Öffnen Sie mit der Enter Taste den schon bestehenden Beitrag.</p>	
<p>25</p>	<p>Wenn Sie den Dialog mit <b>Cancel</b> verlassen haben, können Sie noch den Punkt <b>Advanced Settings</b> bearbeiten. (-&gt; Siehe Punkt 20)</p> <p>An dieser Stelle ist es jedoch nicht notwendig gewesen die Standard Einstellungen zu verändern.</p>	
<p>26</p>	<p>Damit ist die Grundkonfiguration beendet und es können entweder direkt im Menü oder durch einen erneuten Start des Wizards weitere Verbindungen erstellt werden.</p> <p>Die Erstellung der Default Route über UDP Port 500 wird dabei nicht noch einmal durchlaufen.</p> <p>Die Verbindung zwischen zwei Netzwerken ist an dieser Stelle abgeschlossen.</p> <p>Weiter mit <b>OK</b>.</p>	

<p>27</p>	<p>Verlassen des Menüs mit <b>Exit</b>.</p>	 <pre> X2300is Setup Tool                               BinTec Communications AG [WIZARD]: IPsec Configuration - Wizard Menu       Router1  IPsec 1st step configurations wizard  Configuration History: + Check for Peer ...   A Peer (Index 1) already exists:   Peer winccflexiblerouter1.dyndns.org "Router-Router Verbindung"   Active peer exists (1). IPsec already enabled + Check for ISDN Callback configuration ... + Check for Peer Virtual interface ...   Virtual interface now configured + Check for Peer Traffic ... = IPsec Wizard finished =  What to do?                                     clear config [REDACTED] (Create syslog messages for configuration history) (&lt;Space&gt; to choose)   (&lt;Return&gt; to select)  Exit Use &lt;Space&gt; to choose &lt;Return&gt; to select     </pre>
<p>28</p>	<p>Unter dem Menüpunkt <b>Pre IPsec Rules</b> finden Sie Ihre Defaultroute über UDP, die Sie mit dem Wizard angelegt haben.</p>	 <pre> X2300is Setup Tool                               BinTec Communications AG [IPSEC]: IPsec Configuration - Main Menu         Router1  Enable IPsec      : yes  Pre IPsec Rules &gt; Configure Peers &gt; Post IPsec Rules &gt;  IKE (Phase 1) Defaults *autogenerated*      edit &gt; IPsec (Phase 2) Defaults *autogenerated*    edit &gt; Certificate and Key Management &gt;  Advanced Settings &gt; Wizard &gt; Monitoring &gt;  SAVE                                CANCEL     </pre>
<p>29</p>	<p>Default Route</p>	 <pre> X2300is Setup Tool                               BinTec Communications AG [IPSEC][PRE IPSEC TRAFFIC]: IPsec Configuration - Configure Traffic List  Highlight an entry and type 'I' to insert new entry below, 'u'/'d' to move up/down, 'a' to select as active traffic list  Local Address  M/R  Port  Proto Remote Address  M/R  Port  A  Proposal *0.0.0.0      n0   500   udp   0.0.0.0         n0   500   PA  APPEND                                DELETE                                EXIT  Press &lt;Ctrl-n&gt;, &lt;Ctrl-p&gt; to scroll, &lt;Space&gt; tag/untag DELETE, &lt;Return&gt; to edit     </pre>

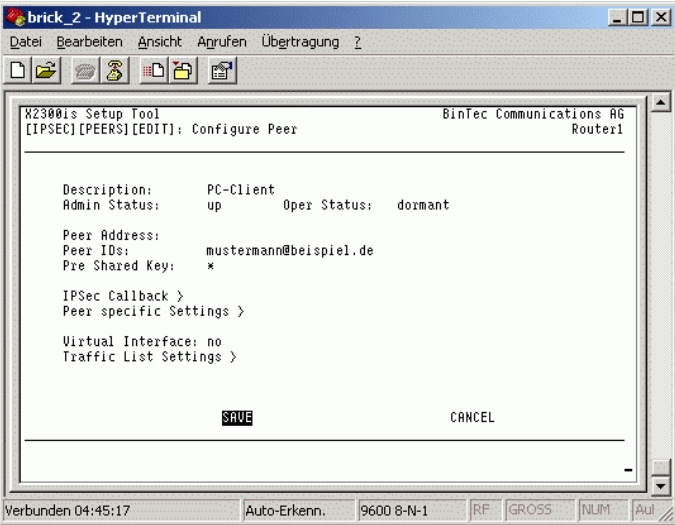
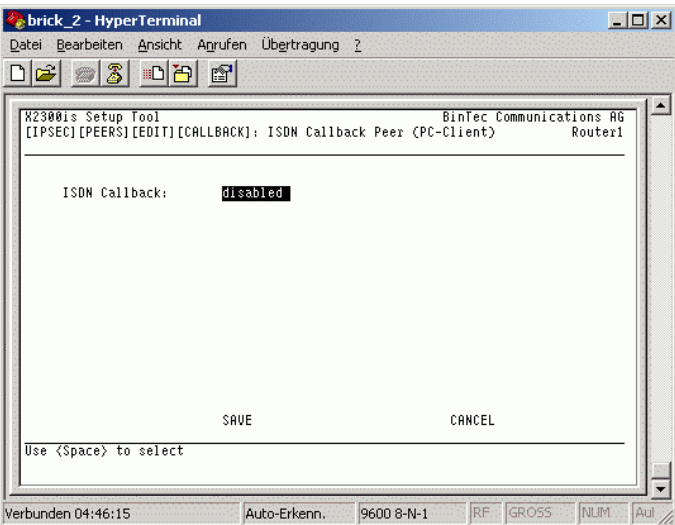
<p>30</p>	<p>Im Menüpunkt <b>Configure Peers</b> legen Sie alle von Ihnen benötigten Verbindungen zu Ihren Partnernetzen fest.</p>	
<p>31</p>	<p>Die bereits projektierte Verbindung zwischen Ihren Routern ist schon in diesem Menü vorhanden. Fügen Sie jetzt noch die PC-Client Verbindung hinzu, um Ihrem Servicemitarbeiter den Zugriff auf Ihr lokales Netzwerk zu ermöglichen.  Betätigen Sie dazu <b>APPEND</b>, um den neuen Eintrag zu erstellen.  Betätigen Sie <b>EXIT</b>, um die Einstellungen zu verlassen.</p>	
<p>32</p>	<p><b>Hinweis:</b> Auf dem zweiten Router müssen die Einstellungen identisch vorgenommen werden. Die Verbindung zwischen den Routern kann einfach getestet werden, indem ein Teilnehmer des einen lokalen Netzwerkes einen Teilnehmer im Partnernetzwerk anspricht. (z.B. Ping) Die Router handeln dann den IPSec Tunnel aus und danach ist die Verbindung wie in einem geschlossenen Netzwerk möglich. Die erste Zeitüberschreitung entsteht, da der Tunnel noch</p>	

	nicht aufgebaut ist.	
--	----------------------	--

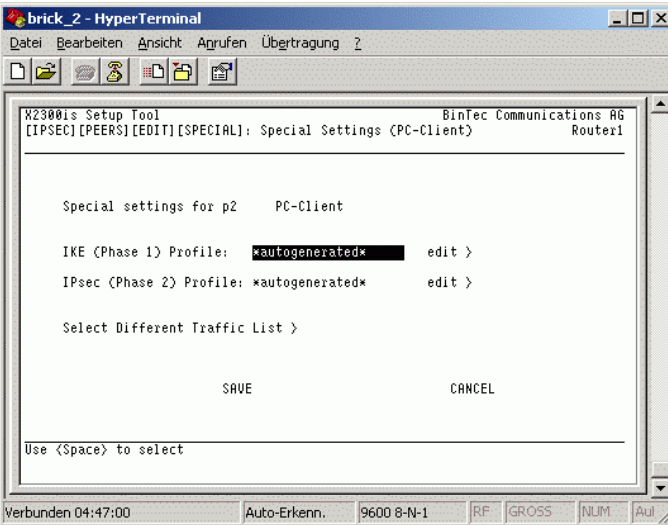
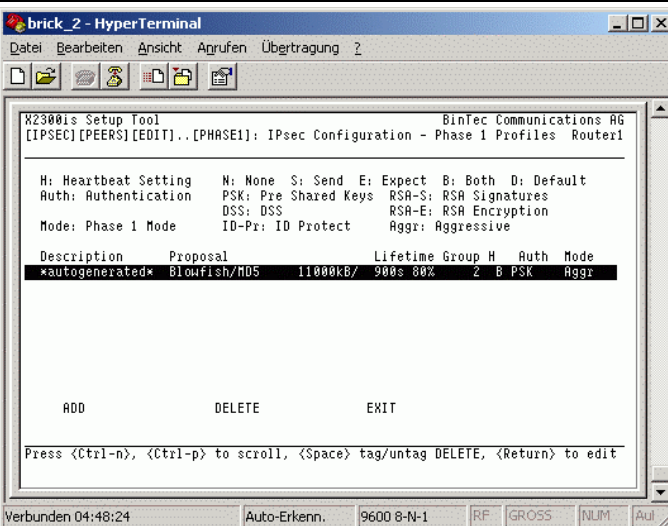


## 2.3.4 Anlegen der PC-Client Partnerverbindung

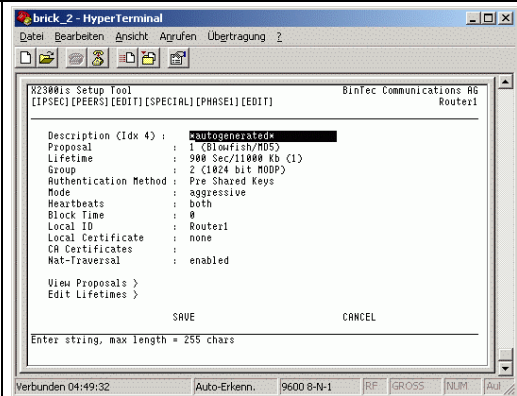
Tabelle 2-3

Nr.	Aktion	Anmerkung
33	<p>Der Name unter <b>Description</b> ist wiederum frei wählbar und für die Verschlüsselung ohne Bedeutung. Den Eintrag zu <b>Peer Address</b> bleibt in diesem Fall frei, da der PC-Client Benutzer in der Regel keine feste IP-Adresse und auch keinen DynDNS Account für seinen Service PC im Internet hat. Als Benutzername <b>Peer IDs</b> verwenden wir eine E-Mail Adresse, da diese eine lange Zeichenkette hat, Sie können aber auch einen beliebigen Namen auswählen. Es ist immer auf beiden Seiten notwendig, die gleichen Parameter zu verwenden. Der <b>Pre Shared Key</b> muss zweimal eingegeben werden, damit er richtig übernommen werden kann.</p>	
34	<p>Der hier gezeigte <b>ISDN Callback</b> ist bei einer PC-Client Verbindung nicht notwendig, da eine Callback Funktion auf dem PC nicht vorhanden ist.</p>	

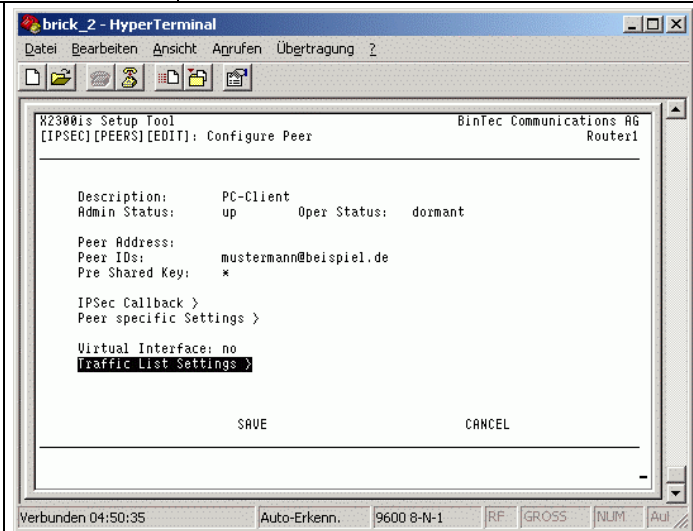


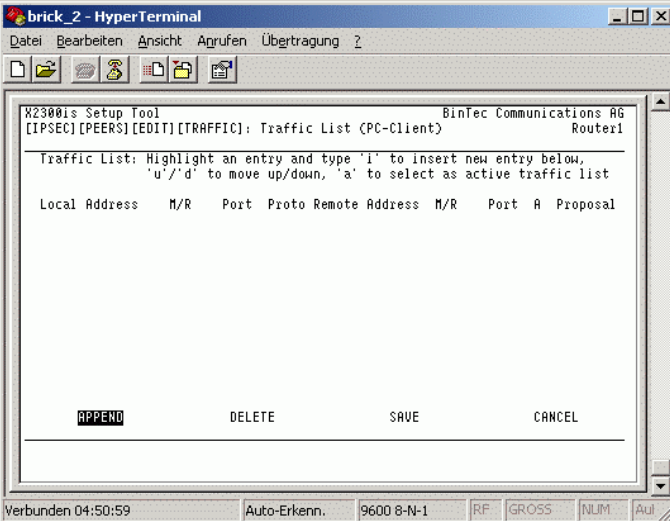
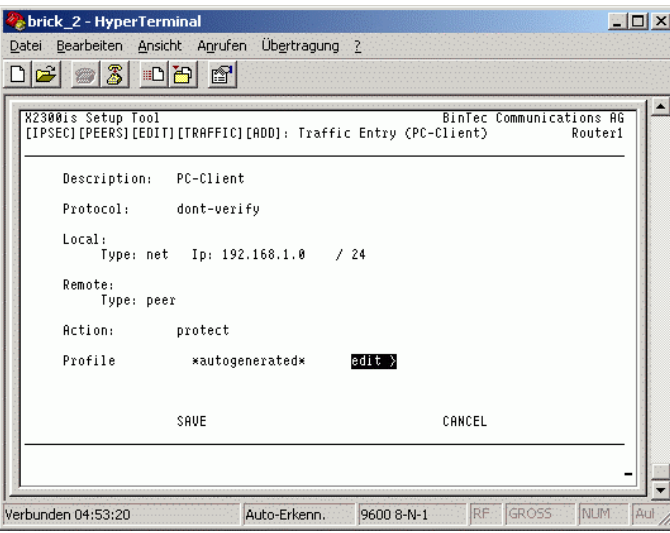
<p>35</p>	<p>Im Menüpunkt <b>Peer specific Settings</b> (Bild 30) finden Sie die Einstellungen für die 1. und 2. Identifizierungsphase. Benutzen Sie die Einstellung <b>autogenerated</b> und somit wählt der Router selbst welche Verschlüsselungsprotokolle er verwendet. Öffnen Sie mit <b>Edit</b> die Einstellungen, da Sie sich diese notieren müssen für die Einstellungen an Ihrem PC-Client.</p>	 <pre> W2300is Setup Tool                               Bintec Communications AG [IPSEC] [PEERS] [EDIT] [SPECIAL]: Special Settings (PC-Client) Router1  Special settings for p2  PC-Client  IKE (Phase 1) Profile: *autogenerated*  edit &gt; IPsec (Phase 2) Profile: *autogenerated*  edit &gt;  Select Different Traffic List &gt;  SAVE                                CANCEL  Use &lt;Space&gt; to select     </pre>
<p>36</p>	<p>Mit <b>Enter</b> können Sie den angewählten Eintrag öffnen, um die Einstellungen zu notieren oder zu ändern.</p>	 <pre> W2300is Setup Tool                               Bintec Communications AG [IPSEC] [PEERS] [EDIT] .. [PHASE1]: IPsec Configuration - Phase 1 Profiles Router1  H: Heartbeat Setting  N: None  S: Send  E: Expect  B: Both  D: Default Auth: Authentication  PSK: Pre Shared Keys  RSA-S: RSA Signatures DSS: DSS              RSA-E: RSA Encryption Mode: Phase 1 Mode    ID-Pr: ID Protect    Aggr: Aggressive  Description  Proposal  Lifetime Group H  Auth  Mode *autogenerated*  Blowfish/MD5  11000kB/ 900s 80%  2  B  PSK  Aggr  ADD                                DELETE                                EXIT  Press &lt;Ctrl-n&gt;, &lt;Ctrl-p&gt; to scroll, &lt;Space&gt; tag/untag DELETE, &lt;Return&gt; to edit     </pre>

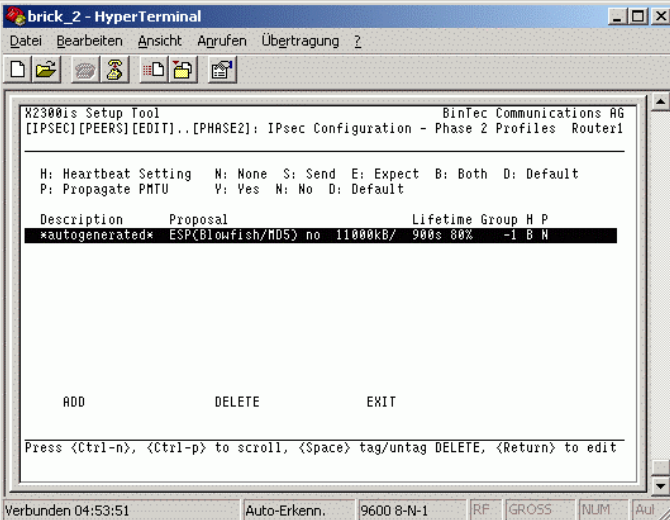
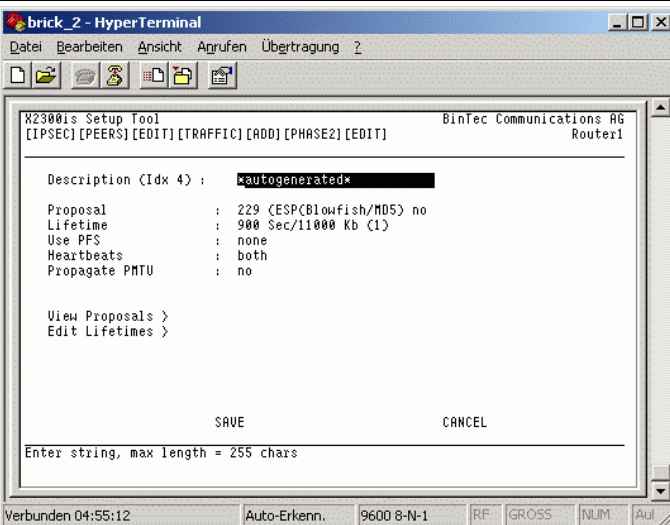
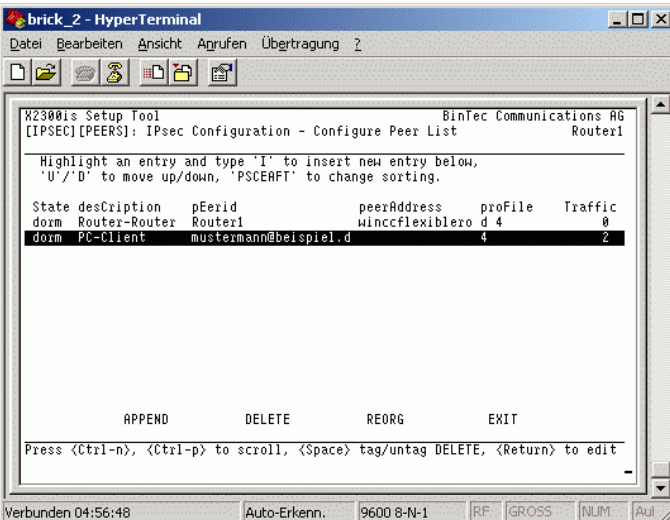
37 Die Einstellungen entsprechen dem Standard, bis auf die Lifetime, die von default auf 900 Sekunden erhöht wurden. Der Router tauscht jetzt die ersten Daten über den Algorithmus Blowfish aus. Die weiteren Algorithmen MD5 und MODP dienen auch der Verschlüsselung und beinhalten die Mechanismen, mit denen die Authentifizierung stattfindet. Da Ihr PC in den meisten Fällen eine dynamische IP-Adresse vom ISP zugewiesen bekommt, muss am Router und am Client der **Aggressive Mode** eingestellt werden. Die **Authentication Method** ist auf das von uns gewählte Verfahren **Pre Shared Keys** einzustellen. Mit den **Heartbeats** Einstellungen legen Sie fest, ob die Verbindung von beiden oder nur einem Teilnehmer kontrolliert wird. Wenn die Lebenszeichen fehlen, kann somit beidseitig der Tunnel schnell abgebaut werden. Die **Block Time** verhindert für eine bestimmte Zeit eine erneute Einwahl, wenn die Schlüssel nicht übereingestimmt haben. Die letzten Einstellungen werden in diesem FAQ nicht behandelt, da es sich hier um eine zusätzliche Zertifizierung handelt. Unter **View Proposals** finden Sie eine Liste mit allen Algorithmen die Sie verwenden können. Als letzten Punkt ist noch **Edit Lifetimes** zu erwähnen, unter dem Sie für Ihre Anforderungen eigene Zeiten definieren können.

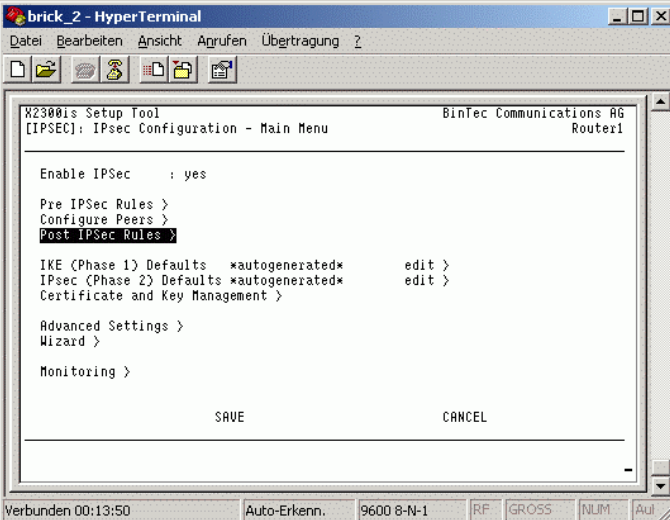
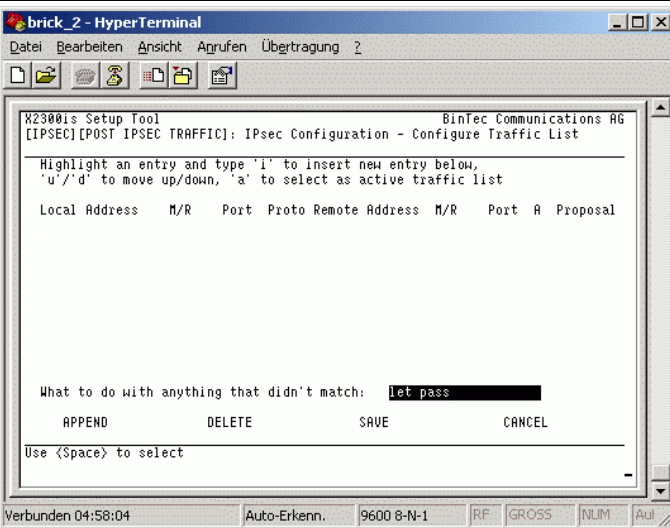
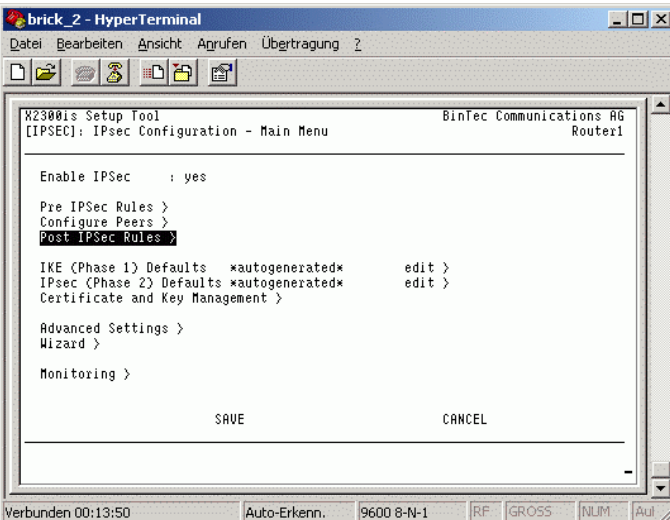


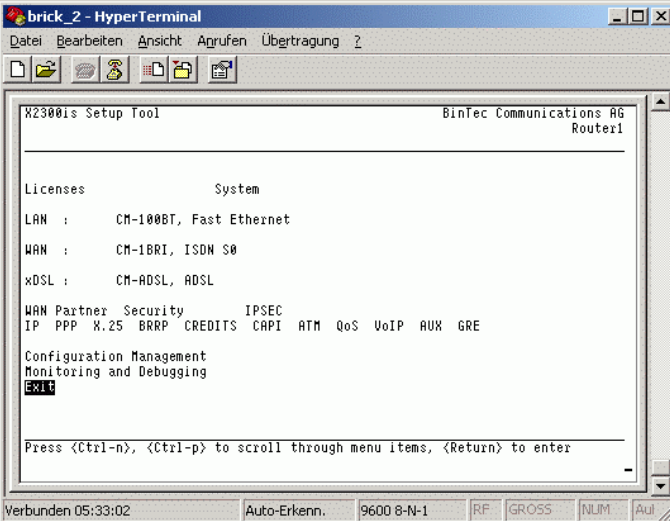
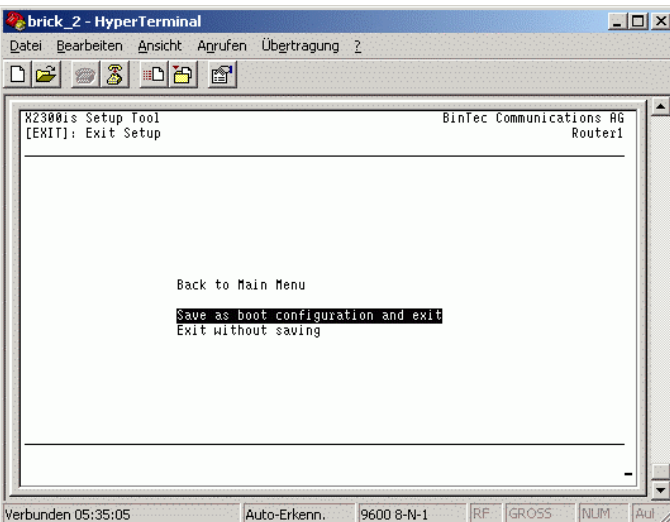
38 Nach dem die Authentifizierung des IPSec Tunnels abgeschlossen ist, müssen Sie noch definieren, welche Teile Ihres Netzwerks der Partner nutzen darf. Dazu benötigen Sie eine **Traffic List**, die Sie unter dem gleichnamigen Menüpunkt erstellen können.



<p>39</p>	<p>Fügen Sie mit <b>APPEND</b> wieder eine neue Liste hinzu.</p>	
<p>40</p>	<p>Damit der PC-Client im Servicefall alle notwendigen Schritte ausführen kann, wurde eine voller Netzwerkzugriff vergeben.</p> <p>Somit ergeben sich die gezeigten Einstellungen. Wählen Sie kein spezielles Protokoll aus, sonder definieren für den Client nur die gesamten IP-Adressen des lokalen Routernetzwerkes. Dazu geben Sie die Startadresse an.</p> <p>Die <b>24</b> sagt aus, dass die Subnetmask 24 Bit benutzt. (255.255.255.0) Die IP-Adresse des Client ist dynamisch. Stellen Sie den <b>Remote Type</b> auf <b>peer</b>, somit nimmt der Router die IP-Adresse mit der sich der Client gemeldet hat als Netzwerkteilnehmer an.</p> <p>Wählen Sie unter dem Eintrag Profile &gt; <b>EDIT</b> aus.</p>	

<p>41</p>	<p>Unter <b>Profile</b> finden Sie wiederum die Einstellungen für die Phase 2, die Sie schon von der Verschlüsselung der ersten Phase her kennen.</p> <p>Öffnen Sie den Eintrag mit <b>Enter</b>.</p>	
<p>42</p>	<p>Nach Bestätigung mit <b>Enter</b> werden die Einstellungen aufgelistet.</p>	
<p>43</p>	<p>Nachdem Sie die Dialoge mit <b>Save</b> abgeschlossen haben, ist Ihre PC-Clientverbindung fertig eingerichtet.</p> <p>Weiter mit <b>EXIT</b>.</p>	

<p>44</p>	<p>Im Menüpunkt <b>Post IPSec Rules</b> müssen Sie kontrollieren, ob der Eintrag <b>What to do with anything that didn't match auf let pass</b> eingestellt ist. Dies bedeutet, dass alles was nicht in den IPSec Rules definiert ist, durchgelassen wird.</p> <p>Weiter mit <b>Enter</b>.</p>	 <pre> brick_2 - HyperTerminal Datei Bearbeiten Ansicht Anrufen Übertragung ? [W2300]s Setup Tool BinTec Communications AG [IPSEC]: IPsec Configuration - Main Menu Router1  Enable IPSec : yes  Pre IPSec Rules &gt; Configure Peers &gt; <b>Post IPSec Rules &gt;</b>  IKE (Phase 1) Defaults *autogenerated* edit &gt; IPsec (Phase 2) Defaults *autogenerated* edit &gt; Certificate and Key Management &gt;  Advanced Settings &gt; Wizard &gt;  Monitoring &gt;  SAVE CANCEL  Verbunden 00:13:50 Auto-Erkenn. 9600 8-N-1 RF GROSS NUMJ AUI     </pre>
<p>45</p>	<p>Kontrolle auf <b>let pass</b>. Damit ist die Konfiguration von IPSec abgeschlossen. Kehren Sie mit <b>Save</b> zurück, um die Einstellungen zu speichern.</p>	 <pre> brick_2 - HyperTerminal Datei Bearbeiten Ansicht Anrufen Übertragung ? [W2300]s Setup Tool BinTec Communications AG [IPSEC][POST IPSEC TRAFFIC]: IPsec Configuration - Configure Traffic List  Highlight an entry and type 'i' to insert new entry below, 'u'/d' to move up/down, 'a' to select as active traffic list  Local Address M/R Port Proto Remote Address M/R Port A Proposal  What to do with anything that didn't match: <b>let pass</b>  APPEND DELETE SAVE CANCEL  Use &lt;Space&gt; to select  Verbunden 04:58:04 Auto-Erkenn. 9600 8-N-1 RF GROSS NUMJ AUI     </pre>
<p>46</p>	<p>Sie befinden sich jetzt wieder im Hauptmenu der IPSec Konfiguration.</p> <p>Verlassen Sie den Dialog wiederum mit <b>SAVE</b>.</p>	 <pre> brick_2 - HyperTerminal Datei Bearbeiten Ansicht Anrufen Übertragung ? [W2300]s Setup Tool BinTec Communications AG [IPSEC]: IPsec Configuration - Main Menu Router1  Enable IPSec : yes  Pre IPSec Rules &gt; Configure Peers &gt; <b>Post IPSec Rules &gt;</b>  IKE (Phase 1) Defaults *autogenerated* edit &gt; IPsec (Phase 2) Defaults *autogenerated* edit &gt; Certificate and Key Management &gt;  Advanced Settings &gt; Wizard &gt;  Monitoring &gt;  SAVE CANCEL  Verbunden 00:13:50 Auto-Erkenn. 9600 8-N-1 RF GROSS NUMJ AUI     </pre>

<p>47</p>	<p>Verlassen Sie das Setup Tool mit <b>EXIT</b>.</p>	
<p>48</p>	<p>Speichern Sie noch einmal alles als Bootkonfiguration ab.</p>	



## 2.4 Einrichtung des IPsec Clients auf dem PC.

Die Einrichtung erfolgt in unserem Beispiel an Hand des SSH Sentinel PC Clients.

Es gibt noch sehr viel mehr Anbieter, jedoch die Authentifizierung und Einstellungen sind bei fast allen ähnlich realisiert.

Die hier beschriebenen Installationsschritte sind eine Erweiterung eines FAQs von der Firma Bintec.

### 2.4.1 Installation der Client Software

Starten Sie die Installation einfach über das auf der CD befindliche Setup.

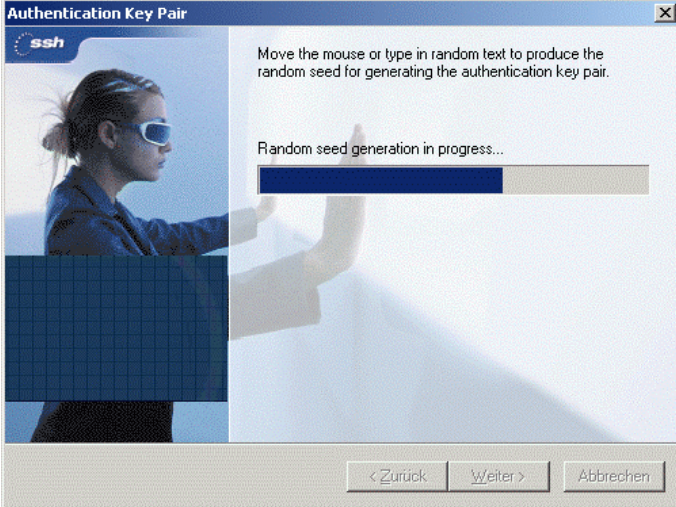
#### Hinweis:

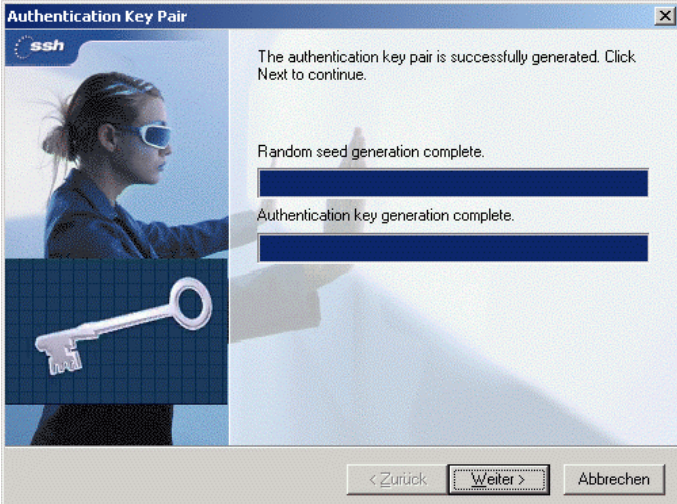
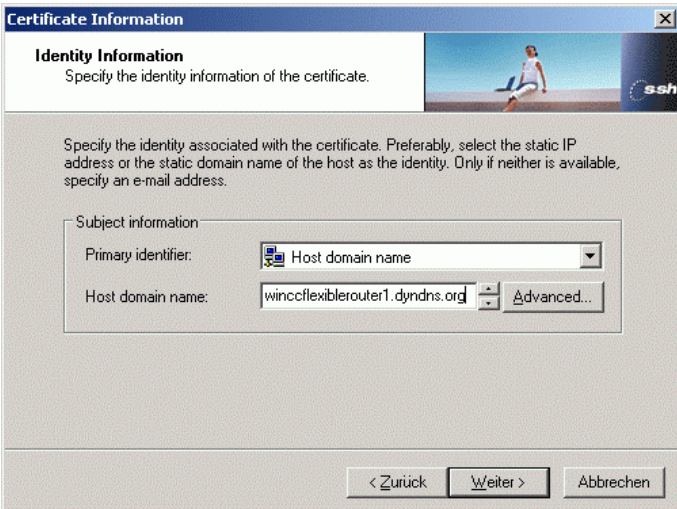
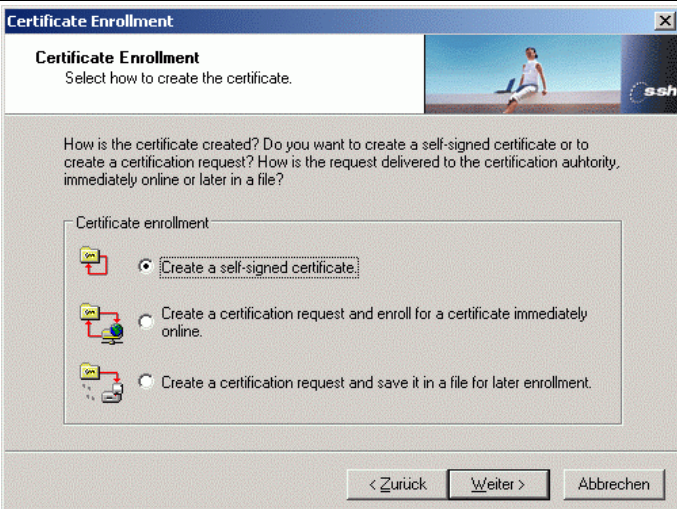
Eine aktuelle Version finden Sie auch immer im Downloadbereich der Firma Bintec.

Die Dialoge können daher auch etwas abweichen.

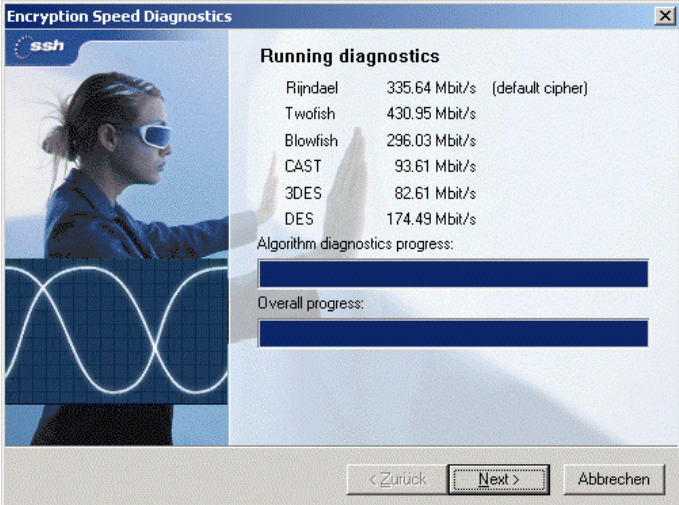
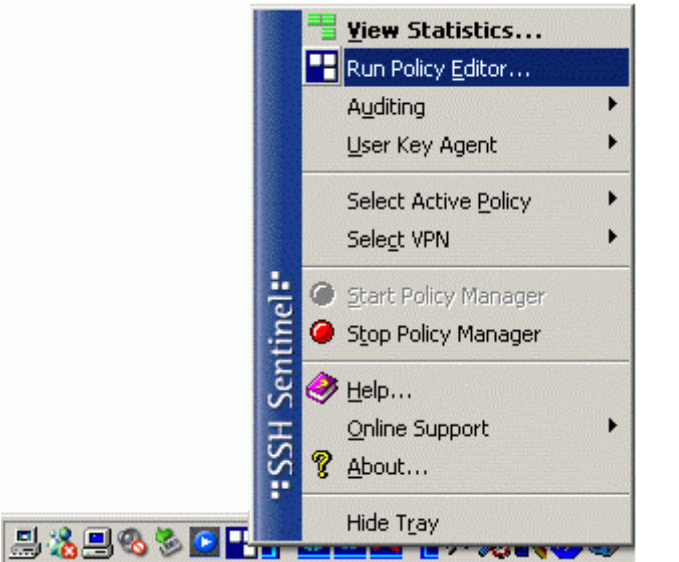
In diesem Dokument sind nicht alle Installationsschritte dokumentiert, da viele Einzelschritte nur mit "Weiter" zu bestätigen sind.

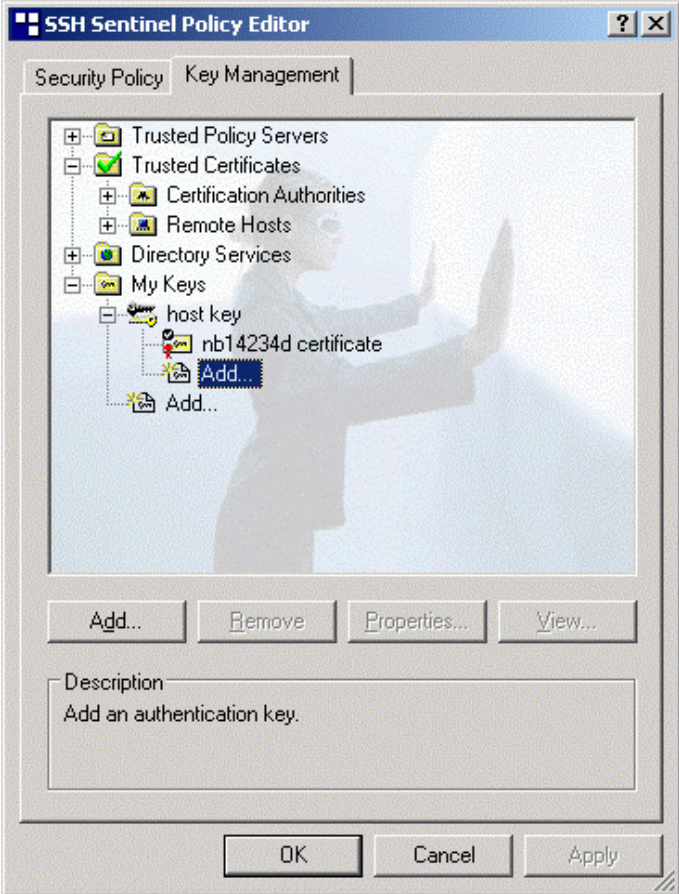
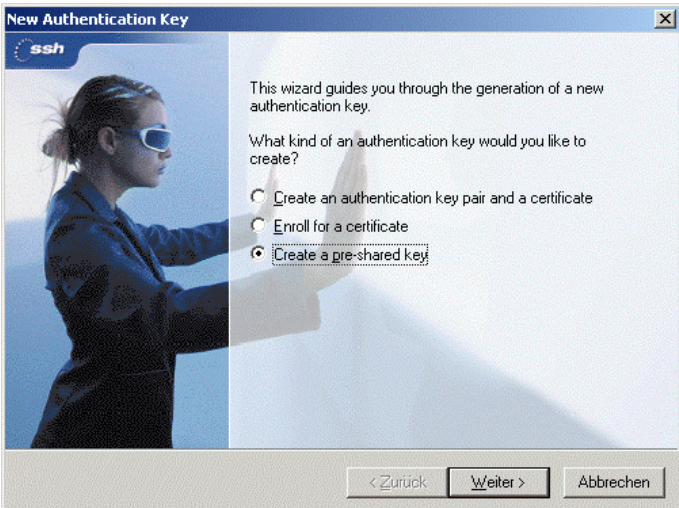
Tabelle 2-4

Nr.	Aktion	Anmerkung
1	Beachten Sie bei diesem Bild, dass Sie die Mouse ständig in Bewegung halten, da sonst der Installationsfortschrittsbalken nicht weiter läuft.	


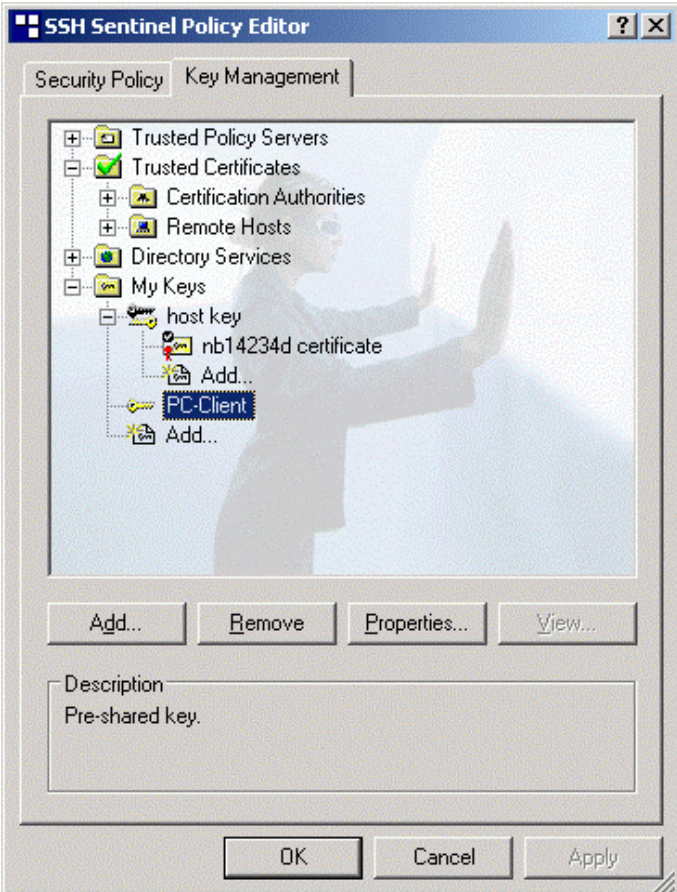
<p>2</p>	<p>Während dieser Phase werden schon bestimmte Teile der Verschlüsselung generiert.</p>	
<p>3</p>	<p>Geben Sie jetzt den Internetnamen Ihres Routers an.</p>	
<p>4</p>	<p>In diesem Fenster wählen Sie den ersten Punkt aus (<b>Create a self-signed certificate</b>), da Sie am Router keine Zertifizierung konfiguriert haben.</p>	

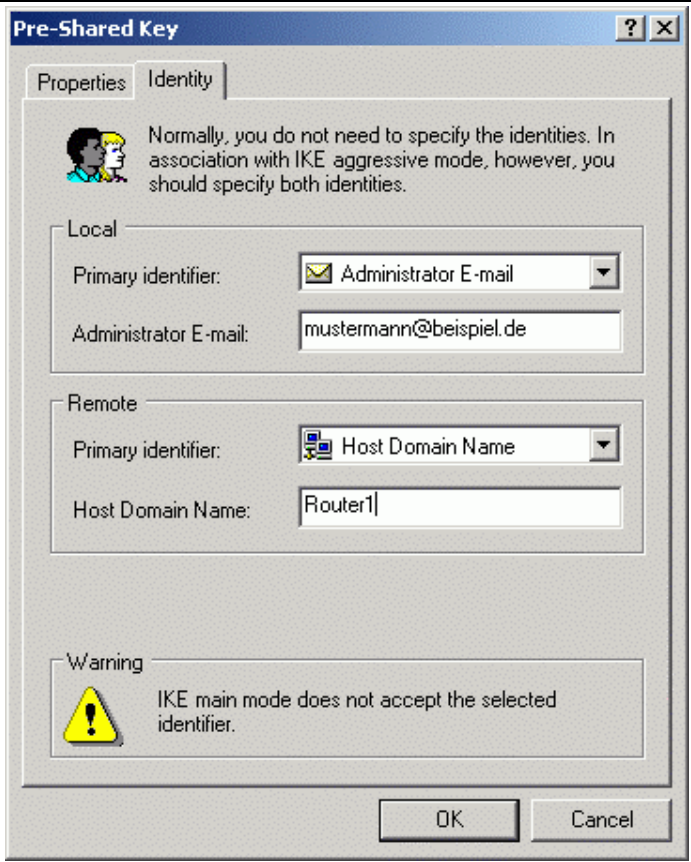


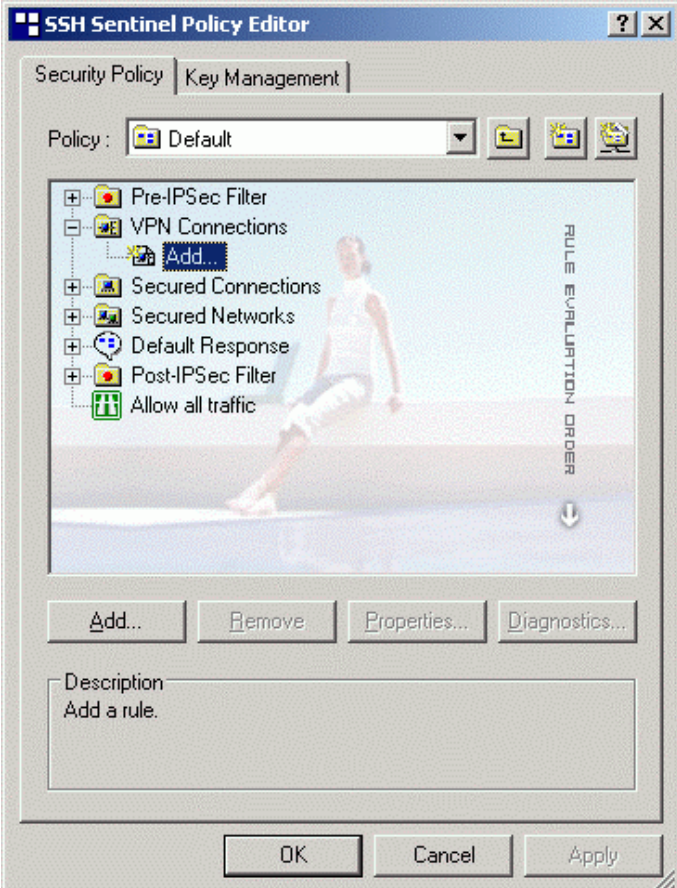

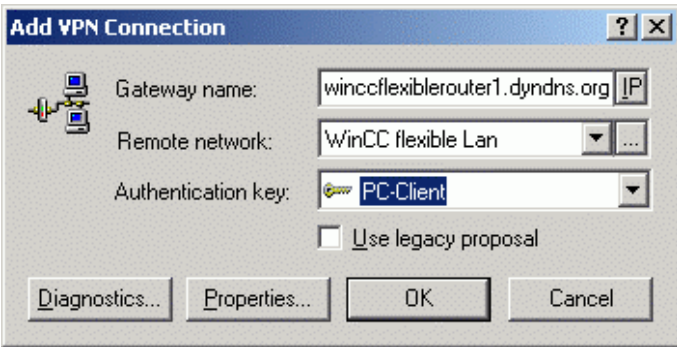
<p>5 Die Installationswizard führt noch eine Diagnose der einzelnen Verschlüsselungsalgorithmen durch und somit ist die Installation beendet.</p>	
<p>6 Nach einem Neustart Ihres PCs, finden Sie in Ihrer Taskleiste das Icon des <b>SSH Sentinel</b>, dass Sie mit der rechten Mausetaste anwählen können um den <b>Policy Editor</b> zu öffnen.</p>	

<p>7 Unter der Registerkarte <b>Key Management</b> fügen Sie im Ordner <b>My Keys</b> über <b>Add</b> einen neuen Schlüssel hinzu.</p>	
<p>8 Wählen Sie den Punkt <b>Create a pre-shared key</b></p>	

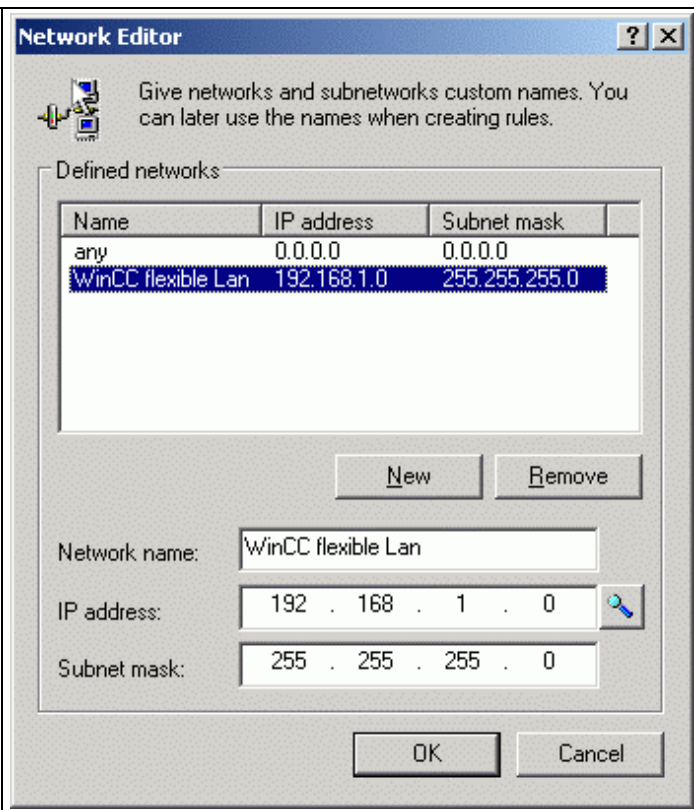


<p>9</p>	<p>Der <b>Name</b> für den Schlüssel kann frei gewählt werden. Unter dem Begriff <b>Shared secret</b> tragen Sie den schon im Router eingetragenen <b>Pre Shared Key</b> ein.</p> <p>Nach dem <b>Fertig stellen</b> müssen Sie noch weitere Einstellungen in den Eigenschaften des Schlüssels vornehmen.</p>	
<p>10</p>	<p>Wählen Sie dazu Ihren neu erstellten Schlüssel an und betätigen Sie die Schaltfläche <b>Properties...</b></p>	

<p>11 Der <b>Local</b> &gt; <b>Primary Identifier</b> entspricht dem Wert, der im Router projektierten Peer IDs.</p> <p>Der <b>Remote</b> &gt; <b>Primary Identifier</b> muss dem für Local ID eingetragenen Namen des Routers entsprechen.</p> <p>Mit diesen Einstellungen ist die Konfiguration des Schlüssels abgeschlossen.</p> <p>Hinweis: Es handelt sich hierbei um die zuvor notierten Einträge aus der PC-Client Partnerkonfiguration Ihres Routers.</p>	
---	---

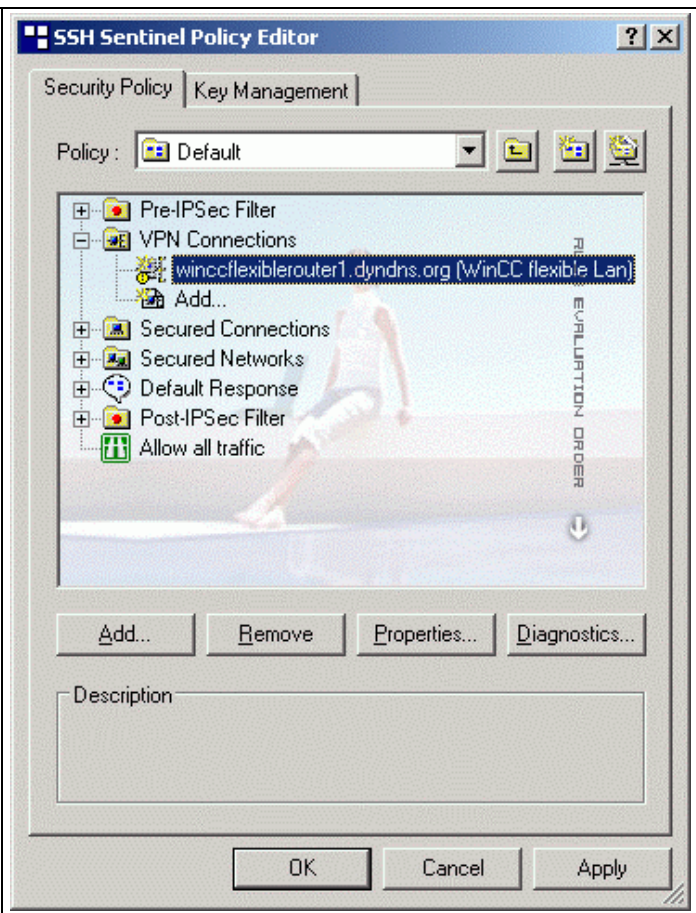
<p>12</p>	<p>Jetzt muss noch die eigentliche VPN Verbindung erstellt werden mit der der Router angesprochen wird.</p> <p>Begeben Sie sich dafür in die Registerkarte <b>Security Policy</b> auf den Ordner <b>VPN Connection</b> und fügen Sie über <b>Add</b> eine Neue Verbindung hinzu. Im <b>Policy Editor</b> können mehrere Schlüssel und auch mehrere Verbindungen projiziert werden. Es kann aber immer nur eine Verbindung gestartet werden.</p>	
<p>13</p>	<p>Tragen Sie zuerst den DYNDNS Namen oder die IP-Adresse Ihres Routers als <b>Gateway name</b> ein. Die Verwendung der IP-Adresse macht jedoch nur Sinn, wenn Ihr Router eine feste Adresse im Internet hat.</p> <p>Als <b>Remote Netzwerk</b> können Sie den default Wert "any" benutzen oder Sie erstellen über die Schaltfläche  selbst ein Remote Netzwerk, mit den lokalen Netzwerkparametern Ihres Routers.</p> <p>Für den <b>Authentication Key</b> benutzen Sie den Schlüssel, der auch auf dem Router hinterlegt ist.</p>	

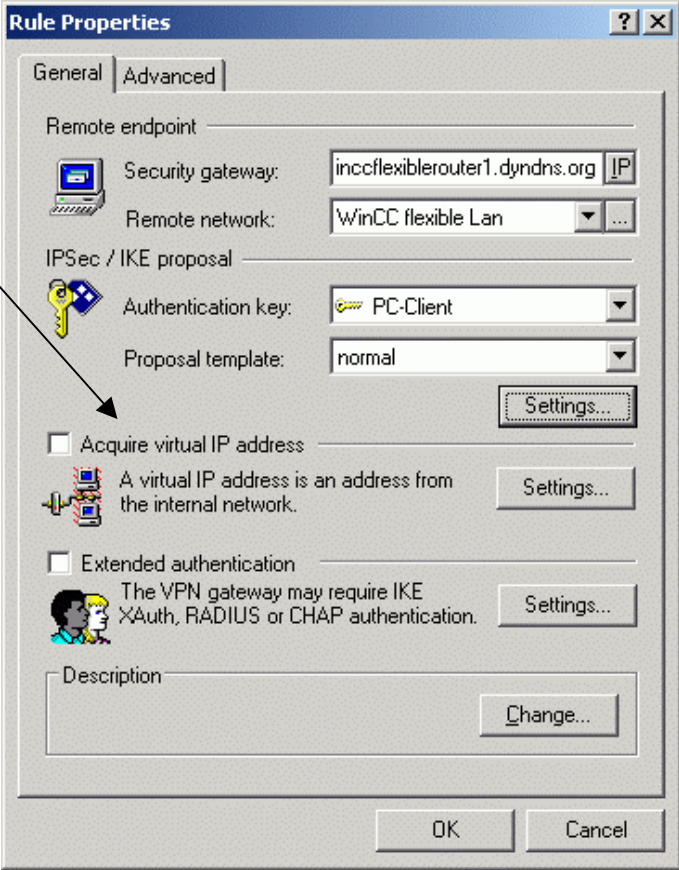
14 Hier sind die Werte aus diesem Beispiel dargestellt. Sie geben wiederum nur die Startadresse an. Auf die Verschlüsselung hat die Angabe des Remote Network keinen Einfluss. Bestätigen Sie alle Dialoge mit **OK**.



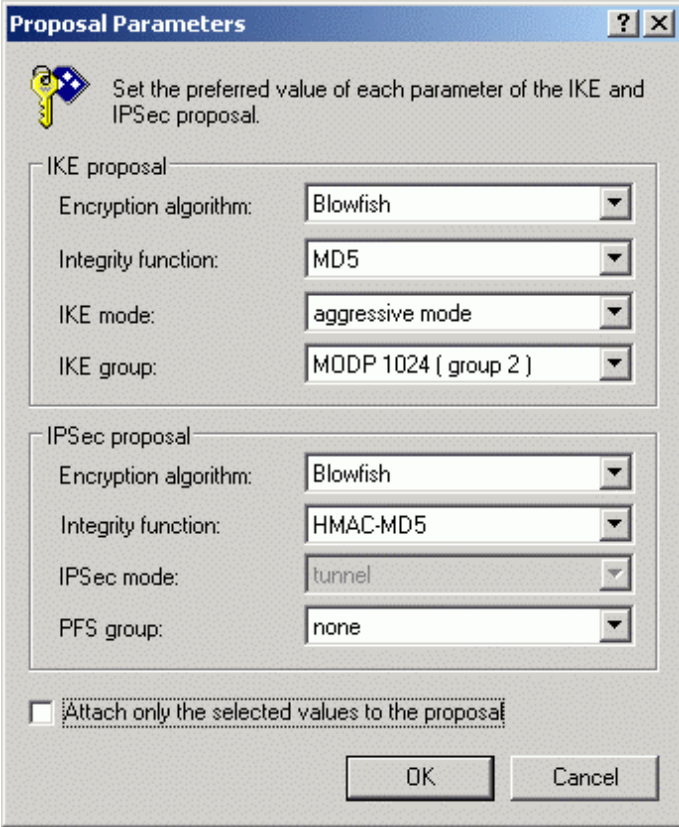
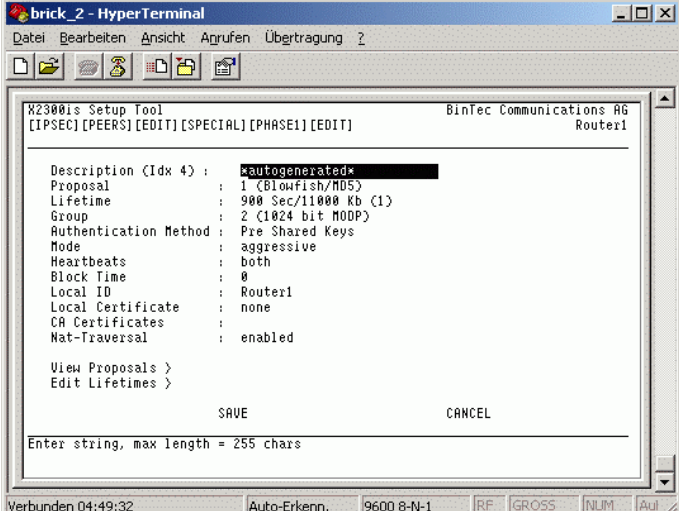


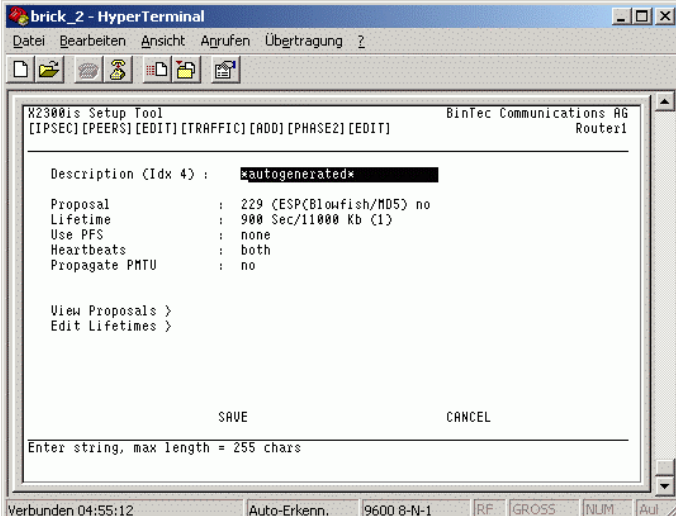
15 In den Eigenschaften der Verbindung müssen nun noch Anpassungen gemacht werden, die die Authentifizierung über die schon erwähnten Algorithmen betreffen. Öffnen Sie dazu erneut über die Schaltfläche **Properties...** den nun folgenden Dialog.



<p>16 In der Registerkarte <b>General</b> betätigen Sie unter dem Punkt <b>IPSec / IKE proposal</b> die Schaltfläche <b>Settings...</b></p> <p><b>Hinweis:</b> In den Settings bei <b>Acquire Virtual IP address</b> kann die Quell-IP-Adresse der Datenpakete angepasst werden. Es kann entweder manuell eine Virtual IP eingetragen werden oder per DHCP bezogen werden. Die Router-Einstellungen müssen darauf abgestimmt werden. Wird die Option " Acquire Virtual IP address " nicht benutzt, so wird als Quell-IP-Adresse die eigene vom ISP zugewiesene IP-Adresse verwendet.</p> <p>In diesem Beispiel wurde die Option " Acquire Virtual IP address " nicht verwendet.</p>	 <p>The screenshot shows the 'Rule Properties' dialog box with the 'General' tab selected. The 'Remote endpoint' section includes 'Security gateway' (inccflexiblerouter1.dyndns.org) and 'Remote network' (WinCC flexible Lan). The 'IPSec / IKE proposal' section includes 'Authentication key' (PC-Client) and 'Proposal template' (normal). The 'Acquire virtual IP address' checkbox is unchecked. Below it, there is a 'Settings...' button. The 'Extended authentication' checkbox is also unchecked, with a 'Settings...' button below it. At the bottom, there is a 'Description' field and a 'Change...' button. The 'OK' and 'Cancel' buttons are at the very bottom.</p>
---	---

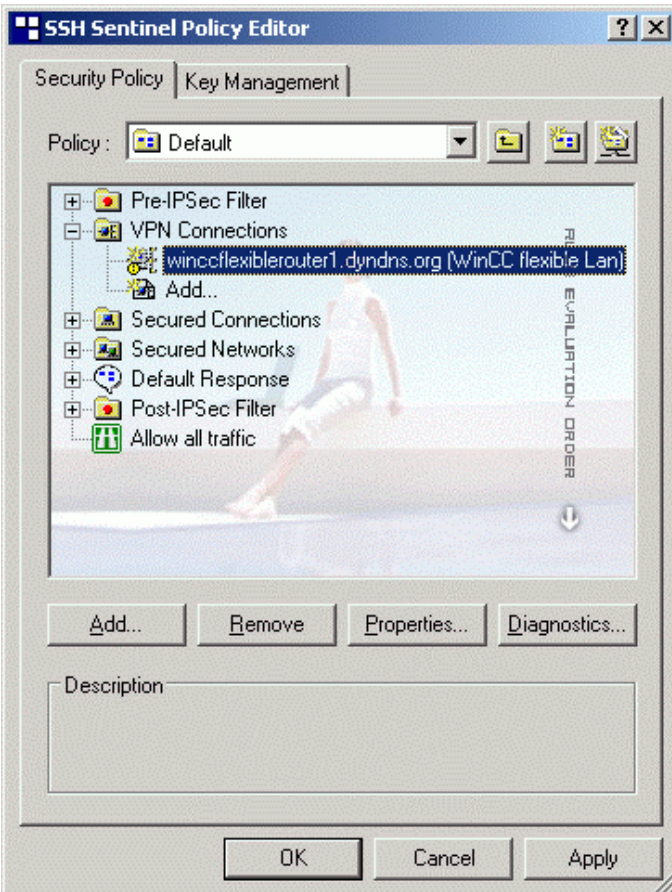


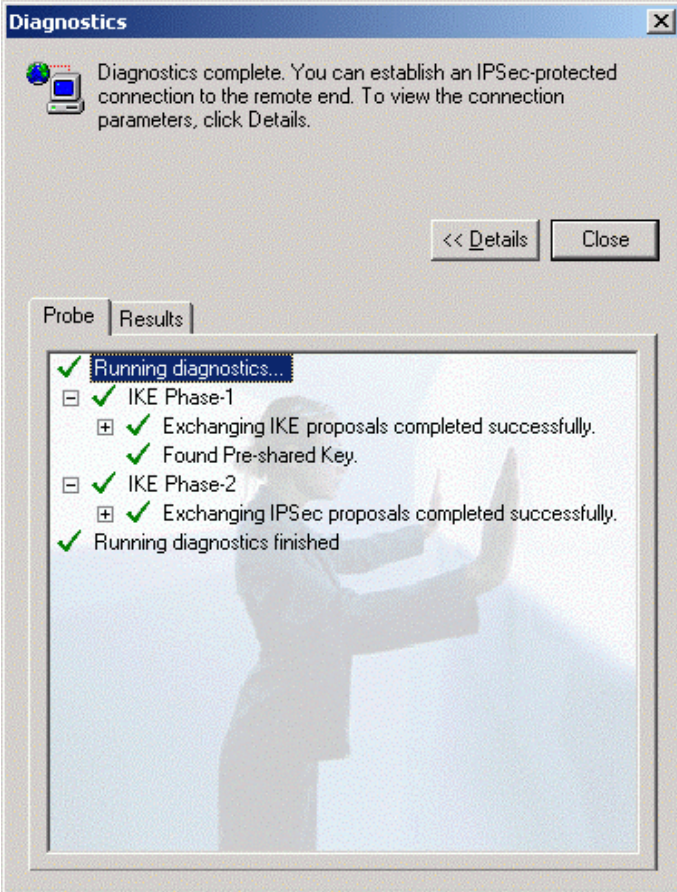
<p>17</p>	<p><b>Hinweis:</b> Da Ihr Rechner immer dynamisch eine offizielle IP-Adresse vom Provider erhält, muss der Parameter <b>IKE Mode</b> auf <b>Aggressive Mode</b> eingestellt werden. Diese Einstellung muss auch am Router so ausgewählt sein.</p> <p>Die Einstellungen für <b>Encryption algorithm</b> sollten denen am Router angepasst werden, wie es in den Bildern 18 und 19 abgebildet ist.</p> <p>Der Client bietet Ihnen grundsätzlich alle unterstützten Verschlüsselungsmethoden an, die Sie auch im Router verwenden können. Nach Vervollständigung der Daten schließen Sie den Dialog mit <b>OK</b>.</p>	
<p>18</p>	<p>Vergleich mit den Einstellungen im Router für die Phase 1 der Authentifizierung. (IKE proposal)</p>	

19	Vergleich mit den Einstellungen im Router für die Phase 2 der Authentifizierung. (IPSec proposal)	 <p>The screenshot shows a terminal window titled 'brick_2 - HyperTerminal' with a menu bar (Datei, Bearbeiten, Ansicht, Anrufen, Übertragung ?) and a toolbar. The main content is the 'X2300is Setup Tool' for 'BinTec Communications AG Router1'. It displays the configuration for Phase 2 of an IPSec proposal:</p> <pre>X2300is Setup Tool                               BinTec Communications AG [IPSEC] [PEERS] [EDIT] [TRAFFIC] [ADD] [PHASE2] [EDIT]   Router1  Description (Idx 4) : *autogenerated*  Proposal      : 229 (ESP(Blowfish/MD5) no Lifetime     : 900 Sec/11000 Kb (1) Use PFS      : none Heartbeats   : both Propagate PMTU : no  View Proposals &gt; Edit Lifetimes &gt;  SAVE                                CANCEL  Enter string, max length = 255 chars</pre> <p>At the bottom of the terminal window, the status bar shows 'Verbunden 04:55:12', 'Auto-Erkenn.', '9600 8-N-1', 'RF', 'GROSS', 'NUM', and 'AUI'.</p>
----	---	--

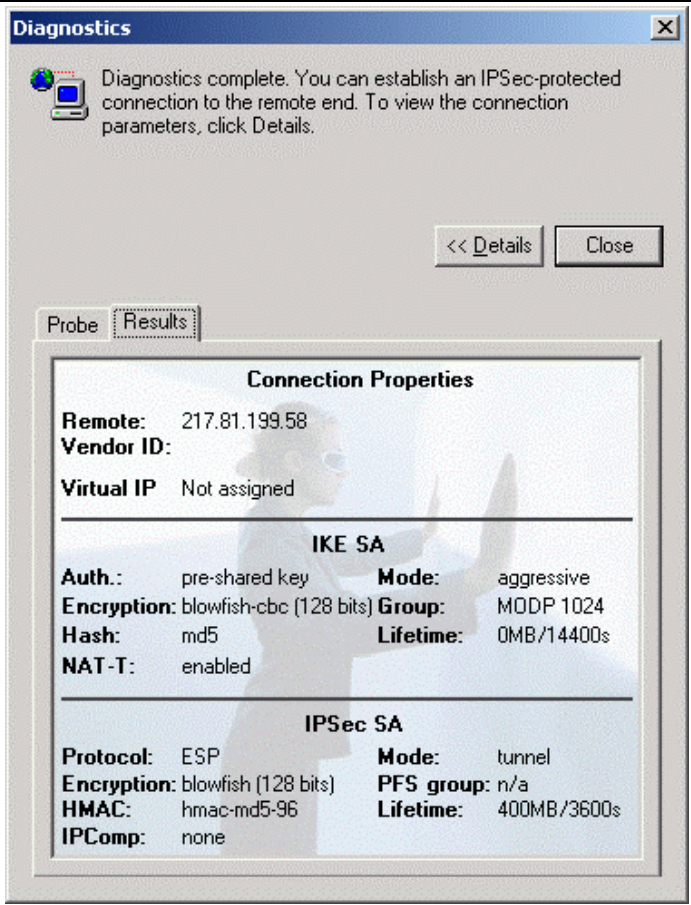
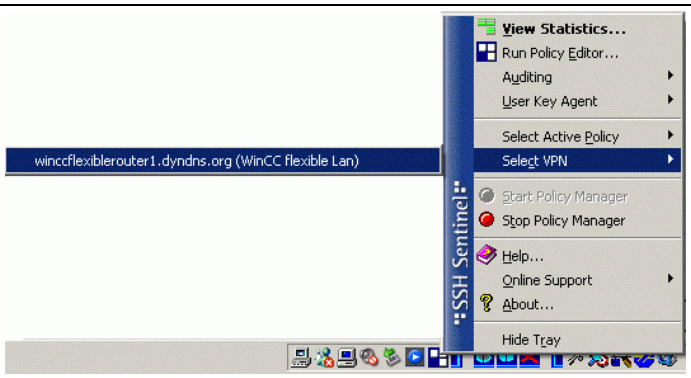
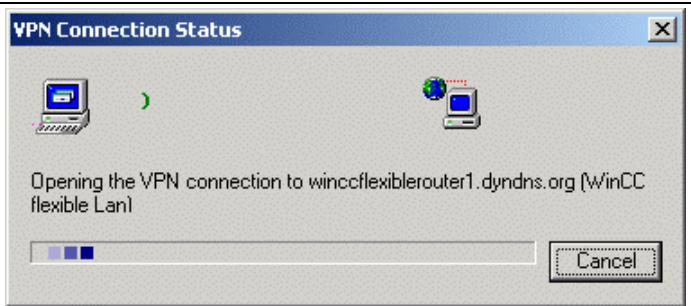
## 2.5 Test der neu erstellten Verbindung:

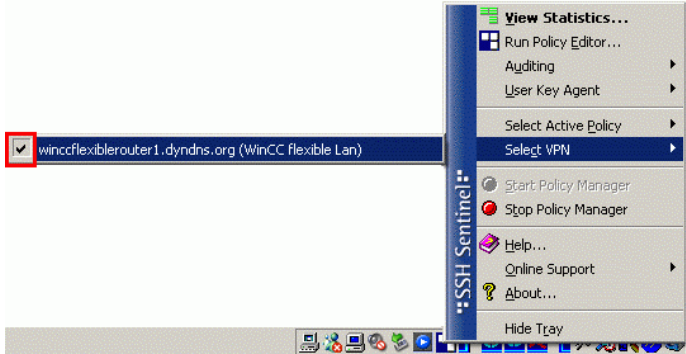
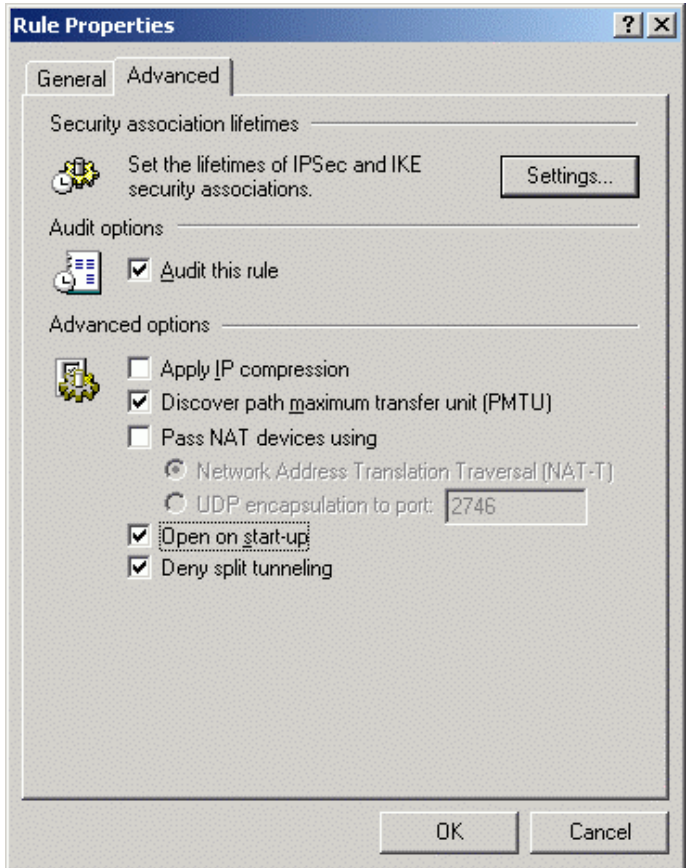
Tabelle 2-5

Nr.	Aktion	Anmerkung
1	<p>Starten Sie die DFÜ Verbindung zu Ihrem Internet Service Provider. Öffnen Sie erneut Ihren <b>Policy Editor</b> und wählen Sie die benötigte VPN Verbindung aus. Mit der Schaltfläche <b>Diagnostics...</b> können Sie nun sehen, ob die Verschlüsselung richtig erkannt wird.</p>	

2	Wenn alles richtig eingestellt ist, sollte der folgende Dialog erscheinen.	 <p>The screenshot shows a 'Diagnostics' dialog box with a blue title bar and a close button. The main text reads: 'Diagnostics complete. You can establish an IPSec-protected connection to the remote end. To view the connection parameters, click Details.' Below this text are two buttons: '&lt;&lt; Details' and 'Close'. The dialog has two tabs: 'Probe' and 'Results'. The 'Results' tab is active, showing a tree view of diagnostic steps, all marked with green checkmarks:</p> <ul style="list-style-type: none"><li>Running diagnostics...</li><li>[-] ✓ IKE Phase-1<ul style="list-style-type: none"><li>[+] ✓ Exchanging IKE proposals completed successfully.</li><li>✓ Found Pre-shared Key.</li></ul></li><li>[-] ✓ IKE Phase-2<ul style="list-style-type: none"><li>[+] ✓ Exchanging IPSec proposals completed successfully.</li></ul></li><li>✓ Running diagnostics finished</li></ul>
---	--	---



<p>3 In der Registerkarte <b>Results</b> sehen Sie, wie die Verbindung eingestellt ist. Bei einer fehlerhaften Projektierung sind entsprechend nur die Teile mit einem Hacken versehen, die korrekt erkannt worden sind.</p>	
<p>4 Schließen Sie bitte jetzt alle Dialoge und klicken Sie mit der rechten Maustaste auf den <b>SSH Sentinel</b> in Ihrer Taskleiste. Über den Menüpunkt <b>Select VPN</b> können Sie nun alle Verbindungen sehen und durch Anwahl aktivieren.</p>	
<p>5 Es erfolgt der Verbindungsaufbau.</p>	

<p>6 Nach erfolgreichem Verbindungsaufbau ist hinter dem Verbindungsnamen ein Haken zu sehen.</p>	
<p>7 Der Tunnelaufbau kann entweder über Auswahl von Select VPN manuell erfolgen oder aber automatisch nach Aufbau der DFÜ-Verbindung zum ISP. Um dies nutzen zu können, muss in der Registerkarte <b>Advanced</b> in den Eigenschaften Ihrer VPN Connection die Option <b>Open on start-up</b> aktiviert werden.</p>	



Damit ist die Einstellung Ihrer IPSec Verbindungen abgeschlossen.

Einen Test können Sie schnell und einfach mit einem Ping auf eine im Firmennetzwerk befindliche IP-Adresse durchführen.

Sollte sie keinen erfolgreichen Verbindungsaufbau erhalten, kontrollieren Sie noch einmal alle Einstellungen im Router und vergleichen diese mit Ihrem Client.

Bei der genaueren Fehlersuche stehen Ihnen auch der Support des jeweiligen Router Herstellers zur Verfügung.

Diese können mit einem Debugger direkt auf dem Router nachsehen, welche Einstellung falsch ist.

Eine Erklärung des Debuggers ist an dieser Stelle nicht möglich.

## 3 Glossar

Tabelle 3-1

Nr.	Abkürzung	Beschreibung
1	ADSL	<p>Abkürzung für Asymmetric Digital Subscriber Line (dt. Asymmetrische digitale Teilnehmeranschlussleitung).</p> <p>ADSL ermöglicht die Nutzung der Infrastruktur des vorhandenen Telefonnetzes für Breitbanddienste. Auf den Kupferdoppeladern der analogen und digitalen Telefonanschlüsse (POTS bzw. ISDN) werden bei ADSL zusätzlich Daten für Internetdienste übertragen. Dazu wird das von ADSL genutzte Frequenzspektrum in mehrere Bereiche aufgeteilt. Zwischen dem Teilnehmeranschluss und der Ortvermittlungsstelle können die Telefonie- und Datensignale so problemlos nebeneinander transportiert werden. Für die Trennung bzw. Zusammenführung der Signale sorgt auf beiden Seiten ein Splitter.</p> <p>Asymmetrisch ist bei ADSL die maximal erreichbare Übertragungsrate in beide Richtungen - Upstream und Downstream. Für den Upstream stehen bei ADSL maximal 1,5 MBit/s zur Verfügung und für den Downstream 8 MBit/s. Da die erreichbare Übertragungsrate mit steigender Entfernung zwischen Ortvermittlungsstelle und Teilnehmer jedoch deutlich abnimmt, sind diese Werte für die überwiegende Anzahl der Anschlüsse in der Praxis nicht zu erreichen.</p> <p>Die asymmetrischen DSL-Varianten, bei denen für den Upstream bis zu 256 kBit/s und für den Downstream bis zu 3 MBit/s zur Verfügung stehen, eignen sich vor allem für private Nutzer und kleinere Unternehmen, die auf ihrem PC keine aufwendigen und häufig angeforderten Internetinhalte für andere Nutzer zur Verfügung stellen wollen.</p>
2	BBAE	<p>Abkürzung für Breitband-Anschlusseinheit (engl. Broadband Access Equipment).</p> <p>Der BBAE bildet auf der Seite des Teilnehmeranschlusses den physikalischen Abschluss einer breitbandig genutzten Anschlussleitung. Er trennt das Anbieternetz von der Anschlussverkabelung beim Teilnehmer und bereitet die Signale für die Übermittlung über den jeweiligen Verbindungsabschnitt auf.</p> <p>Bei ADSL-Anschlüssen beinhaltet der BBAE meist auch den Splitter, der das Breitband- und Schmalbandsignal voneinander trennt bzw. wieder zusammenführt</p>
3	CAPI	<p>Common Application Programming Interface.</p> <p>Normierte Software-Schnittstelle für die Kommunikation zwischen Soft- und Hardware.</p> <p>Mit CAPI wird ein Programm bezeichnet, das mit einer ISDN-Karte geliefert wird und deren Ansteuerung übernimmt. Andere Programme, die über die Karte Daten übertragen wollen, müssen diese Daten nur an den CAPI-Treiber übergeben.</p>

4	DSL	<p>Abkürzung für Digital Subscriber Line (dt. digitale Teilnehmeranschlussleitung)</p> <p>Die DSL-Technik ermöglicht es, über herkömmliche Telefonleitungen die Datenübertragung wesentlich zu beschleunigen und bietet sich somit vor allem für die schnelle Internetnutzung an. ISDN-Dienste oder analoge Telefonie laufen dabei ungestört auf der gleichen Leitung weiter. Die hohen Übertragungsraten werden erreicht, indem man den verwendeten Frequenzbereich vergrößert. So ermöglicht ADSL Übertragungsraten von bis zu 8 MBit/s. Sehr verbreitet sind Anschlüsse mit 768 kBit/s.</p> <p>Hinter der Bezeichnung DSL verbirgt sich eine ganze Familie von Technologien, die unter dem Sammelbegriff xDSL zusammengefasst wird. In Deutschland werden Anschlüsse für Privatkunden vor allem mit den Technologien Asymmetric DSL (ADSL) und Single Pair DSL (SDSL) angeboten. Das wesentlich verbreitetere ADSL überträgt die Internetdaten im vorhandenen Telefonnetz oberhalb der Telefonfrequenzen zwischen 138 und 1.104 kHz. ADSL ist beispielsweise auch die Basis für das T-DSL-Angebot der Deutschen Telekom AG.</p>
5	DynDNS	<p>Der Begriff DynDNS steht für dynamisches DNS und soll darauf hindeuten, dass Sie als Kunde die zu einem Namen gehörige IP-Adresse selbst im DNS-Server eintragen können</p> <p>Man kontaktiert die IP Adresse des Partners und die Verbindung steht. Da feste IP Adressen aber teuer sind, wählen sich die meisten Benutzer bei Diensteanbietern ein und bekommen eine dynamische IP Adresse zugewiesen.</p> <p>Diese wechselt bei jeder Einwahl (daher der Ausdruck dynamisch), so dass das Auffinden eines Partners mit dynamischer IP Adresse unmöglich ist. Hier bieten DynDNS Server im Internet Abhilfe. Sie ermöglichen das Auffinden von Partnern trotz dynamischer IP Adresse. Ist der Partner bekannt, d.h. ist seine IP Adresse bekannt, steht einer Kommunikation nichts mehr im Wege. Zur Sicherheit kann in einem zweiten Schritt die Kommunikation mit dem Partner mit Hilfe von z.B. IPSec verschlüsselt werden.</p>
6	IPsec (Internet Protocol Security)	<p>IPSec ist ein Protokoll, das zum Aufbau einer sicheren IP-Verbindung verwendet werden kann.</p> <p>Man unterscheidet zwei Betriebsarten:</p> <ol style="list-style-type: none"> <li>1. Der Tunnelmodus Bei dieser Betriebsart wird das ganze IP-Paket verschlüsselt. Der Tunnelmodus wird v.a. zur abhörsicheren Übertragung von Daten zwischen zwei Firmenstandorten oder zwischen einem privaten Computer und einem Firmennetzwerk (z.B. bei Arbeiten von Zuhause) über das Internet verwendet (VPN).</li> <li>2. Der Transportmodus Hierbei wird ausschließlich der Datenteil verschlüsselt. Dies wird für die Übertragung von kritischen Daten verwendet, z.B. bei Passwörtern</li> </ol>

7	ISDN	<p>Abkürzung für Integrated Services Digital Network (dt. Dienste integrierendes digitales Fernmeldenetz)</p> <p>Hervorstechendes Merkmal von ISDN-Telefonanschlüssen ist die Verfügbarkeit von mindestens zwei gleichzeitig nutzbaren Basiskanälen (B-Kanäle). Dadurch bleibt ein Teilnehmer auch dann telefonisch erreichbar, wenn er mit dem Internet verbunden ist oder ein Fax verschickt. Zwei parallele Telefongespräche von einem Anschluss aus sind ebenso möglich. Zudem werden höhere Übertragungsraten als mit einem analogen Anschluss erreicht: Jeder B-Kanal kann 64 kBit/s übertragen, beide zusammen also 128 kBit/s. Die digitale Übertragungs- und Vermittlungstechnik von ISDN gestattet, dass am Telefonanschluss so unterschiedliche Kommunikationsarten wie Telefonieren, Faxen oder Internetverbindungen möglich sind.</p> <p>ISDN verwendet für die Anbindung der Kunden an die Vermittlungsstelle weiterhin die Kabel des zuvor analog betriebenen Telefonnetzes. Die ISDN-Technologie nutzt diese jedoch deutlich effizienter und flexibler. Verbindungen lassen sich schneller aufbauen, die Sprachqualität ist erheblich besser und die Übertragung von Daten ist nicht nur schneller, sondern dank Fehlerkorrektur auch extrem zuverlässig.</p>
8	NTBA	<p>Abkürzung für Network Termination Basic Rate Access (dt. Netzabschlussgerät am Basisanschluss).</p> <p>Der NTBA bildet den Netzabschluss des öffentlichen ISDN-Netzes. Er setzt das Signal des Netzbetreibers von dessen Zweidrahtleitung (UK0-Bus) auf eine Vierdrahtleitung (S0-Bus) um.</p> <p>Der NTBA wird über die ISDN-Speisespannung von der Vermittlungsstelle mit Strom versorgt - der NTBA versorgt wiederum den S0-Bus. Im normalen Betriebszustand wird der NTBA dazu zusätzlich über ein Netzteil gespeist. In diesem Betriebszustand kann er bis zu vier am S0-Bus angeschlossene Endgeräte versorgen, die über keine eigene Stromversorgung verfügen.</p> <p>Wird der NTBA ohne ein zusätzliches Netzteil betrieben bzw. fällt die Stromversorgung aus, so verwendet der NTBA die ISDN-Speisespannung des Netzbetreibers für einen Notstrombetrieb.</p>
9	Port Forwarding	<p>Port-Forwarding ist eine Technik, um die Abbildung von Ports auf IP-Adressen in NAT-Netzen (Network Address Translation) zu ermöglichen. Das heisst, wenn Router-Ports fest auf eine bestimmte IP-Adresse weitergeleitet werden müssen. Diese Technik wird auch Mapping oder Port-Weiterleitung genannt und ist eine Funktion, die viele der aktuellen DSL Router anbieten. Zu diesem Zweck ist meist in den erweiterten Einstellungen des Routers eine Tabelle vorhanden, in der ein zu "mappender" Port fest einer bestimmten lokalen IP-Adresse zugeordnet wird.</p>
10	Router	<p>Router sind zunächst und grundsätzlich Hardware-Geräte oder Software-Programme, mit denen ein oder mehrere Rechner oder ganze Netzwerke mit anderen Netzwerken verbunden werden können.</p>

		<p>Der Router übernimmt dabei die Steuerungszentrale, um Verbindungsanfragen an das gewünschte Netz oder den Dienst weiterzuleiten.</p> <p>Hardware-Router und insbesondere die heutigen ISDN- oder DSL Router verfügen über die Grundfunktionalität hinaus über DHCP-Dienste bzw. DHCP-Server, mit denen die Adressvergabe und Steuerung zentral verwaltet werden kann. Je nach Einstellung können auf die Weise ganze Netzwerke automatisch mit IP-Adressen versorgt werden, was insbesondere unerfahrenen Anwendern entgegen kommt.</p>
11	Splitter	<p>Splitter von engl. to split, dt. aufspalten.</p> <p>Bei ADSL-Anschlüssen teilt der Splitter das vom Anbieternetz kommende Signal in das breitbandige ADSL-Signal und das schmalbandige ISDN-Signal bzw. analoge Telefonsignal auf. Für die Übermittlung in der Gegenrichtung werden die beiden Signalanteile hingegen zusammengeführt, sodass eine zeitgleiche Übermittlung über die Teilnehmeranschlussleitung möglich ist.</p> <p>Der Splitter ist häufig direkt in der Breitband-Anschlusseinheit enthalten (BBAE).</p>
12	TCP	<p>TCP, die Abkürzung für Transmission Control Protocol, ist ein wesentlicher Bestandteil des TCP/IP-Protokolls. Es ist auf Verbindungen aufgebaut und verlangt für jedes abgeschickte Paket eine Empfangsbestätigung.</p>
13	TCP/IP	<p>TCP/IP Abkürzung für Transmission control protocol/internet protocol. Bezeichnet zumeist die ganze Familie von Protokollen. Es wurde entwickelt, um Computer in verschiedenen Netzwerken miteinander zu verbinden.</p> <p>Heute wird TCP/IP in vielen LANs (Local Area Network) eingesetzt und ist Basis für das weltumspannende Internet.</p>
14	T-DSL	<p>Die Deutsche Telekom bietet seit Ende der 90er Jahre ADSL-Anschlüsse unter dem Namen T-DSL an. T-DSL ist die meistgenutzte DSL-Variante und damit zugleich der meistgenutzte Breitbandzugang ins Internet in Deutschland. Nicht nur die Deutsche Telekom ermöglicht über die Tochtergesellschaft T-Online den T-DSL Zugang zum Internet, sondern auch eine größere Anzahl von Wiederverkäufern (Reseller). Alle setzen bei der physikalischen Kundenanbindung aber auf die Infrastruktur der Deutschen Telekom. Die restlichen Anbieter verwenden vor allem eigene ADSL-Varianten oder SDSL, das aber symmetrisch arbeitet und Datenraten bis zu 2,3 MBit/s gestattet.</p>
15	VPN (Virtual Privat Network)	<p>Mit Hilfe eines Virtual Private Network (VPN) können Firmen Mitarbeitern von Zuhause oder firmenfremden Standorten sich über das Internet in das Firmennetzwerk (Intranet) einwählen. Ebenso können verschiedene Firmensitze auf diese Weise verbunden werden.</p> <p>Der Vorteil hierbei ist, dass keine Modemstrecken oder angemietete</p>

		<p>Kanäle nötig sind, sondern lediglich eine Internetverbindung. Der Mitarbeiter wählt sich zunächst ins Internet ein. Anschließend wird ein verschlüsselter Kanal (Tunnel) zwischen dem VPN Client und VPN Server aufgebaut. Nach einer Authentifizierung mittels Benutzernamen und Passwort oder öffentlichem Schlüssel/Zertifikat, wird ein verschlüsselter IPSec-Tunnel aufgebaut über den die Daten abhörsicher übertragen werden können.</p>
16	WAN	<p>Unter dem Begriff WAN (Wide Area Network) versteht man Netzwerke, welche Daten über größere Entfernung transportieren als ein LAN (Local Area Network).</p>



## 4 Gewährleistung und Support

Für die vorstehenden/nachfolgenden Siemens-internen Informationen übernehmen wir keine Gewähr.

Eine Haftung von A&D, gleich aus welchem Rechtsgrund, für durch die Verwendung der in der Fachkommunikation beschriebenen Beispiele, Hinweise, Programme, Projektierungs- und Leistungsdaten usw. verursachte Schäden ist ausgeschlossen, soweit nicht z.B. bei Schäden an privatgenutzten Sachen, Personenschäden oder wegen Vorsatzes oder grober Fahrlässigkeit zwingend gehaftet wird.